Kebijakan Sistem Informasi Manajemen Keamanan IT (Information Security Management Policy) Standard ISO 17799 : 27002

Deris Stiawan (Dosen Jurusan Sistem Komputer FASILKOM UNSRI)
Sebuah Pemikiran, Sharing, Ide Pengetahuan, Penelitian

Pendahuluan ...

Perkembangan yang sangat cepat saat ini mau tidak mau perusahaan dan pelaku bisnis harus dapat beradaptasi dengan cepat, kebutuhan akan informasi dan koneksi data untuk update informasi dari kantor tidak mengenal waktu dan tempat, munculnya solusi-solusi unified communications, mobile commuters, dan sebagainya semakin menguatkan bahwa ketepatan dan kecepatan dalam mendapatkan informasi mutlak dibutuhkan. Lihat saja saat ini dimana penggunaan blackberry sangat tinggi penetrasinya di pasar.

Sistem yang dapat diakses dengan availability yang tinggi saat ini dibutuhkan, openness dan terdistribusi pasti sudah menjadi keharusan untuk sistem yang terintegrasi. Server-server yang dikoneksikan terus menerus tiada henti ke jaringan publik mau tidak mau akan membuka lubang-lubang sistem keamanan. Tidak ada sistem yang sempurna, kita hanya dapat meningkatkan dari status tidak aman menjadi relatif lebih aman, karena banyak sekali cara atau metode lubang-lubang keamanan yang dapat ditembus. Lubang keamanan itu baik pada lapisan sistem operasi, aplikasi, layanan, dan sebagainya pasti dapat ditemuka titik kelemahanya. Secara garis besar keamanan sistem informasi dan komputer dapat dibagi dua yaitu keamanan secara *phisikal* dan secara *logikal*. Secara Phisik berarti bagaimana kita mengamankan semua infrastruktur peralatan sistem keamanan kita baik dari sisi server, ruangan, kabel, system backup redundant system, system cadangan power listrik dan lain-lain sedangkan keamanan secara logikal tentang metode keamanan seperti protocol yang digunakan, metode komunikasi datanya, model basis datanya dan sistem operasinya.

Saat ini dengan kesadaran yang tinggi, telah banyak perusahaan atau pelaku bisnis yang telah memperhatikan masalah keamanan sistem informasi dan computernya, apalagi dengan tawaran one stop solution dari vendor-vendor IT semakin mempekecil masalah-masalah keamanan. Namun seringkali peralatan yang mahal tidak diikuti dengan aturan yang jelas dan rasa kesadaran yang tinggi pada pengguna.

Banyak sekali terdapat statement yang salah dari pengguna atau manajemen tentang masalah sistem keamanan computer atau informasi, seperti :

1. "…tetapi kita sudah menggunakan NAT"
2. "kami telah menutup semua paket yg masuk "
3. "Anti virus original kami "keeps us safe"
4. "Maaf kami tidak menggunakan WINDOWS"
5. "Kami mempunyai sistem DMZ"
6. "Kami bukan sebuah target"
7. "Kami tidak mempublikasikan yang krusial di web"
8. "Kami telah mengekripsi data"
9. "kami sudah memiliki firewall yang banyak dan terbaru"
10. "kami mempunyai team tangguh dan hebat"
11. "kami mempunyai dana IT yang unlimitted"

Maka dibutuhkan suatu aturan yang dapat mengikat kepada seluruh pengguna dan karyawan di tempat tersebut yang sifatnya menyeluruh dan standar. Ada banyak standar yang dapat digunakan yang biasanya standar-standar tersebut dibuat oleh vendor solusi IT. Misalnya standarisasi perkabelan, standarisasi pembangunan ruang server, standarisasi server farm, dan sebagainya. Kebutuhan akan kebijakan sistem keamanan sangat dibutuhkan disaat suatu perusahaan atau proses bisnis telah menggunakan peralatan atau sistem IT sebagai salah satu faktor strategi bisnisnya. ISO sebagai salah satu badan dunia yang membuat standarisasi yang digunakan oleh para pengguna dan produsen dalam bidang tertentu. ISO 17799 : 27002 adalah standar yang berisi tentang tahapan praktis untuk mengatur sistem keamanan informasi.

Standar ISO mempunyai 12 klausa keamanan, dengan jumlah 39 kategori utama dalam bidang keamana, dimana dalam beberapa kategori itu mempunyai banyak komponen-komponen yang lebih detail.

Penjabaran kedua-belas klausa itu adalah ;

1. **Risk assessment and treatment**
    a. *Assessing security risks*, perlu dibuat kebijakan tentang resiko yang mungkin akan timbul. Kebijakan dapat dibuat dengan diawali analisa tentang resiko yang mungkin muncul pada sistem keamanan, misalnya ;

        - Berapa besar efek dari berhentinya layanan IT
        - Berapa besar efek resiko pada saat data dan informasi berhasil ditembus oleh penyusup
        - Berapa lama sistem akan normal pada saat layanan terhenti

    b. *Treating security risks treatment*, kebijakan untuk menjamin perawatan pada seluruh sistem IT yang digunakan, aturan yang akan mengikat secara standar tentang perawatan, misalnya
        - Perlu dibuat aturan tentang berapa kali dalam satu waktu untuk masalah maintenance, analisa penetrasi sistem, backup, restorasi, dan sebagainya yang berhubungan dengan kegagalan resiko keamanan.

2. **Security policy**
    a. *Information security policy document & Review of information security policies*, kebijakan ini menyangkut permasalahan tentang bagaimana perusahaan memenuhi berbagai aturan keamanan dan privacy regulation seperti standar dari Health Insurance Portability and Accountability Act (HIPAA) , *Gramm-Leach-Bliley Financial Services Modernization Act (GLBA)*. Misalnya beberapa tipe dari security policy document, seperti ;
        - Mobile computer policy
        - Firewall policy
        - Electronic mail policy
        - Data classification policy
        - Network Security Policy
        - Internet Acceptable use policy
        - Password Policy

b. *Coordination with other security policies*, jangan sampai kebijakan yang telah dibuat atau akan dibuat akan menyebabkan kontradiktif dengan kebijakan yang telah ada dengan departemen lain atau malah dengan visi dan misi perusahaan. Masalah seperti ini sering kali muncul jika policy keamanan yang dibuat tidak melihat blue print perusahaan, misalnya ;

- Dalam policy keamanan karyawan bagian teknis harus dapat leluasa masuk ke ruangan lain sesuai dengan tingkatannya, namun dalam policy perusahaan dibuat aturan tentang model authentikasi sistem untuk masuk ke ruangan tertentu.

3. **Organization of information security**

a. *Internal organization*, hal ini diperlukan untuk koordinasi dengan internal perusaahan, misalnya

- komitmen yang tinggi untuk setiap level management dalam mematuhi semua kebijakan sistem keamanan yang dibuat, akan lebih baik jika dibuatkan aturan tentang komintem manajemen
- Menanamkan tanggung jawab terhadap semua level manajemen dan karyawan atas kebijakan yang telah dibuat
- Harus membuat kebijakan tentang pendefinisian informasi yang masuk dan keluar dari perusahaan dan informasi tersebut harus diklasifikasikan
- Secara periodic melakukan analisa terhadap sistem yang telah dibuat, misalnya dengan menyewa dari pihak luar.

b. *External parties*, karena informasi dan data juga dimanfaatkan dan diakses oleh partner business maka dibutuhkan juga kebijkan untuk arus informasi masuk dan keluar, misalnya ;

- Karena telah mengimplementasikan ERP / Supply chain maka beberapa rekan bisnis dikoneksikan ke sitem database, jangan sampai hak akses yang diberikan disalahgunakan, maka dibutuhkan aturan yang jelas tentang hak aksesnya
- Berapa nilai resiko yang akan terjadi dengan mengkoneksikan rekan bisnis ini, hal ini harus di identifikasi dari awal.
- Antara perusahaan dan rekan bisnis harus dibuat rambu-rambu yang jelas mengenai hak akses informasi ini

- *User id dan Group id*, menerapkan kelompok-kelompok berdasarkan user dan kelompok agar mudah dimaintenence. Dengan password atau user root maka kita bisa mengatur mesin computer tersebut secara penuh. Kita bisa membuat user dan menghapus user, mengakifkan dan menonaktifkan user, membagi quota bagi para user, memberikan akses resource jaringan, sampai dengan instalasi secara penuh pada server.

4. **Asset management**
   a. *Responsibility for assets*, permasalahan asset perusahaan harus juga menjadi perhatian khusus, hal ini dibutuhkan untuk mengklasifikasikan asset data, informasi dan barang serta lainnya dalam sebuah kebijakan, misalnya ;
      - Bagaimana kita dapat mengetahui jumlah barang dan spesifikasi barang jika tidak mengetahui model/format, tanggal creation manufacture dan informasi penting lainnya pada saat ingin mengetahui tentang barang tersebut
      - Harus mendokumentasikan dengan baik tentang informasi database, kontrak atau kerjasama, informasi dari bagian R&D, user manual, training material, operasional, SOP, dan support procedure.
      - Mendata semua peralatan keseluruhn computer secara phisik, peralatan komunikasi, storage media, sistem penyimpanan backup, perangkat lunak, data base, tools dan utilities lainnya.
      - Melakukan klasifikasi informasi, misalnya dengan membuat guidelines atau membuat labeling informasi, bayangkan jika asset yang ada banyak dengan spesifikasi yang sama atau berbeda, haruslah informasi asset dibuat standard dengan mempunyai karakteristik dari setiap asset yang ada.

5. **Human resources security,** pada kebijakan ini terfokus pada employees, kontraktor, dan pengguna lannya tentang tanggung jawab yang ada, misalnya permasalahan pencurian, perusakan dan kehilangan fasilitas, misalnya ;
      - Membuat batasan tanggung jawab, term dan kondisi dari setiap employee
      - Harus membuat pertemuan-pertemuan untuk meningkatkan information security awareness, melakukan edukasi dan training tentang kebijakan dan sistem yang telah dan akan dibangun, hal ini untuk meningkatkan rasa memiliki dan respon dari pengguna

- Perusahaan harus bisa membuat aturan dan regulasi yang baku bagaimana pengaturan hak akses semua karyawan dan pihak luar lainnya yang berhubungan dengan sistem informasi
- Setiap employee harus mempunyai batasan hak akses sesuai dengan jobsdesk dan departemnya
- Kebijakan tentang bagaimana jika seorang pegawai karena sesuatu masalah harus dicabut hak yang melekat, misalnya hak untuk akses ke server, hak bagian dari suatu group, hak akses ke ruang tertentu, dan sebagainya.
- Kebijakan harus dapat mengatur bagaimana jika employee di cabut hak aksesnya dan dalam waktu tertentu di kembalikan dengan persetujuan managemen

6. **Physical and environmental security,** dalam bagian ini harus dapat diatur tentang hak akses secara phisik, kerusakan yang diakibatkan infrastruktur, dapat mengidentifikasi resiko dan nilai dari setiap asset yang diproteksi, ada beberapa isu yang dapat diangkat misalnya ;
    - Membuat sistem dengan mengatur bagaimana jika terjadi force majure (kebakaran, huru-hara, bencana alam)
    - Membuat standar sistem redundant dan backup, membuat aturan dengan menerapkan kegiatan backup secara berkala atau menggunakan sistem cadangan, saat ini trend perkembangan DRC (Disaster Recovery Center) yang biasa digunakan perusahaan banking, dimana menggunakan server cadangan untuk menyalin database ke dalam server lain secara mirroring dengan metode penyalinan bisa diatur.
    - Membuat membuat aturan baku tentang akses computer dan jaringan secara langsung misalnya kabel, server yang diletakkan diruangan khusus, hub, router, dan lain-lain. Ruang server ini sering disebut NOC (Network Operating Center) yang biasanya diruangan khusus yang terpisah dari user dan terdapat rack-rack khusus untuk menempatkan perangkat jaringannya.
    - Ruang server yang dibuat harus memperhatikan masalah ruang akses publik, dan ruang loading dock.
    - Membuat aturan tentang akses kontrol ke ruang server, akses masuk dengan menggunakan id otentikasi (misalnya barcode atau sidikjari) agar tidak semua user dapat masuk ke parimeter keamanan,

- Memperhatikan fasilitas penunjang keamanan seperti alat pemadam kebakaran, pendeteksi asap, alat pendeteksi gerakan dan pendeteksi audio video surviillance dan bahan kimia lainnya yang membahayakan area ruangan.
- Membuat pendataan asset ruangan khusus untuk mendata tentang proses maintenance perangkat tersebut
- Membuat aturan tentang pembatasan penggunaan audio video termasuk kamera photo, HP dan perangkat portable lainnya serta mengatur tentang makan minum dan merokok di area tertentu.

7. **Communications and operations management,** pada bagian ini kebijakan harus dibuat dengan memastikan memeriksa dan mengamankan operasi fasilitas-fasilitas pengolahan informasi.

   a. **Operational procedures and responsibilities,** dengan membuat standar dokumen untuk setiap operasional,
      - Dibutuhkan SOP (Standar Operating Procedure) untuk semua kegiatan, misalnya bagaimana cara mengatur kerja shift pada ruang server, standar penanganan service desk, standar penanganan teknis dan sebagainya

   b. **Third-party service management**, semakin banyak pihak ketiga yang digunakan, maka dibutuhkan mekanisme layanan, report dan perekaman secara berkesinambungan untuk memantau dan menganalisa
      - Buat aturan tentang kerjasama antara pengembang aplikasi third-party yang digunakan
      - Mengatur level instalasi setiap user untuk mengakses data di hardisk

   c. **Protection against malicious and mobile code**, buat aturan tentang pencegahan, pendeteksian dan respon terhadap code malicious, misalnya
      - Pengaturan tentang kebijakan instalasi software third-party terutama yang didapat dari ekternal network
      - Aturalah untuk selalu menggunakan anti-virus, anti-spyware dan lakukan update secara regular
      - Aturalah untuk proses update tersebut apakah akan dilakukan secara terpusat atau di remote oleh admin
      - Lakukan review secara periodic terhadap sistem yang berjalan, bila perlu uninstalled software yang bermasalah dengan kompatibilitas dan membahayakan sistem

- Buat perjanjian yang mengikat dengan produk software yang dibeli, jika nanti ditemukan masalah dapat menghubungi call centernya
- Buat aturan tentang bagaimana jika terjadi trouble sistem pada saat instalasi software third-party
- Lakukan training dan sosialisai tentan kebijakan dan metode ini

d. **Network security management**, Dalam aturan ini akan melindungi semua informasi pada jaringan dan pada supporting network infrastructure.
    - Buat aturan tentang "push information" ke level manajemen untuk performance network
    - Buatlah tampilan untuk memonitor network baik dari sisi perangkat atau akses user, hal ini berguna untuk membuat report
    - Membuat dokumentasi gambar-gambar topology network
    - Mengatur jangan sampai informasi-informasi sensitive infrastructure network dari akses public, hal ini untuk memperkecil kasus social engineering
    - Aturlah tentang pengumpulan logging termasuk aktivitas keamanan
    - Lakukan koordinasi dengan pihak lain (konsultan, CERT, ID-SIRTI, dan lain-lain)
    - Implementasikan layanan network, seperti authentication, encryption dan koneksi control
    - Buat kerjasama dengan penyelenggara sistem keamanan seperti penggunaan digital certificate, kunci public, sistem OTP dan sebagainya
    - Buat control akses ke infrastruktru network termasuk akses wireless, akses data, atau lainnya yang berhubungan dengan informasi dan data
    - Aturan tentang proteksi pertukaran informasi dari interception, copying, modification, mis-routing
    - Pada saat data disimpan secara physical buatlah aturan yang baku tentang packaging, locked container, temper-evident tangging, penomeran locker, surat pengantar dan recording historinya.
    - Buat aturan tentang penggunaan electronic messaging (email, IM, audio-video conference, dan sebagainya), misalnya tentang pembatasan akses, attachment file, transmit file, yang berhubungan dengan pengaruh pada sistem keamanan
    - Jika dimungkinkan tetapkan untuk penggunaan kunci public dengan PGP atau sistem keamanan lainnya untuk proses email

- Jika menggunakan layanan e-commerce, buatlah aturan layanan dengan pihak lain (authority security atau banking) dan perhatikan penggunaan aplikasi yang digunakn

e. **Monitoring**, dalam kategori ini aktivitas proses menjadi perhatian utama, diantaranya ;

- Buat team NMC (Network Monitoring Center) untuk memantau traffic, aktivitas di jaringan dan infrastruktur yang memantau secara terus-menurs 24 jam
- Team NMC dibawah tanggung jawab departemen teknis,NMC sangat berperan dalam mengetahui aktivitas secara dini baik anomaly, serangan atau failure dari sistem yang berjalan
- Buat sistem ticketing untuk pengantrian gangguan di helpdesk, hal ini untuk meningkatkan layanan
- Buat sistem monitoring secara menyeluruh untuk mengatahui semua proses dan aktivitas yang terjadi di jaringan, dengan protocol SNMP dan beberapa aplikasi standar dapat memberikan informasi yang detail
- Lakukan monitoring secara keseluruhan (router, switching, server, last miles, resources hardware dan devices lainnya)
- Bila perlu integrasikan monitoring ke sistem lainnya misalnya sms, email, dan aplikasi mobile lainnya
- Buat aturan untuk memproteksi Logging akses dan proses, lakukan recording untuk setiap log dari administrator sampai dengan operator, Fault logging, hal ini juga untuk mendukung dari job desk ID-SIRTI.
- *Automatic Lock*, aturan yang memungkinkan penguncian sistem secara otomatis, jika terjadi misalkan penulisan password yang salah sebanyak tiga kali. Ini sangat berguna untuk user yang bisa login ke server.
- *Check Log adminstrasi* secara priodik dengan melakukan checking semua aktivitas sistem computer baik dari sisi akses ke user, jalannya daemon sistem, dan akses user ke sistem.
- Lakukan review log dengan mencocokan policy pada mesin firewall atau IDS
- Lakukan clock synchronization terutama jika mempunyai banyak server di banyak tempat untuk menghindari kesalahan prosedur pada sistem.

8. **Access control,** bagian ini hendaknya membuat aturan tentang akses ke informasi, fasilitas proses informasi dan business process.
    - Membuat aturan tentang akses ke sistem informasi
    - Membuat baku tentang format persetujuan, penolakan dan administrasi
    - User Registrasi, perlu dibuat untuk mengimplementasikan prosedur registrasi, grating dan revoking access ke semya sistem dan layanan informasi
    - Buat account dengan unik untuk semua ID user
    - Buat aturan tentang pemberitahuan admin kepada user tentang permasalahan pada sistem account
    - Buat standart untuk "term and condition" dan confidentiality agreement
    - Buat standar dokumentasi untuk menyimpan semua informasi user agar mudah di restorasi
    - *Account*, apakah sebuah account dapat digunakan bersama, disaat accountnya ditolak apa yang harus dilakukan oleh user. Account yang expired seperti keluarnya pegawai / resign yang dahulu mendapatkan hak akses ke server seperti account mail, account web atau quota di server untuk menyimpan datanya harus segera dihapus setelah pegawai tersebut resmi resign dari perusahaan.
    - *Automatic Lock*, aturan yang memungkinkan penguncian sistem secara otomatis, jika terjadi misalkan penulisan password yang salah sebanyak tiga kali. Ini sangat berguna untuk user yang bisa login ke server.
    - Ganti password secara berkala (admin & user) dan dokumentasikan, Password yang baik selain terdiri dari karakter dan angka juga panjangnya, ada baiknya password diganti secara berkala misalnya 1 bulan sekali dan di dokumentasikan
    - *New accounts*, membatasi user baru dengan quota, memory dan akses beserta hak yang dimilikinya
    - Batasi ruang lingkup user dengan menerapkan quota, jam akses, hak akses instalasi di PC atau server dan sebagainya
    - *Root Security*, sistem administrasi dengan menggunakan remote sistem harus melalui jaringan yang aman, misalnya VPN, SSL, atau SSH. Dibuat aturan dimana setiap user yang akan login ke server dengan account root atau super user harus login dengan user biasa dulu baru pindah ke user root.

- Buat aturan tentang network routing control, pastikan algortima yang digunakan benar dan link ke routing dapat dipercaya, perhatikan hop routing, latency dan protocol yang digunaka

9. **Information systems acquisition, development and maintenance,** pada bagian ini akan membicarakan tentang aturan bagian dari sistem informasi, dan proses bisnis yang merupakan bagian dari kegiatan sistem yang berlangsung.
    a. **Security Requirement of information system & application,** menyangkut tentang sistem informasi secara keseluruhan
        - Membuat aturan tentang legalitas tentang asset informasi pada perubahan atau implementasi sistem yang baru.
        - Membuat aturan tentang data input pada aplikasi untuk memastikan kebenaran data tersebut
        - Membuat aturan tentang pemeriksaan ulang dan manual untuk memverifikasi dan cross checking
        - Hal ini sebagian dari penanggulangan injection pada serangan yang akan dilakukan pada sistem yang dibangun dengan memanfaatkan celah yang ada.
        - Membuat definisi untuk tanggung-jawab dan proses untuk merespon pada saat terjadi atau mendeteksi errors.
        - Memperhatikan tentang output data dengan memvalidasi untuk memastikan data yang diproses dan disimpan adalah benar
        - Gunakan metode enkripsi kriptographi tertentu untuk menjamin keamanan, integrasi dan otentikasi informasi dengan menggunakan aplikasi yang mendukungnya
    b. **Security Systems**, menjamin sistem file yang ada,
        - Membuat prosedur implementasi untuk mengontrol instalasi software
        - Minimalkan terjadinya konflik / inkompatibel antara perangkat lunak dengan sistem operasi dan perangkat keras
        - Melakukan training untuk mensosialisasikan sistem yang telah dibuat
        - Membuat prosedur tentang bagaimana perubahan yang akan dilakukan