ISO 17799: Standar Sistem Manajemen Keamanan Informasi

Melwin Syafrizal

STMIK AMIKOM Yogyakarta

e-mail : melwin@amikom.ac.id

ABSTRAK

Informasi adalah salah satu asset penting yang sangat berharga bagi kelangsungan hidup suatu organisasi/bisnis, pertahanan keamanan dan keutuhan negara, kepercayaan publik atau konsumen, sehingga harus dijaga ketersediaan, ketepatan dan keutuhan informasinya. . Informasi dapat disajikan dalam berbagai format seperti: teks, gambar, audio, maupun video. Manajemen pengelolaan informasi menjadi penting ketika terkait dengan kredibilitas dan kelangsungan hidup orang banyak. Tujuan manajemen informasi adalah untuk melindungi kerahasiaan, integritas dan ketersediaan informasi tersebut.

I. Pendahuluan

Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti: perusahaan export-import, tranportasi, lembaga pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting).

Informasi atau data adalah aset bagi perusahaan. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan return on investment dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan.

Bagaimana data atau informasi tersebut dikelola, dipelihara dan diekspose, melatarbelakangi disusunnya ISO 17799, standar untuk sistem manajemen keamanan informasi.

Penyusunan standar ini berawal pada tahun 1995, dimana sekelompok perusahaan besar seperti BOC, BT, Marks & Spencer, Midland Bank, Nationwide Building Society, Shell dan Unilever bekerja sama untuk membuat suatu standar yang dinamakan BS (British Standard) 7799.

BS 7799 Part 1: the Code of Practice for Information Security Management. Februari 1998 BS 7799 Part 2: The Specification for Information Security Management Systems (ISMS) menyusul diterbitkan. Desember 2000 ISO (International Organization of Standardization) dan IEC (International Electro-Technical Commission) mengadopsi BS 7799 Part 1 dan menerbitkannya sebagai standar ISO/IEC 17799:2000 yang diakui secara internasional.

II. Pembahasan

2.1.Apa itu Keamanan Informasi?

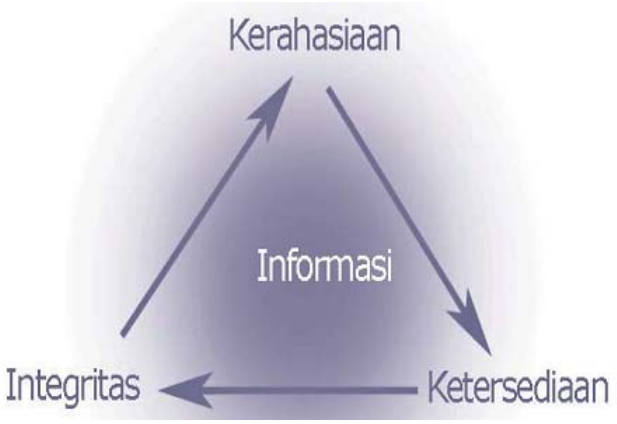
Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

1. *Confidentiality (kerahasiaan)* aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

2. *Integrity (integritas)* aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.

3. *Availability (ketersediaan)* aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

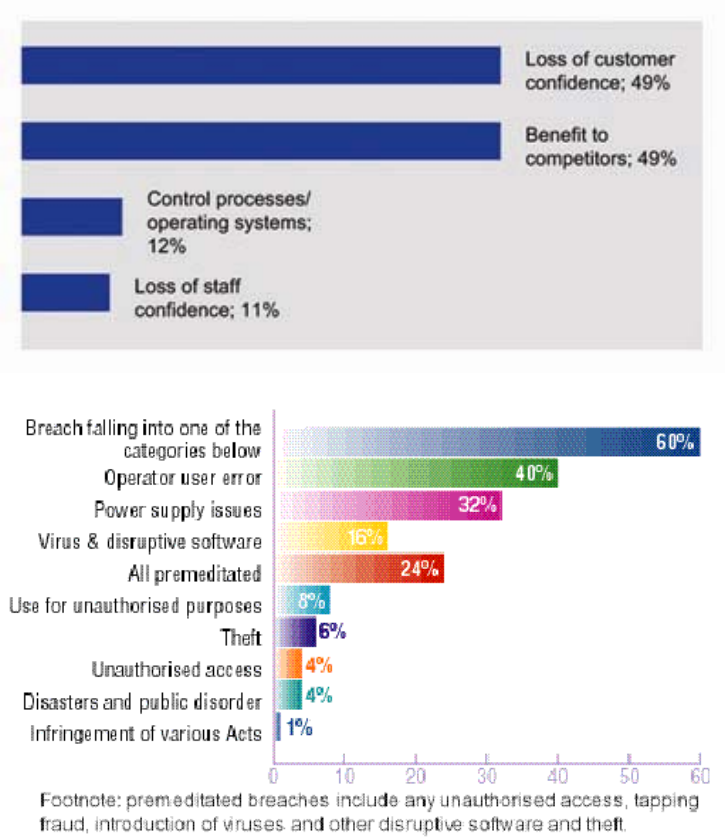


Gambar 2.1 Elemen-elemen keamanan informasi

2.2. Mengapa diperlukan keamanan informasi?

Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar.

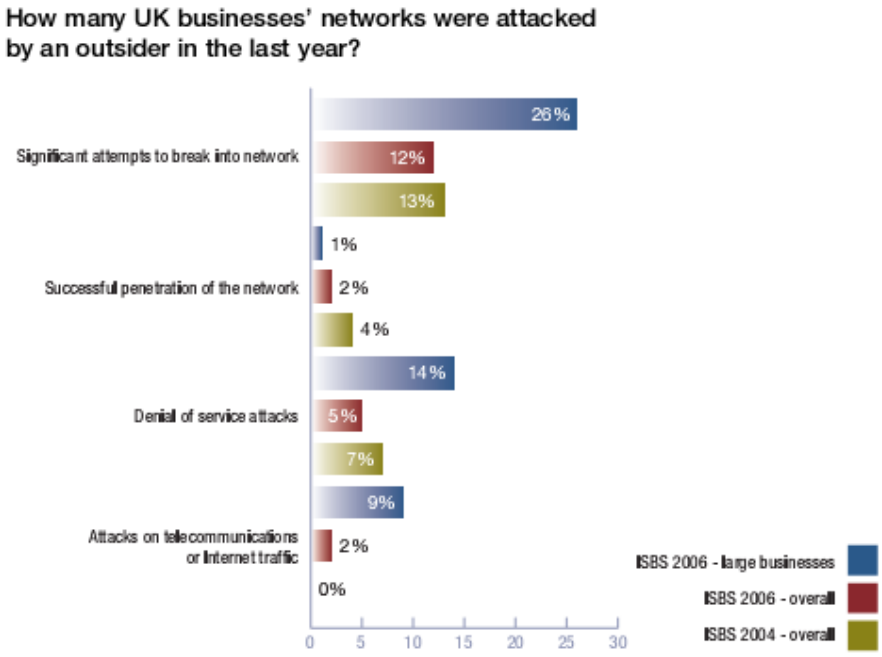
Hasil survey ISBS (Information Security Breaches Survey) pada tahun 2000 menunjukkan bahwa sebagian besar data atau informasi tidak cukup terpelihara/terlindungi sehingga beralasan kerawanan. Hasil survey yang terkait dengan hal ini dapat dilihat dalam gambar berikut:



Gambar 2.2 Grafik persentase ancaman keamanan sistem informasi

Survey tersebut juga menunjukkan bahwa 60% organisasi mengalami serangan atau kerusakan data karena kelemahan dalam sistem keamanan. Kegagalan sistem keamanan lebih banyak disebabkan oleh faktor internal dibandingkan dengan faktor eksternal. Faktor internal ini diantaranya kesalahan dalam pengoperasian sistem (40%) dan diskontinuitas power supply (32%).

Hasil survey ISBS tahun 2004-2006 menunjukkan bahwa terdapat banyak jaringan bisnis di Inggris (UK) telah mendapatkan serangan dari luar.



Gambar 2.3 UK business network attack

Langkah-langkah untuk memastikan bahwa sistem benar-benar mampu menjamin keamanan data dan informasi dapat dilakukan dengan menerapkan kunci-kunci pengendalian yang teridentifikasi dalam standar ini.

2.3. Apa Isi dari ISO-17799 ?

Isi ISO 17799, meliputi :

- 10 control clauses (10 pasal pengamatan)
- 36 control objectives (36 objek/sasaran pengamanan)
- 127 controls securiy (127 pengawasan keamanan)

10 control clouse tersebut, antara lain:

- Security Policy
- System Access Control
- Communication & Operations Management
- System Development and Maintenance
- Physical and Environmental Security

- Compliance
- Personnel Security
- Security Organization (Information Security)
- Asset Classification and Control
- Business Continuity Management (BCM)

Security Policy *(kebijakan keamanan)***,** mengarahkan visi dan misi manajemen agar kontinuitas bisnis dapat dipertahankan dengan mengamankan dan menjaga integritas/keutuhan informasi-informasi krusial yang dimiliki oleh perusahaan.

Security Policy sangat diperlukan mengingat banyak ditemuinya masalah-masalah non teknis salah satunya penggunaan *password* oleh lebih dari satu orang. Hal ini menunjukan tidak adanya kepatuhan dalam menerapkan sistem keamanan informasi. Harus dilakukan inventarisasi data-data perusahaan. Selanjutnya dibuat peraturan yang melibatkan semua departemen sehingga peraturan yang dibuat dapat diterima oleh semua pihak. Setelah itu rancangan peraturan tersebut diajukan ke pihak direksi. Setelah disetujui, peraturan tersebut dapat diterapkan.

Security Policy meliputi berbagai aspek, yaitu :

a. Information security infrastructure

b. Information security policy

System Access Control *(sistem kontrol akses)***,** mengendalikan/membatasi akses user terhadap informasi-informasi yang telah diatur kewenangannya, termasuk pengendalian secara mobile-computing ataupun tele-networking. Mengontrol tata cara akses terhadap informasi dan sumber daya yang ada meliputi berbagai aspek, yaitu :

a. Access control.

b. User Access Management.

c. User Responsibilities.

d. Network Access Control

e. Operation System access Control

f. Application Access Control.

g. Monitor system Access and use.

h. Mobile Computing and Telenetworking.

Communication and Operations Management *(manajemen komunikasi dan operasi)***,** menyediakan perlindungan terhadap infrastruktur sistem informasi melalui perawatan dan pemeriksaan berkala, serta memastikan ketersediaan panduan sistem yang terdokumentasi dan

dikomunikasikan guna menghindari kesalahan operasional. Pengaturan tentang alur komunikasi dan operasi yang terjadi meliputi berbagai aspek, yaitu :

a. Operational procedures and reponsibilities.

b. System Planning and acceptance.

c. Protection against malicious software.

d. Housekeeping

e. Network Management.

f. Media handling and security.

g. Exchange of Information and software.

System Development and Maintenance *(pengembangan sistem dan pemeliharaan)***,** memastikan bahwa sistem operasi maupun aplikasi yang baru diimplementasikan mampu bersinergi melalui verifikasi/validasi terlebih dahulu sebelum diluncurkan ke live environment.

Penelitian untuk pengembangan dan perawatan sistem yang ada meliputi berbagai aspek, yaitu :

a. Security requirements of system.

b. Security in application system.

c. Cryptographic control

d. Security of system files

e. Security in development and support process.

Physical and Environmental Security *(keamanan fisik dan lingkungan)***,** membahas keamanan dari segi fisik dan lingkungan jaringan, untuk mencegah kehilangan/ kerusakan data yang diakibatkan oleh lingkungan, termasuk bencana alam dan pencurian data dalam media penyimpanan atau fasilitas informasi yang lain. Aspek yang dibahas antara lain:

a. Secure Areas

b. Equipment security

c. General Control

Compliance *(penyesuaian)***,** memastikan implementasi kebijakan-kebijakan keamanan selaras dengan peraturan dan perundangan yang berlaku, termasuk persyaratan kontraktual melalui audit sistem secara berkala. Kepatuhan yang mengarah kepada pembentukan prosedur dan aturan – aturan sesuai dengan hukum yang berlaku meliputi berbagai aspek, yaitu :

a. Compliance with legal requirements

b. Reviews of security policy and technical comliance.

c. System audit and consideration

Personnel Security (*keamanan perorangan)***,** mengatur tentang pengurangan resiko dari penyalahgunaan fungsi penggunaan atau wewenang akibat kesalahan manusia (human error), sehingga mampu mengurangi human error dan manipulasi data dalam pengoperasian sistem serta aplikasi oleh user, melalui pelatihan-pelatihan mengenai security awareness agar setiap user mampu menjaga keamanan informasi dan data dalam lingkup kerja masing-masing.

Personnel Security meliputi berbagai aspek, yaitu :

a. Security in Job Definition and Resourcing.

b. User Training.

c. Responding to Security Incidens and Malfunction.

Security Organization *(organisasi keamanan)***,** mengatur tentang keamanan secara global pada suatu organisasi atau instansi, mengatur dan menjaga integritas sistem informasi internal terhadap keperluan pihak eksternal termasuk pengendalian terhadap pengolahan informasi yang dilakukan oleh pihak ketiga (outsourcing). Aspek yang terlingkupi, yaitu :

a. Security of third party access

b. Outsourcing

Asset Classification and Control *(klasifikasi dan kontrol aset)***,** memberikan perlindungan terhadap aset perusahaan dan aset informasi berdasarkan level proteksi yang ditentukan. Membahas tentang penjagaan aset yang ada meliputi berbagai aspek, diantaranya :

a. Accountability for Assets.

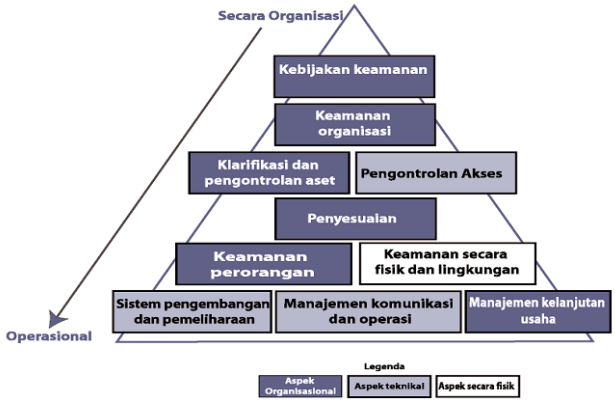
b. Information Classification.

Business Continuity Management *(manajemen kelanjutan usaha)***,** siap menghadapi resiko yang akan ditemui didalam aktivitas lingkungan bisnis yang bisa mengakibatkan ”major failure” atau resiko kegagalan yang utama ataupun ”disaster” atau kejadian buruk yang tak terduga, sehingga diperlukan pengaturan dan manajemen untuk kelangsungan proses bisnis, dengan mempertimbangkan:

a. Aspects of business continuity management

Membangun dan menjaga keamanan sistem manajemen informasi akan terasa jauh lebih mudah dan sederhana dibandingkan dengan memperbaiki sistem yang telah terdisintegrasi. Penerapan standar ISO 17799 akan memberikan benefit yang lebih nyata bagi organisasi bila didukung oleh kerangka kerja manajemen yang baik dan terstruktur serta pengukuran kinerja sistem keamanan informasi, sehingga sistem informasi akan bekerja lebih efektif dan efisien.

36 objek pengamatan/pengawasan keamanan merupakan uraian dari aspek 10 control clouse tersebut.



Gambar 2.4 Struktur dari kesepuluh wilayah standar (10 control clouse)

2.4. Aset dan aspek yang dinilai dalam ISO 17799

- Information assets (aset informasi),
- Software assets (aset perangkat lunak yang dimiliki),
- Physical assets (aset fisik) dan
- Services (pelayanan).

III.Penutup

Apa itu ISO 17799?

- ISO 17799 merupakan suatu struktur dan rekomendasi pedoman yang diakui secara internasional untuk keamanan informasi.
- Suatu proses keamanan informasi yang menyeluruh yang dapat diusahakan atau di implementasikan bagi perusahaan agar memperoleh manfaat keamanan yang diinginkan.
- Proses evaluasi, implementasi, pemeliharaan dan pengaturan keamanan informasi yang singkat.
- Upaya penggunaan oleh konsorsium perusahaan untuk memenuhi kebutuhan industri.
- ISO 17799 merupakan proses yang seimbang antara fisik, keamanan secara teknikal dan prosedur, serta keamanan pribadi.

ISO-17799 bukan merupakan:

- Sebuah aturan atau ketetapan yang dikeluarkan pemerintah

- Sebuah standard teknis atau standard yang berdasarkan pada orientasi produk/teknologi.

- Sebuah metodologi evaluasi perlengkapan (alat) seperti kriteria umum (CC/ISO 15408), yang disepakati untuk fungsi tertentu atau jaminan yang terdapat pada peralatan yang diproduksi khusus.

- Bagian "General Accepted System Security Principles" atau "GASSP", yang merupakan bagian dari kumpulan penerapan sistem keamanan yang terbaik.

- Bagian dari 5 point yang terdapat di "Guidelines for the Management of IT Security", atau GMITS / ISO-13335, yang menyediakan sebuah konsep kerangka kerja (framework) untuk manajemen keamanan IT.

- Sistem yang menuntun pada sertifikasi keamanan (untuk saat ini, hanya BS 7799-2 dan derivatif nasional yang menyediakan sebuah proses sertifikasi).

- ISO 17799 tidak mengkhususkan obligasi manapun yang berhubungan dengan metode penaksiran resiko. Cukup memilih apa saja sesuai dengan kebutuhan perusahaan.

3.3. Keuntungan menerapkan ISO-17799

Keuntungan utama dari BS7799/ISO17799 berhubungan dengan kepercayaan publik. Sama seperti ISO 9000 yang mencerminkan jaminan kualitas.

- Standar ini merupakan tanda kepercayaan dalam seluruh keamanan perusahaan.

- Manajemen kebijakan terpusat dan prosedur.

- Menjamin layanan informasi yang tepat guna.

- Mengurangi biaya manajemen,

- Dokumentasi yang lengkap atas segala perubahan/revisi.

- Suatu metoda untuk menentukan target dan mengusulkan peningkatan.

- Basis untuk standard keamanan informasi internal perusahaan

Suatu organisasi yang menerapkan ISO 17799 akan mempunyai suatu alat untuk mengukur, mengatur dan mengendalikan informasi yang penting bagi operasional sistem mereka. Pada gilirannya ini dapat mendorong kearah kepercayaan pelanggan, efisiensi dan efektifitas.

Istilah dan Definisi di ISO-17799

ISO - the International Standards Organization adalah lembaga idependent yang mengeluarkan standar operasional prosedur (SOP) terhadap kualitas suatu layanan.

Information Security - merupakan gambaran dari 3 aspek penting keamanan informasi yang meliputi *confidentiality, integrity dan availability.*

Risk Assessment – perkiraan kemungkinan ancaman akibat kelemahan keamanan sistem informasi dan proses ketersediaan informasi sehingga bisa menyebabkan gangguan.

Risk Management – proses identifikasi, pengawasan, minimalisasi atau eliminasi resiko keamanan yang akan mempengaruhi sistem informasi, untuk biaya yang dapat diterima.

ISMS - *Information System Management System*. Sistem manajemen keamanan informasi organisasi yang menyediakan pendekatan sistematik dalam mengatur informasi yang sensitif agar dapat memproteksinya. Ini meliputi pegawai, proses-proses dan sistem informasi.

PUSTAKA

Ferdinand Aruan, Tugas Keamanan Jaringan Informasi (Dosen. Dr. Budi Rahardjo) Tinjauan Terhadap ISO 17799 - Program Magister Teknik Elektro Bidang Khusus Teknologi Informasi Institut Teknologi Bandung 2003

Indocommit, Kepatuhan terhadap Sistem Keamanan Informasi http://www.indocommit.com/ index.html?menu=29&idnews=1506&kid=0&PHPSESSID=ac0fa9bf4b764ea21e26b230102b4ec, 23 Desember 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, http://202.57.1.181/~download/ linux_opensource/ artikel+tutorial/general_tutorials/wp_iso_id.pdf

News Release, ISO17799: Standar Sistem Manajemen Keamanan Informasi http://www.nevilleclarke.com/newsReleases/newsController.php?do=toNews&id=45 April 27, 2006

Sany Asyari, Keamanan Jaringan Berdasarkan ISO 17799, http://sanyasyari.com/ 2006/09/26/keamanan-jaringan-berdasarkan-iso-17799/ 26 September 2006