Standar dan Manajemen Keamanan Komputer

Herny Februariyanti
Fakultas Teknologi Informasi, Universitas Stikubank Semarang
email : herny@unisbank.ac.id

Abstrak : Salah satu kunci keberhasilan pengaman sistem informasi adalah adanya visi dan komitmen dari pimpinan top manajemen. Upaya atau inisiatif pengamanan akan percuma tanpa hal ini. Dengan tidak adanya komitmen dari top manajemen, berdampak kepada investasi pengamanan data. Selain itu keberhasilan juga ditentukan seperti proses desain, implementasi, konfigurasi, dan pemakaian. Untuk itu diperlukan standar dan manajemen yang memadai agar kemanan dapat dilakukan secara memadai pula. Standar kompetensi dapat dilakukan sesuai dengan TKTI jika menggunakan standar Nasional. Standar kompetensi tidak berarti hanya kemampuan menyelesaikan suatu tugas, tetapi dilandasi pula bagaimana serta mengapa tugas itu dikerjakan. Selain itu standar ISO yang merupakan standar internasional dapat diterapkan yaitu menggunakan ISO 17799 dan ISO 27000 serta turunannya. Manajemen operasi keamanan harus memenuhi beberapa hal penting yaitu kontrol dan proteksi, monitoring dan auditing, serta pemahaman tentang *threat* dan *vulnerabilitas*.

Kata kunci : keamanan, manajemen, standar, ISO, dan kontrol

PENDAHULUAN

Permasalahan keamanan komputer selalu menarik untuk dibahas, hal ini karena perkembangan teknologi informasi yang semakin canggih dan meluas. Semakin canggih teknologi informasi ternyata terkadang tidak diikuti dengan penerapan keamanan yang memadai, sehingga ancaman keamanan selalu menjadi momok bagi penerapan sistem komputer dalam sebuah organisasi atau perusahaan.

Salah satu kunci keberhasilan pengaman sistem informasi adalah adanya visi dan komitmen dari pimpinan top manajemen. Upaya atau inisiatif pengamanan akan percuma tanpa hal ini. Dengan tidak adanya komitmen dari top manajemen, berdampak kepada investasi pengamanan data. Pengamanan data tidak dapat tumbuh demikian saja tanpa adanya usaha dan biaya. Pengamanan data elektronik membutuhkan investasi, tanpa investasi akan sia-sia upaya pengamanan data. Sayangnya hal ini sering diabaikan karena tidak adanya komitmen dari pihak manajemen untuk solusi keamanan.

Selain peran utama dari top manajemen, masih terdapat lagi masalah pengamanan sistem informasi, yaitu :

- **Kesalahan desain** terjadi pada tahap desain dimana keamanan seringkali diabaikan atau dipikirkan belakangan (*after thought*). Sebagai contoh ada sebuah sistem informasi yang menganggap bahwa sistem operasi akan aman dan juga jaringan akan aman sehingga tidak ada desain untuk pengamanan data, misalnya dengan menggunakan enkripsi.
- **Kesalahan implementasi** terjadi pada saat desain diimplementasikan menjadi sebuah aplikasi atau sistem. Sistem informasi diimplementasikan dengan menggunakan software. Sayangnya para pengembang software seringkali tidak memiliki pengetahuan mengenai keamanan sehingga aplikasi yang dikembangkan memiliki banyak lubang keamanan yang dapat dieksploitasi.
- **Kesalahan konfigurasi** terjadi pada tahap operasional. Sistem yang digunakan biasanya harus dikonfigurasi sesuai dengan kebijakan perusahaan. Selain salah

konfigurasi, ada juga permasalahan yang disebabkan karena tidak adanya kebijakan prosedural dari pemilik sistem sehingga menyulitkan bagi pengelola untuk melakukan pembatasan.

- **Kesalahan penggunaan** terjadi pada tahap operasional juga. Kadang-kadang karena sistem terlalu kompleks sementara sumber daya yang disediakan sangat terbatas maka dimungkinkan adanya kesalahan dalam penggunaan.

Kesalahan-kesalahan di atas dapat menimbulkan celah lubang keamanan. Celah ini belum tentu menimbulkan masalah, sebab bisa saja memang celah ada akan tetapi tidak terjadi eksploitasi. Namun celah ini merupakan sebuah resiko yang harus dikendalikan dalam sebuah manajemen keamanan.

STANDAR KEAMANAN KOMPUTER

1. Standart Kompetensi Keamanan menurut TKTI.

Standar kompetensi diartikan sebagai suatu ukuran atau patokan tentang pengetahuan, keterampilan, dan sikap kerja yang harus dimiliki oleh seseorang untuk mengerjakan suatu pekerjaan atau tugas sesuai dengan unjuk kerja yang dipersyaratkan oleh Tim Koordinasi Telematika Indonesia (TKTI, 2004). Standar kompetensi tidak berarti hanya kemampuan menyelesaikan suatu tugas, tetapi dilandasi pula bagaimana serta mengapa tugas itu dikerjakan.

Berdasarkan jenis kelompok Sumber daya manusia (SDM) pada teknologi informasi dan komunikasi (*information and communication technology* - ICT) berikut kompetensinya, yang berhubungan dengan keamanan dan pemeliharaan komputer, adalah :

a. unit kompetensi no. 16.

- Judul Unit : Mendeskripsikan Kewaspadaan Terhadap Keamanan Informasi
- Uraian Unit : Unit kompetensi ini berhubungan dengan pemahaman prinsip keamanan informasi guna meningkatkan kewaspadaan atas keamanan informasi. Berupa :
  - Kaidah Umum Kemanan Informasi
  - Pemilihan dan Penggunaan Password
  - Identifikasi Resiko Keamanan Atas Penggunaan Internet
  - Pengelolaan Data/Informasi Secara Aman

b. unit kompetensi no. 17

- Judul Unit : Mempergunakan Piranti lunak Anti Virus
- Uraian Unit : Unit kompetensi ini berkaitan dengan penggunaan piranti lunak anti virus yang umum digunakan dengan tujuan agar dapat melindungi komputer dari berbagai jenis virus standard yang dapat menyebar di komputer kita. Berupa :
  - Mengidentifikasi jenis virus
  - Mempersiapkan Piranti lunak Anti Virus dijalankan.
  - Mengoperasikan piranti lunak anti virus
  - Melakukan pencegahan

c. unit kompetensi no. 20

- Judul Unit : Melakukan penanganan awal (*Troubleshooting*) atas masalah pada PC
- Uraian Unit : Unit kompetensi ini berhubungan dengan pemahaman tentang cara kerja komputer (PC) dan penanganannya apabila komputer tersebut tidak bisa bekerja. Berupa :
  - Cara Kerja Komputer
  - Instalasi Komponen Komputer
  - Penggunaan Alat Bantu Deteksi Masalah
  - Diagnosa Masalah dan Penanganan Masalah (*Troubleshoot*)

d. unit kompetensi no. 21

- Judul Unit : Mengoperasikan utilitas dasar untuk Backup, Restore, Data Recovery
- Uraian Unit : Unit kompetensi ini berkaitan dengan langkah-langkah dasar dalam melakukan pengamanan terhadap data-data elektronik dalam komputer yang dimiliki. Berupa :
  - Mengidentifikasi dan mendeskripsikan aspek-aspek pengamanan data
  - Melindungi data di komputer dari gangguan
  - Melakukan Data Revovery

e. unit kompetensi no. 24

- Judul Unit : Mengimplementasikan sistem keamanan dan keselamatan pada pengoperasian komputer
- Uraian Unit : Unit kompetensi ini berhubungan dengan penguasaan konsep dasar keamanan sistem komputer yang harus dibuat untuk menjamin kemanan sistem komputer yang digunakan. Berupa :
  - Mengidentifikasi Ancaman Keamanan
  - Standar Pengamanan Komputer Dasar

2. Manajemen Keamanan sesuai ISO 17799

ISO (*International Standart Organisation*) atau Organiasasi standar Internasioanal merupakan badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standar nasional setiap negara. ISO menetapkan standar-standar industrial dan komersial dunia.

Standard ISO 17799 adalah merupakan suatu standar sistem manajemen keamanan informasi (*Informasi Secuity Management system*) yang telah disempurnakan dan diterapkan untuk digunakan oleh peruasahaan-perusahaan di dalam mengamankan data atau informasi yang dimilikinya. Dengan adanya standar ISO 17799 maka kita akan dapat mengukur apakah sistem keamanan informasi yang kita terapkan sudah efektif dan memberikan jaminan keamanan terhadap konsumen.

Sebelum diperkenalkan ISO 17799, pada tahun 1995, *Britania Standard Institut* (BSI) meluncurkan standard pertama mengenai manajemen informasi di seluruh dunia, yaitu "B 7799", Bagian Pertama: Kode Praktek untuk Manajemen Keamanan Informasi, yang didasarkan pada Infrastruktur pokok B 7799. Kemudian pada tanggal 1 Desember, 2000, ISO 17799 standard mengenai manajemen informasi baru diterbitkan.

Pemakaian standar ISO 17799 meliputi kebutuhan akan hal-hal sebagai berikut :

- Dokumen kebijakan keamanan informasi
- Adanya Tanggung jawab keamanan informasi
- Adanya program pendidikan dan pelatihan keamanan informasi untuk semua pemakai (*user*)
- Mengembangkan suatu sistem untuk pelaporan peristiwa keamanan
- Memperkenalkan teknik pengendalian virus
- Mengembangkan suatu rencana kesinambungan bisnis
- Mengendalikan pengkopian perangkat lunak kepemilikan
- Surat pengantar arsip organisatoris untuk mengikuti kebutuhan perlindungan data,
- Dan menetapkan prosedur dalam mentaati kebijakan keamanan.

Sedangkan Kebijakan pengendalian atau kontrol menurut standar ISO 17799 meliputi : kebijakan keamanan, organisasi keamanan, penggolongan dan pengendalian asset, keamanan personil, keamanan phisik dan kendali lingkungan, pengembangan dan

manajemen jaringan komputer, sistem akses kendali, pemeliharaan sistem, perencanaan kesinambungan bisnis, dan pemenuhan.

Guna meminimalkan resiko ancaman keamanan yang merugikan bisnis, maka masalah tersebut harus ditangani dengan menggunakan suatu tindakan pencegahan (*preventive action*) tanpa harus menunggu dalam keadaan darurat dalam melakukan tindakan keamanan. Dalam rangka pro aktif terhadap kebutuhan keamanan, arsitektur keamanan meliputi tiga unsur pokok:

- Kebijakan perusahaan yaitu keterlibatan manajemen dalam alokasi sumber daya dan suatu visi yang strategis dan permasalahan global dalam keamanan,
- Instrumen teknologi,
- Perilaku individu (pelatihan karyawan, dan adanya proses komunikasi).

Dalam standar ISO 17799, sistem manajemen keamanan informasi yang efektif dan efisien akan memberikan petunjuk bagi perusahaan atau organisasi untuk:

- Secara konstan memperbaharui (*update*) atas adanya ancaman baru serta mengambil tindakan dengan pertimbangan yang sistematis.
- Melakukan penanganan kecelakaan dan kerugian dengan tindakan pencegahan dan peningkatan keamanan sistem yan berkelanjutan.
- Mengetahui ketika kebijakan dan prosedur tidak cukup mampu diterapkan dalam usaha pencegahan ancaman keamanan.
- Menerapkan kebijakan dan prosedur tentang pentingnya managemen keamanan, dengan mengikuti " prosedur praktek terbaik" dan manajemen resiko yang baik.

Dengan mengenali nilai manajemen keamanan informasi yang strategis ini, maka dapat ditawarkan suatu rencana inovasi sertifikasi, berdasar pada rencana sertifikasi BS7799-2:1999 dan petunjuk ISO17799. Dimana isi dari ISO-17799 meliputi : 10 Ketentuan Pengendalian (*control clauses*), 36 Tujuan Pengendalian (*control objectives*), dan, 127 Kendali (*controls*). Kendali / Kontrol tersebut diuraikan pada tingkat tinggi, tanpa memasukkan masalah teknologi secara detail, dalam rangka membiarkan perusahaan / organisasi masing-masing secara total bebas untuk memilih kendali itu yang terdekat ke situasi cultural/technological dan kebutuhan sendiri.

3. Standar Pengelolaan Keamanan Informasi sesuai ISO 27001 dan ISO 27002

Serial ISO 27000 saat ini memainkan peranan yang penting dalam dukungannya terhadap perusahaan untuk dapat menerapkan konsep keamanan informasi dalam organisasi serta keseluruhan proses bisnis. Proses dan manusia adalah dua aspek yang tidak kalah pentingnya.

Keamanan Informasi

"Keamanan teknologi informasi" atau IT Security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari tentunya, gangguan - gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan. Berbeda dengan "keamanan informasi" yang fokusnya justru pada data dan informasi, yang dalam hal ini tentunya data serta informasi milik perusahaan Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan. Berdasarkan penjelasan di atas, 'kemananan teknologi informasi' merupakan bagian dari keseluruhan aspek 'keamanan informasi'. Karena teknologi informasi merupakan salah satu alat atau tool penting yang digunakan untuk mengamankan akses serta penggunaan dari data dan informasi perusahaan. Dari pemahaman ini pula, kita akan mengetahui

bahwa teknologi informasi bukanlah satu-satunya aspek yang memungkinkan terwujudnya konsep keamanan informasi di perusahaan.

Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (*Information Security Management System* – ISMS) merupakan sebuah kesatuan system yang disusun berdasarkan pendekatan resiko bisnis, untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan. Dan sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut:

- Struktur organisasi, biasanya berupa keberadaan fungsi-fungsi atau jabatan organisasi yang terkait dengan keamanan informasi. Misalnya; Chief Security Officer dan beberapa lainnya.
- Kebijakan keamanan. Contoh kebijakan keamanan ini misalnya adalah sebagai berikut: Semua kejadian pelanggaran keamanan dan setiap kelemahan sistem informasi harus segera dilaporkan dan administrator harus segera mengambil langkah-langkah keamanan yang dianggap perlu. Akses terhadap sumber daya pada jaringan harus dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak. Akses terhadap sistem komputasi dan informasi serta periferalnya harus dibatasi dan koneksi ke jaringan, termasuk logon pengguna, harus dikelola secara benar untuk menjamin bahwa hanya orang/ peralatan yang diotorisasi yang dapat terkoneksi ke jaringan.
- Prosedur dan proses. Yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan. Misalnya prosedur permohonan ijin akses aplikasi, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya.
- Tanggung jawab. Yang dimaksud dengan tanggung jawab atau responsibility di sini adalah tercerminnya konsep dan aspek aspek keamanan informasi perusahaan di dalam job description setiap jabatan dalam perusahaan. Begitu pula dengan adanya program-program pelatihan serta pembinaan tanggung jawab keamaan informasi perusahaan untuk staf dan karyawannya.

Serial ISO 27000

ISO mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, yaitu pada serial ISO 27000. ISO 27000 berisi dokumen definisi-definisi keamanan informasi Adapun beberapa standar di seri ISO ini adalah sebagai berikut:

- ISO 27001—berisi aspek-aspek pendukung realisasi serta implementasi sistem manajemen keamanan informasi perusahaan
- ISO 27002—terkait dengan dokumen ISO 27001, namun dalam dokumen ini terdapat panduan praktis pelaksanaan dan implementasi sistem manajemen keamanan informasi perusahaan.
- ISO 27003—panduan implementasi sistem manajemen keamanan informasi perusahaan.
- ISO 27004—dokumen yang berisi matriks dan metode pengukuran keberhasilan implementasi sistem manajemen keamanan informasi.
- ISO 27005—dokumen panduan pelaksanaan manajemen risiko.
- ISO 27006—dokumen panduan untuk sertifi kasi sistem manajemen keamanan informasi perusahaan.
- ISO 27007—dokumen panduan audit sistem manajemen keamanan informasi perusahaan.

ISO 27001

ISO 27001 merupakan dokumen standar sistem manajemen keamanan

informasi atau *Information Security Managemen System*–ISMS yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka mengimplementasikan konsep-konsep keamanan informasi di perusahaan. Secara umum ada 11 aspek atau yang biasa disebut sebagai *control*, yang harus ada dalam setiap perusahaan dalam usahanya mengimplementasikan konsep keamanan informasi. Control dalam hal ini adalah hal-hal, bisa berupa proses, prosedur, kebijakan maupun *tool* yang digunakan sebagai alat pencegahan terjadinya sesuatu yang tidak dikehendaki oleh adanya konsep keamanan informasi, seperti akses terlarang terhadap data atau informasi rahasia perusahaan. Adapun ke-11 control tersebut adalah sebagai berikut: *Security policy, organization of information security, Asset management, Human resources security, Physical and environmental security, Communications and operations management, Access control, Information system acquisition, development, and maintenance, Information security incident management, Business continuity management, Compliance.*

Personal Keamanan Teknologi Informasi

Menurut *National Institute of Standards and Technology* (NIST) kebutuhan sumberdaya personel keamanan teknologi informasi (TI) yang ideal, mestinya disertai dengan tingkat dukungan minimal (*minimum level of support*) dalam perencanaan sebuah organiasasi. Perencanaan ini khususnya ditujukan pada lembaga Pemerintahan dan organisasi atau instansi sejenis yang bersifat memberikan jasa kepada pihak lain. Minimnya anggaran yang tersedia bagi beberapa lembaga, membuat mereka harus membuat keputusan dengan pertimbangan biaya yang efektif dan alokasi sumberdaya yang efisien. Dalam perencanaan ini susunan kepegawaian (staff) bidang keamanan TI pada umumnya dibagi menjadi:

1. *Director of Program Operations* (CIO atau Kepala Departemen/Lembaga)
2. *Special Assistant to Director* (*Information Security Officer*)
3. Supervisor
4. User

FUNGSI KEAMANAN DALAM ORGANISASI

Setiap personal (staff) keamanan TI harus mengerti dan mengimplementasi kontrol manajemen, operasional dan teknikal. Implementasi penuh terhadap semua jenis kontrol membutuhkan staff keamanan Ti dengan berbagai keahlian. Pada suatu saat tim keamanan tersebut bias bertindak sebagai spesialis pengadaan barang yang meninjau sebuah spefisikasi dari system upgrade atau kemudian bertindak sebagai pengajar dalam kelas IT security awareness.

Dalam kenyataannya diberbagai organisasi dengan beragam tugas dari tim keamanan TI sering dihadapkan pada kekurangan sumberdaya atau prioritas beban kerja untuk menyelesaikan hanya tugas-tugas yang penting. Fungsi-fungsi yang dibahas dibawah ini mengandung jumlah staff yang dibutuhkan untuk menyelesaikan fungsi tersebut dalam tingkat yang minimal. Tingkat ini dihitung dalam bentuk prosentasi dari 1 staff per tahun.

a. Audit.

Auditor bertanggungjawab dalam memeriksa sistem untuk melihat apakah sistem tersebut telah memenuhi kebutuhan keamanan TI. termasuk sistem dan kebijakan organisasi, dan apakah kontrol keamanan TI telah dijalankan dengan benar.

b. Physical Security

Pada banyak organisasi, bagian keamanan fisik ini pada umumnya adalah staff keamanan berupa satuan pengamanan (satpam). Bagian kemanan fisik biasanya bertanggungjawab untuk mengembangkan dan menjalankan kontrol keamanan fisik yang baik, dengan konsultasi dengan manajemen keamanan komputer. program dan manajer fungsional, dan yang pihak lain yang diperlukan.

c. Disaster Recovery/Contingency Planning

Staff keamanan TI harus memiliki disaster recovery/contingency planning team. Tim ini bertanggungjawab pada aktifitas contingency planning organisasi tersebut dan bekerjasama dengan dengan bagian keamanan fisik, telekomunikasi, IRM, pengadaan barang dan pegawai lainnya.

d. Pengadaan (*Procurement*)

Bagian pengadaan bertanggungjawab untuk memastikan pengadaan barang dalam organisasi telah ditinjau oleh petugas yang berwenang.

e. Pelatihan

Pelatihan mengenai keamanan TI termasuk dalam kebutuhan keamanan TI. Staff keamanan TI memiliki salah satu tanggung jawab utama untuk memberikan pelatihan kepada user, operator, dan manajer mengenai keamanan komputer.

f. Sumberdaya Manusia (Personalia)

Bagian personalia dan staff keamanan TI harus bekerjasama dalam lekaukan investigasi terhadap latar belakang dan, prosedur pemberhentian kerja dari seorang pegawai yang hendak mengundurkan diri.

g. Risk Management/Planning

Beberapa organisasi memiliki staff yang bertugas mempelajari berbagai tipe resiko yang mungkin dihadapi oleh organisasi. Staff keamanan TI harus mengembangkan proses untuk mengenali resiko yang ada dalam siklus hidup organisasi. Ketika sebuah kelemahan (vulnerabilities) terdeteksi, tim keamanan harus menganalisa resiko dan jumlah sumberdaya yang dibutuhkan untuk menurunkan resiko (mitigate the risk).

h. Building Operations

Bagian pemeliharaan gedung bertanggungjawab dalam memastikan bahwa setiap fasilitas keamanan gedung, daya listrik dan kontrol lingkungan gedung, aman digunakan selama masa operasional organisasi.

i. System Management/System Administrators

Pegawai ini adalah manajer dan teknisi yang merancang dan mengoperasikan suatu sistem, jaringan komputer dan LAN dari organisasi. Mereka bertanggungjawab dalam mengimplementasikan kemanan teknis dan harus paham terhadap teknologi pengamanan TI yang berhubungan dengan sistem mereka. Mereka juga perlu memastikan kontinuitas dari layanan mereka dalam memenuhi kebutuhan manajer fungsional, serta menganalisa kelemahan yang ada pada sistem.

j. Telekomunikasi

Bagian telekomunikasi bertanggungjawab untuk menyediakan layanan telekomunikasi termasuk telekomunikasi suara, data, video dan layanan faks.

k. Help Desk

Apakah bagian Help Desk menangani atau tidak menangani setiap insiden, ia harus dapat mengenali gangguan keamanan dan meneruskan panggilan tersebut kepada pihak yang berwenang dalam organisasi untuk direspon. Tim keamanan TI harus bekerjasama dengan manajemen help desk untuk memastikan prosedur yang ada telah dijalankan dalam menangani insiden yang berhubungan dengan keamanan TI.

l. Maintenance of Security Program

Program keamanan membutuhkan beberapa aktifitas tambahan yang tidak tercantum dalam fungsi-fungsi diatas. Untuk setiap area fungsi harus memiliki dokumen penuntun bagi staff dan tim keamanan TI. Dokumen tersebut harus diteliti, ditulis, ditinjau dan diawasi secara berkala.

MANAJEMEN OPERASI KEAMANAN

Dalam penggunaan teknologi infromasi di setiap institusi, terutama yang mengutamakan teknologi informasi dalam proses bisnisnya membutuhkan suatu operasional yang optimal untuk dapat mendukung bisnis yang berjalan. Bila berbicara tentang operasional, maka banyak hal yang bisa dilibatkan mulai dari *hardware*,

software, prosedur dan sumber daya manusianya sendiri untuk bisa melaksanakan operasional itu. Ketergantungan dari setiap komponen di atas sangatlah menentukan keberhasilan operasional yang dilakukan tetapi dengan keberhasilan operasional dengan teknologi yang canggih pun tanpa melibatkan faktor keamanan semuanya menjadi kurang berarti karena informasi atau data apapun yang dihasilkan dari teknologi tanpa adanya keamanan bisa menjadi bencana bila tidak memperhatikan *confidenciality*, *integrity* dan *avaibility* pada umumnya dan keamanan pada khususnya sehingga setiap informasi yang dimiliki benar-benar diperlakukan sebagai asset yang berharga bagi institusi.

Untuk menjamin keamanan operasional tidak hanya bicara teknologi pelindungnya, tetapi kebijakan yang jelas dalam melakukan kemanan operasional adalah sangat penting untuk dapat dijalankan dengan baik karena ancaman yang paling tinggi pada prakteknya adalah dari sumber daya internal sendiri. Hal ini adalah ancaman yang sebenarnya sangat mengancam dan sulit untuk diperkirakan, karena internal sumber daya sudah ada di dalam sistem itu sendiri. Dalam rangka meminimalisasi ancaman ini maka kebijakan untuk keamana operasional harus dibuat dengan sedetail mungkin memperkirakan hal-hal yang dapat menjadi ancaman, dan melakukan prosedur – prosedur keamanan dengan konsekwen. Jadi tanpa kebijakan dan prosedur yang baik maka tidak hanya ancaman dari luar yang menakutkan tetapi juga lebih menakutkan ancaman dari dalam. Untuk itu setiap divisi teknoogi informasi harus punya kebijakan untuk *corporate user* dalam menggunakan sumber daya teknologi informasi yang dipunyai.

Dalam pembahasan ini akan dijelasakan setidaknya terdapat 3 hal besar yang harus dapat dipahami :

1. ***Control and Protection.*** Berisi pemahaman tentang pengaturan dan proteksi dalam kegiatan operasional untuk dapat mencapai tingkat keamanan operasional yang optimal ada bererapa hal yang harus diperhatikan diantaranya adalah *preventive control*, *corrective control detective control*, *deterrent control, application control*, *transaction control* dan *separation and rotation of duties* lebih menekankan kepada *confidenciality* (kerahasiaan) dan *integrity* atau keutuhan data. Semua hal di atas lebih memfokuskan juga pada prosedur pengawasan yang optimal dalam melakukan berbagai hal mulai dari pencegahan hingga rotasi tugas yang baik dan bila tidak dilakukan dengan benar akan menjadi ancaman dan membuka lebar pintu keamanan.
2. ***Monitoring and Auditing***. Setelah dilakukan pengaturan dan proteksi yang baik maka tidak bisa hanya berhenti untuk bisa melakukan proteksi tetapi tetap diperlukan monitoring and auditing untuk bisa mengetahui dan menjamin sejauh mana keamanan yang sudah dicapai, faktor yang harus diperhatikan adalah *Change management*, *Escalation management*, *Record retention*, *Due dilligince*, dan *Logging monitoring*. Dengan melakukan hal-hal diatas yang lebih bersifat prosedur maka pengawasan keamanan dapat lebih ditingkatkan.
3. ***Threat and Vulnerabilities.*** Berisi pemahaman tentang jenis ancaman dan kelemahan yang dapat mengancam operasional keamanan yang sudah dilakukan. Untuk *threat* dan *vulnerability* beberapa hal yang akan dibahas adalah *Accidental Loss*, *Inappropriate Activities*, *Illegal computer operations*, *Account maintenance*, *Data Scavenging Attacks*, *IPL/rebooting*, dan *Network highjacking*.

KESIMPULAN

Penerapan sistem keamanan dalam sebuah organisasi yang ideal tentunya harus memenuhi persyaratan standarisasi sesuai dengan ketentuan yang berlaku pada standar sistem keamanan baik itu TKTI dan ISO. Namun begitu mengingat keterbatasan sumber daya pada beberapa organisasi atau perusahaan kecil dan menengah, maka standar tersebut beberapa bagian diantaranya dapat digabungkan. Namun begitu prinsip keamanan harus tetap memenuhi aspek-aspek yang menjadi persyaratan keamanan yaitu *confidenciality*, *integrity* dan *avaibility*.

Untuk mencapai aspek tersebut maka perlu diperhatikan beberapa hal yang penting yaitu adanya kontrol dan proteksi, monitoring dan auditing, serta pemahaman tentang *threat* dan *vulnerabilitas*.

DAFTAR PUSTAKA

1. Depkominfo, 2006, "*Pedoman Praktis manajemen Keamanan Informasi untuk Pimpinan Organisasi, 10 Rekomendasi Terbaik Manajemen Keamanan Informasi* ", Direktorat Sistem Informasi, Perangkat Lunak Dan Konten Direktorat Jenderal Aplikasi Telematika Departemen Komunikasi Dan Informatika
2. Budi Raharjo, 2005, "*Keamanan Sistem Informasi Berbasis Internet*", PT Insan Infonesia - Bandung & PT INDOCISC – Jakarta Internet
3. Gary Stoneburner, dkk, 2004, "*Computer Security:Engineering Principles For Information Technology Security (Baseline for Achieving Security), Revisian A*", NIST.
4. http://www.wikipedia.org
5. http://amutiara.files.wordpress.com/2007/01/sp800-86.pdf
6. IEEE 802.11Working Group. http://grouper.ieee.org/groups/802/11/index.html.
7. NIST Special Pub. 800-86:, 2005, "*Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (Draft)* ", http://csrc.nist.gov/publications/drafts/Draft-SP800-86.pdf.