Keamanan data/informasi elektronik menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur penting. Sebab data/informasi adalah aset bagi perusahaan tersebut.

Keamanan data/informasi secara langsung maupun tidak langsung dapat mempertahankan kelangsungan bisnis, mengurangi resiko, mengoptimalkan *return of investment* dan bahkan memberikan peluang bisnis semakin besar. Semakin banyak informasi perusahaan yang disimpan, dikelola dan digunakan secara bersama, akan semakin besar pula resiko terjadinya kerusakan, kehilangan atau tereksposnya data/informasi ke pihak lain yang tidak berhak.

Ancaman dan resiko yang ditimbulkan akibat kegiatan pengelolaan dan pemeliharaan data/informasi menjadi alasan disusunnya [standar](https://hadiwibowo.wordpress.com/2009/02/03/2008/04/20/standar-keamanan-informasi-nasional/) sistem manajemen keamanan informasi yang salah satunya adalah ISO 17799.

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

BS 7799 terdiri dari beberapa bagian yaitu : ***Part 1***, *The Code of Practice for Information Security Management*. ***Part 2***, *The Specification for Information Security Management Systems* (ISMS).

Pada tahun 2000, *International Organization of Standardization* (ISO) dan *International Electro-Technical Commission* (IEC) mengadopsi BS 7799 Part 1 dan menerbitkannya sebagai standar ISO/IEC 17799:2000 yang diakui secara internasional sebagai standar sistem manajemen keamanan informasi.

ISO 17799 meliputi 10 klausula pengendalian (10 *control clauses*), 36 sasaran pengendalian (36 *control objectives*) dan 127 pengendalian keamanan (127 *controls securiy*).

Pengendalian adalah cara yang dipilih untuk menyingkirkan atau meminimalkan risiko ke level yang dapat diterima. Berikut adalah penjabaran 10 klausula pengendalian :

**1. Kebijakan Pengamanan *(Security Policy)*,** mengarahkan visi dan misi manajemen agar kelangsungan organisasi dapat dipertahankan dengan mengamankan dan menjaga integritas/keutuhan data/informasi penting yang dimiliki oleh perusahaan.

Kebijakan pengamanan sangat diperlukan mengingat banyaknya masalah-masalah non teknis seperti penggunaan *password* oleh lebih dari satu orang yang menunjukan tidak adanya kepatuhan dalam menjalankan sistem keamanan informasi. Kebijakan pengamanan ini meliputi aspek infratruktur dan regulasi keamanan informasi.

Hal pertama dalam pembuatan kebijakan keamanan adalah dengan melakukan inventarisasi data-data perusahaan. Selanjutnya dibuat regulasi yang melibatkan semua departemen, sehingga peraturan yang akan dibuat tersebut dapat diterima oleh semua pihak. Setelah itu rancangan peraturan tersebut diajukan ke pihak direksi untuk mendapatkan persetujuan dan dukungan agar dapat diterapkan dengan baik.

**2. Pengendalian Akses Sistem (*System Access Control*),** mengendalikan/membatasi akses *user* terhadap informasi-informasi dengan cara mengatur kewenangannya, termasuk pengendalian secara *mobile-computing* ataupun *tele-networking*. Mengontrol tata cara akses terhadap informasi dan sumber daya yang ada yang meliputi berbagai aspek seperti :

a. Persyaratan bisnis untuk kendali akses; b. Pengelolaan akses user (*User Access Management*); c. Kesadaran keamanan informasi (*User Responsibilities*); d. Kendali akses ke jaringan (*Network Access Control*); e. Kendali akses terhadap sistem operasi (*Operating System Access Control*); f. Pengelolaan akses terhadap aplikasi (*Application Access Management*); g. Pengawasan dan penggunaan akses sistem (*Monitoring System Access and Use*); dan h. *Mobile Computing* dan *Telenetworking.*

**3. Pengelolaan Komunikasi dan Kegiatan (Communication and Operations Management),** 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. Prosedur dan tanggung jawab operasional; b. Perencanaan dan penerimaan sistem; c. Perlindungan terhadap software jahat (*malicious software*); d. *Housekeeping*; e. Pengelolaan Network; f. Pengamanan dan Pemeliharaan Media; dan g. Pertukaran informasi dan software.

**4. Pengembangan dan Pemeliharaan Sistem (*System Development and Maintenance*),** memastikan bahwa sistem operasi maupun aplikasi yang baru diimplementasikan mampu bersinergi melalui verifikasi dan validasi.

Penelitian untuk pengembangan dan pemeliharaan sistem meliputi berbagai aspek, seperti : Persyaratan pengamanan sistem; Pengamanan sistem aplikasi; Penerapan Kriptografi; Pengamanan file sistem; dan Pengamanan pengembangan dan proses pendukungnya.

**5. Pengamanan Fisik dan Lingkungan (*Physical and Environmental Security*),** mencegah kehilangan dan/atau kerusakan data yang diakibatkan oleh lingkungan secara fisik, termasuk bencana alam dan pencurian data yang tersimpan dalam media penyimpanan atau dalam fasilitas penyimpan informasi yang lain.

Pengamanan fisik dan lingkungan ini meliputi aspek : Pengamanan area tempat informasi disimpan; Pengamanan alat dan peralatan yang berhubungan dengan informasi yang akan dilindungi; dan Pengendalian secara umum terhadap lingkungan dan hardware informasi.

**6. Penyesuaian (*Compliance*),** memastikan implementasi kebijakan-kebijakan keamanan selaras dengan peraturan dan perundangan yang berlaku, termasuk perjanjian kontrak melalui audit sistem secara berkala*.* Aspek-aspek yang diperlukan untuk membentuk prosedur dan peraturan, yaitu : Penyesuaian dengan persyaratan legal; Peninjauan kembali kebijakan pengamanan dan penyesuaian secara teknis; serta Pertimbangan dan audit sistem.

**7. Keamanan personel/sumber daya manusia (*Personnel Security*),** upaya pengurangan resiko dari penyalahgunaan fungsi dan/atau wewenang akibat kesalahan manusia (*human error*),manipulasi data dalam pengoperasian sistem serta aplikasi oleh *user*. Kegiatan yang dilakukan diantaranya adalah pelatihan-pelatihan mengenai kesadaran informasi (*security awareness*) agar setiap *user* mampu menjaga keamanan data dan informasi dalam lingkup kerja masing-masing.

*Personnel Security* meliputi berbagai aspek, *yaitu : Security in Job Definition and Resourcing*; Pelatihan-pelatihan dan *Responding to Security Incidens and Malfunction.*

**8. Organisasi Keamanan (*Security Organization*),** memelihara keamanan informasi secara global pada suatu organisasi atau instansi, memelihara dan menjaga keutuhan sistem informasi internal terhadap ancaman pihak eksternal, termasuk pengendalian terhadap pengolahan informasi yang dilakukan oleh pihak ketiga (*outsourcing*). Aspek yang terlingkupi, yaitu : keamanan dan pengendalian akses pihak ketiga dan *Outsourcing*

**9. Klasifikasi dan pengendalian aset (*Asset Classification and Control*),** memberikan perlindungan terhadap aset perusahaan yang berupa aset informasi berdasarkan tingkat perlindungan yang telah ditentukan. Perlindungan *aset ini meliputi accountability for Asset* dan klasifikasi informasi.

**10. Pengelolaan Kelangsungan Usaha (*Business Continuity Management*),** siaga terhadap resiko yang mungkin timbul didalam aktivitas lingkungan bisnis yang bisa mengakibatkan ”*major failure*” atau resiko kegagalan sistem utama ataupun ”*disaster*” atau kejadian buruk yang tak terduga, sehingga diperlukan pengaturan dan pengelolaan untuk kelangsungan proses bisnis, dengan mempertimbangkan semua aspek dari *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.