BAB 2
LANDASAN TEORI

2.1. KEAMANAN INFORMASI

Informasi adalah aset, sebagaimana aset-aset penting lainnya, yang esensial terhadap bisnis organisasi dan oleh sebab itu perlu dilindungi dengan sepantasnya. Lebih penting lagi karena makin bertambahnya interkoneksi lingkungan bisnis. Sebagai hasil dari meningkatnya interkonektivitas, informasi diekspos terhadap ancaman dan *vulnerability* yang jumlahnya meningkat dan keanekaragaman yang lebih luas.

Informasi terdapat dalam berbagai bentuk. Bisa berupa hasil cetakan atau tulisan pada kertas, disimpan secara elektronik, dikirimkan lewat pos atau secara eletronik, ditampilkan dalam film, atau disebutkan dalam percakapan. Apapun bentuk dari informasi tersebut, atau dengan cara bagaimana dibagi atau disimpan, harus selalu dilindungi dengan selayaknya.

Information Security atau keamanan informasi adalah perlindungan informasi dari berbagi ancaman agar menjamin kelanjutan bisnis, mengurangi resiko bisnis, dan meningkatkan *return of investment* dan peluang bisnis.

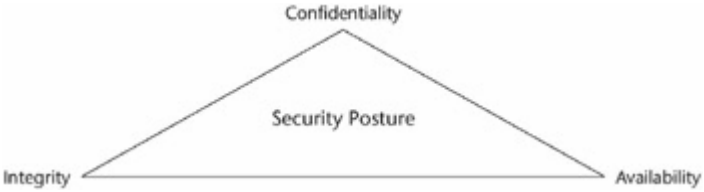
Keamanan informasi meliputi perlindungan terhadap aspek-aspek berikut [HARR2008]:

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 pihak yang berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas 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).



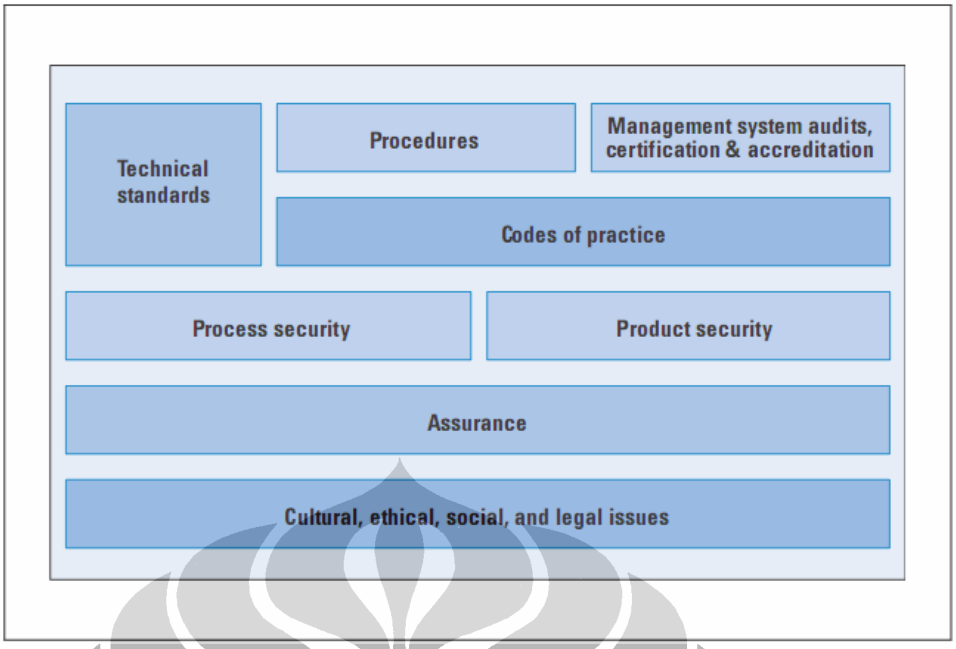
Gambar 2.1. CIA Triad [HARR2008]

Ketiga aspek tersebut dikenal dengan CIA Triad. Selama lebih dari 20 tahun CIA Triad ini sudah dipegang menjadi prinsip dasar keamanan informasi.

Keamanan informasi diperoleh dengan mengimplementasikan kumpulan kontrol yang sesuai, termasuk kebijakan, proses, prosedur, struktur organisasi, dan fungsi-fungsi perangkat lunak dan perangkat keras. Kontrol-kontrol ini perlu dibuat, diimplementasikan, dimonitor, ditinjau, dan ditingkatkan untuk memastikan kesesuaian antara keamanan yang spesifik tersebut dan tujuan bisnis. Ini harus dilakukan dalam kaitan dengan proses pengelolaan bisnis lainnya.

Standar-standar untuk menyediakan keamanan sistem informasi menjadi perlu sekali di lingkungan sistem informasi karena lingkungan tersebut cukup kompleks mencakup berbagai macam sistem *storage*, server, workstation, jaringan lokal, Internet, dan koneksi jaringan jarak jauh lainnya. Standar dapat menentukan cakupan kebutuhan fungsi-fungsi dan fitur-fitur keamanan, kebijakan-kebijakan untuk mengelola aset-aset informasi dan manusia, kriteria untuk mengevaluasi keefektifan dari tindakan-tindakan keamanan, teknik-teknik pengukuran yang berkesinambungan dari keamanan, dan untuk pengawasan terus-menerus dari pelanggaran-pelanggaran keamanan, dan prosedur-prosedur untuk menghadapi kegagalan-kegagalan keamanan.

Gambar 2.2 merupakan pendekatan yang efektif untuk manajemen keamanan informasi yang berupa elemen-elemen dalam bentuk yang terintegrasi. Fokus dari pendekatan ini adalah pada dua aspek yang berbeda dari menyediakan keamanan informasi yaitu proses dan produk [STAL2005]. Elemen-elemen tersebut adalah sebagai berikut:



Gambar 2.2. Elemen-elemen Manajemen Keamanan Sistem Informasi [STALL 2005]

- *Process security* melihat keamanan informasi dari sudut pandang manajemen kebijakan, prosedur, dan kontrol.
- *Product security* berfokus pada aspek-aspek teknis dan ditujukan dengan penggunaan produk-produk bersertifikat dalam lingkungan TI jika memungkinkan.
- *Technical standards* merujuk pada spesifikasi-spesifikasi yang mengacu pada aspek-aspek seperti keamanan jaringan TI, *digital signatures*, *access control, nonrepudiation, key management,* dan *hash functions.*
- *Procedures* operasional, manajemen, dan teknis meliputi kebijakan dan pelaksanaan yang ditentukan dan dilaksanakan oleh manajemen. Contohnya mencakup kebijakan *personnel screening*, pedoman pengklasifikasian informasi, dan prosedur pemberian *user ID*.
- *Management system audits, certification & accreditation* berhubungan dengan kebijakan dan prosedur manajemen untuk pengauditan dan sertifikasi produk-produk keamanan informasi.
- *Code of practice* berhubungan dengan standar-standar kebijakan yang spesifik yang mendefinisikan aturan-aturan dan tanggung jawab dari berbagai karyawan dalam pemeliharaan keamanan informasi.

- *Assurance* berhubungan dengan pengujian produk dan sistem serta evaluasi.
- *Cultural, ethical, social, and legal issuers* mengacu kepada aspek-aspek faktor manusia yang berhubungan dengan keamanan informasi.

Banyak standar dan dokumen-dokumen panduan telah dikembangkan belakangan ini untuk membantu manajemen di bidang keamanan informasi. Dua yang paling penting adalah ISO 17799 yang berhubungan dengan proses keamanan dan *Common Criteria,* yang berhubungan dengan produk keamanan. Yang menjadi bagian pembahasan dalam penelitian adalah adalah ISO 17799.

2.2. ARSITEKTUR KEAMANAN

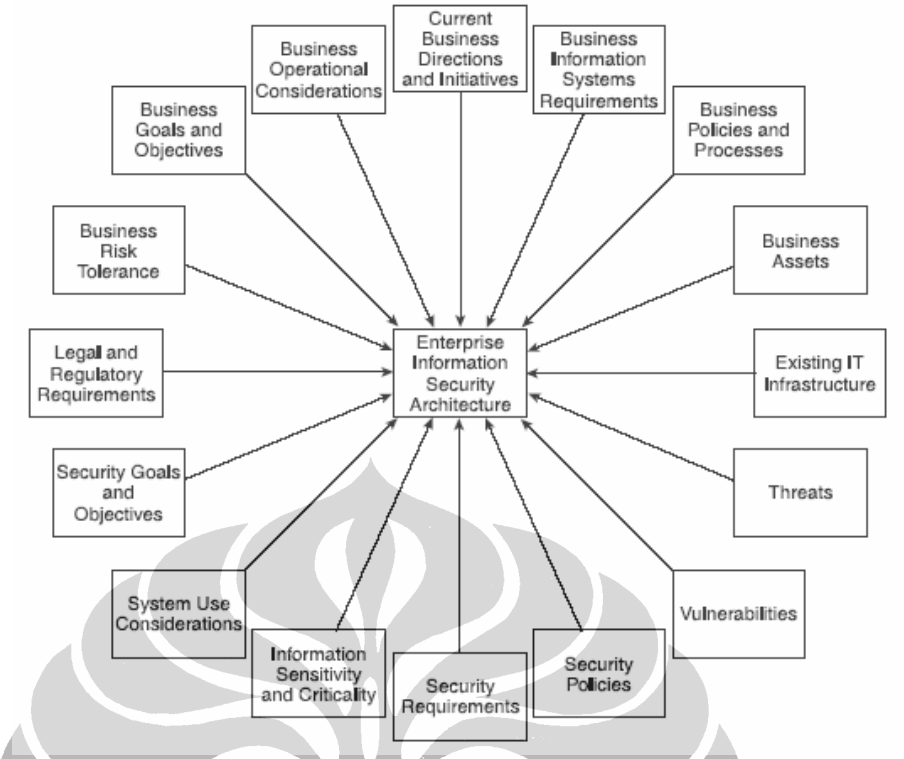
2.2.1. Prinsip-prinsip Umum Arsitektur Keamanan Informasi Enterprise

Tujuan-tujuan arsitektur keamanan informasi enterprise, dalam mendukung tugas bisnis, harus berisi hal-hal berikut ini [TIPT2005] :

- Tidak menghalangi aliran informasi yang terautorisasi atau efek yang merugikan produktifitas pengguna
- Melindungi informasi pada titik masuk ke dalam organisasi
- Melindungi informasi sepanjang masih dibutuhkan
- Menerapkan proses-proses dan pelaksanaan umum di seluruh organisasi
- Menjadi modular untuk memperbolehkan teknologi baru menggantikan yang sudah ada dengan dampak sekecil mungkin
- Menjadi transparan secara virtual terhadap pengguna
- Mengakomodasi infrastruktur yang ada

2.2.2. Masukan Terhadap Arsitektur Keamanan

Gambar 2.3 menerangkan masukan-masukan pada proses awal perumusan arsitektur keamanan informasi enterprise. Proses tersebut harus, setidaknya, mempertimbangkan masukan-masukan berikut [TIPT2005] :



Gambar 2.3. Pertimbangan-pertimbangan untuk perumusan Enterprise Information Security Architecture [TIPT2005]

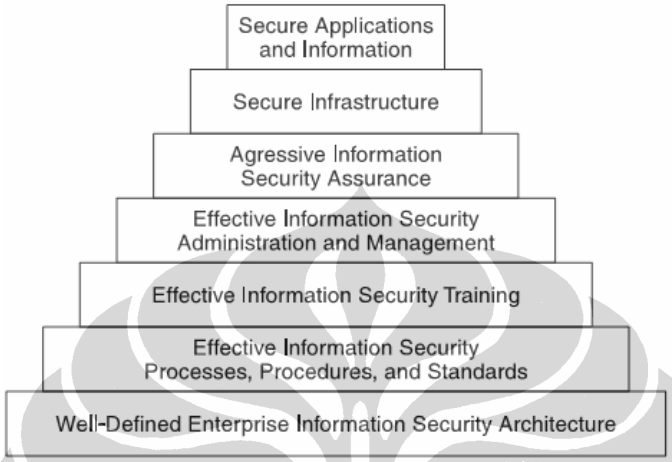
1. Masukan-masukan terkait dengan Bisnis:
   - Tujuan dan sasaran bisnis untuk memproteksi kepentingan-kepentingan bisnis organisasi, aset, personil, dan publik; serta tujuan ke depan dari sistem informasi bisnis dan pendukungnya
   - Pertimbangan-pertimbangan operasional bisnis bagaimana bisnis akan beroperasi tiap hari (cth: pendekatan tersentralisasi atau desentralisasi pada administrasi keamanan)
   - Arahan dan inisiatif bisnis sekarang ini untuk sistem informasi yang terinstal dan yang sedang dalam pengembangan
   - Kebutuhan-kebutuhan sistem informasi bisnis (cth: kebutuhan akses, kebutuhan ketersediaan, konektivitas rekan bisnis)
   - Kebijakan dan proses bisnis yang menetapkan tindakan keamanan mana yang bisa dan yang tidak bisa diterima
   - Aset-aset bisnis yang diproteksi oleh arsitektur

- Infrastruktur yang ada termasuk karakterisasi lingkungan teknikal yang sekarang dan apa yang mungkin menolong atau berakibat negatif terhadap keamanan informasi
- Toleransi resiko bisnis untuk penyingkapan informasi, modifikasi yang tidak terautorisasi dan kehilangan, ketidaktersediaan, *downtime* karena *hacker* dan virus, dan web page yang di-*deface*
- Syarat-syarat legal dan ketentuan yang berlaku termasuk hukum dan regulasi
- Ancaman-ancaman terhadap infrastruktur yang ada atau pekerjaan bisnis
- *Vulnerabilities* yang berhubungan dengan infrastruktur yang ada atau *computing operations.*

2. Masukan-masukan terkait Keamanan:
   - Tujuan dan sasaran keamanan (cth: melindungi aset-aset informasi dari penggunaan yang tidak terautorisasi dan tidak tepat, kehilangan, atau kerusakan; proteksi informasi sensitif dari penyingkapan yang tidak terautorisasi dan manipulasi; dan proteksi ketersediaan informasi yang kritikal
   - Pertimbangan-pertimbangan penggunaan sistem termasuk siapa yang akan menggunakan sistem informasi (pegawai, kontraktor), level mana dari *background screening*, kapan (jam berapa, hari apa), dimana (kantor, rumah, perjalanan), kenapa (*inquries, file updating, research*), dll.
   - Sensitivitas dan kekritisan informasi untuk diproteksi, termasuk dampak terkait *unavailability* atau kehilangan
   - Kebutuhan keamanan untuk melindungi informasi, aplikasi, platform, dan jaringan berdasarkan sensitivitas dan kekritisan informasi (cth: menandai media yang sensitif, *backup* informasi, menyimpan *backup* di luar lokasi, mengenkripsi informasi yang disimpan di lokasi yang tidak aman atau ditransmisikan melalui jaringan yang tidak dapat dipercaya.

3. Kebijakan-kebijakan keamanan terhadap tindakan keamanan mana yang bisa dan yang tidak bisa diterima.

2.2.3. Membangun *Secure Computing Environment*



Gambar 2.4 Blok Bangunan dari *Secure Computing Enviroment* [TIPT2005]

Seperti pada Gambar 2.4, arsitektur keamanan informasi enterprise yang terdefinisi dengan baik menyediakan landasan untuk infrastruktur yang aman dan lingkungan *computing* yang aman. Blok bangunan dari lingkungan *computing* yang aman mencakup [TIPT2005] :

- *Well-defined enterprise information security architecture*, dengan akuntabilitas, strategi-strategi penerapan, teknologi, dan layanan-layanan keamanan
- *Effective Information Security Processess, Procedures, and Standards*, yang diperoleh dari kebijakan-kebijakan, tapi berhubungan dengan komponen-komponen dan teknologi-teknologi yang spesifik dan menyediakan spesifikasi rinci yang dapat diaudit
- *Effective Information Security Training*, termasuk pelatihan pegawai baru, pelatihan operasional berkaitan dengan pekerjaan untuk para eksekutif
- *Effective Information Security Administration and Management,* termasuk manajemen konfigurasi, *information resources management*

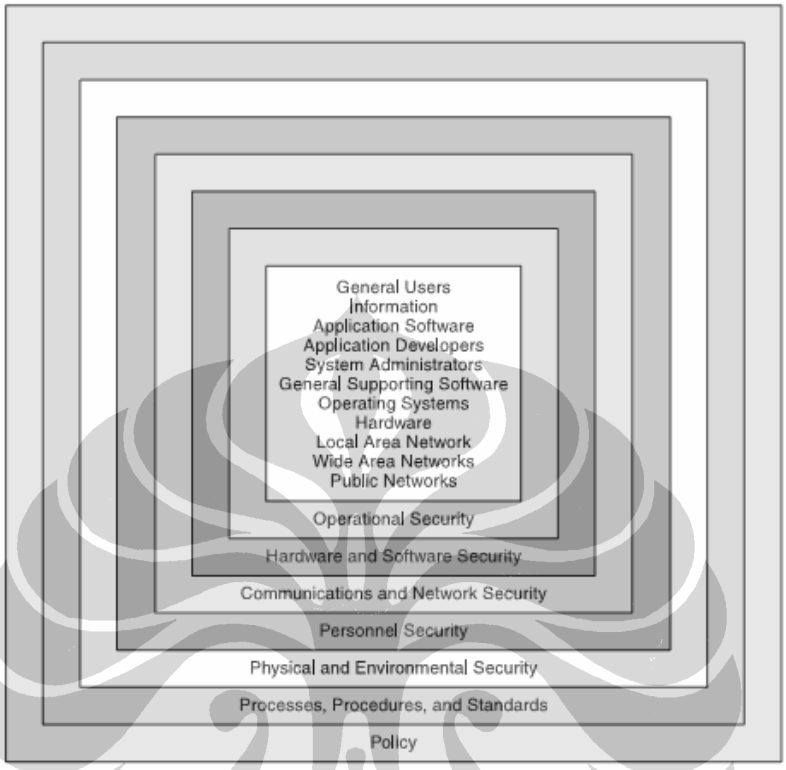
(IRM), platform-platform yang dipertegas dengan *patch* keamanan terbaru, logging, alarm, dan review dari *common vulnerabilities and exposures (CVEs)*

- *Aggressive information security assurance*, termasuk sertifikasi, akreditasi, *self-assessments,* inspeksi, audit, dan *independent verification and validation (IV&V)*
- *Secure Infrastructure*, termasuk DMZ, routers, filters, firewalls, gateways, air gaps, *protected distribution systems (PDSs), virtual private networks (VPNs),* daerah *(enclave)* yang aman, dan lingkungan percobaan yang terpisah
- *Secure Applications,* termasuk modul-modul yang dirancang dengan baik, terstruktrur, dan terdokumentasi; *software quality assurance; code review;* pemeriksaan integritas file atau perangkat lunak deteksi perubahan, termasuk produk seperti Tripwire dan Advanced Intrution Detection Environment (AIDE); dan akses berdasarkan *principles of clearance, need-to-know,* dan *least privilege*
- *Secure Information,* termasuk enkripsi, backup, dan *integrity checking software.*

2.2.4. Defense-in-Depth untuk Lingkungan *Secure Computing*

Gambar 2.5 [TIPT2005] menjelaskan syarat-syarat untuk sebuah lingkungan *secure computing*. Kurangnya keamanan pada salah satu dari komponen-komponen ini akan berdampak negatif pada keamanan pada lingkungan *computing*. Jika tidak ada *Policy*, maka tidak ada arahan manajemen yang seragam akan bagaimana melindungi bisnis, operasinya, orang-orangnya, dan informasinya. Jika tidak ada *processes and procedures* dengan *standard* yang terkait, implementasi kebijakan akan berdasarkan pada interpretasi individu pada kebijakan yang berbeda dari satu orang ke orang lain. Jika tidak ada *phisycal security*, maka kontrol logikal dan administratif dapat dengan mudah diperdaya tanpa diketahui. Kurangnya kontrol lingkungan dapat menjatuhkan organisasi dan menyebabkan pengrusakan yang lebih banyak daripada *malicious agent.* Jika *personnel security* tidak mencukupi, maka kemungkinan ancaman dari dalam

meningkat secara dramatis dan dampaknya mungkin tidak terdeteksi dalam periode waktu yang signifikan.



Gambar 2.5. Defense-in-Depth [TIPT2005]

Kebutuhan untuk *Communication and Network Security* begitu nyata; kita hidup di dunia yang terhubung *(connected word)*. Bagaimanapun, penggunaan yang tidak diakui dan kehadiran yang tidak diketahui dari modem atau *access point* jaringan wireless akan menggagalkan proteksi firewall. Kontrol *Hardware* harus sejalan dengan kegunaan perangkat, cth: server harus diperkuat sebelum digunakan jika itu akan menjadi efektif. *Software* dan kotrol yang berkaitan dengannya harus *up to date*, termasuk *patch* dan file signature virus yang terupdate. Pegawai, kontraktor, vendor, dan pengunjung harus tahu apa yang dibutuhkan dari mereka untuk mendukung keamanan informasi enterprise. *Public Networks*, meskipun penting untuk banyak operasi bisnis, harus dilihat sebagai komponen yang *untrusted* dari arsitektur enterprise dan ditangani dengan layak. *Wide Area Networks (WANs)* dan *local area networks (LANs)* memiliki syarat-syarat operasi tertentu yang harus dinilai pada kemampuannya melakukan fungsi-

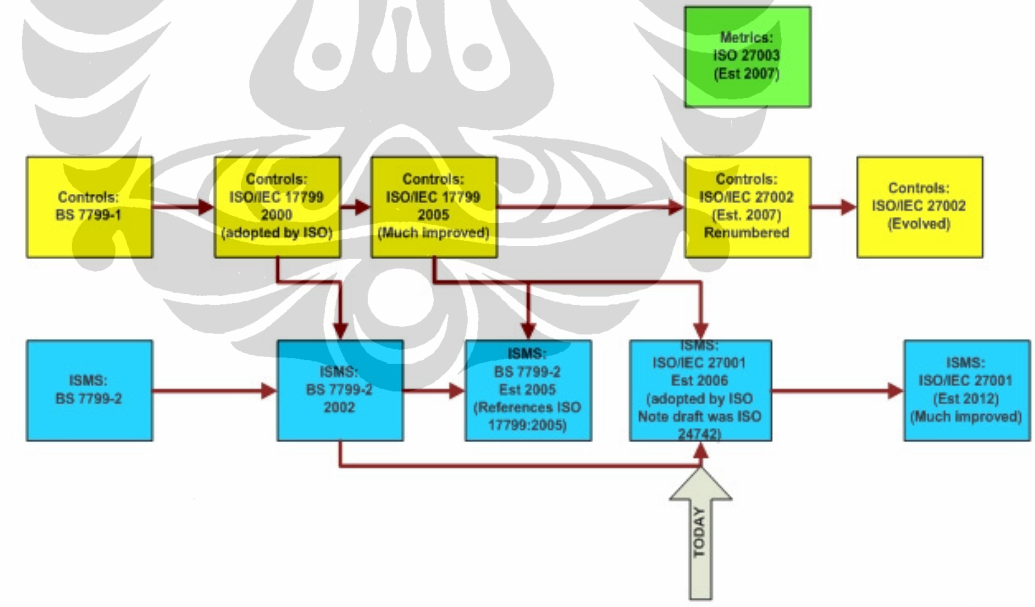
fungsi yang dibutuhkan, dan harus diproteksi sehingga tidak bisa dikonfigurasi ulang untuk melakukan fungsi-fungsi yang tidak teraoutorisasi. Perangkat lunak harus berlisensi, dibeli dari sumber yang terpercaya, dan dinilai untuk memastikan tidak mengandung *malicious code* bahkan jika terkompres *(shrink-wrapped).* Administrasi sistem dan pengembang aplikasi harus orang-orang yang terpercaya dengan *clearences* yang sesuai yang telah dilatih untuk melakukan tanggung jawab pekerjaannya secara akurat dan efektif. *Application Software* harus dirancang, dikembangkan, dan diimplementasikan dengan akurat untuk melindungi informasi dan lingkungan bisnis. *Information* adalah sumber hidup dari organisasi dan harus diproteksi dari penyingkapan yang tidak terautorisasi, meskipun dibuat tersedia ketika dibutuhkan dalam format yang akurat, bisa digunakan, dan lengkap. *General users* menggambarkan ancaman yang signifikan pada lingkungan *secure computing*, secara sengaja atau dengan maksud jahat. Tindakan-tindakan pengguna harus dikendalikan, dan penguna harus dilatih dalam pengerjaan-pengerjaan yang aman dan penggunaan informasi dan sumber-sumber *computing* dan komunikasi. Pengguna adalah komponen terlemah dari lingkungan *secure computing*, dan pengabaian atau *social engineering* dapat berakibat kontrol yang dibangun diperdaya. Oleh karena itu, *defense-in-depth* harus juga termasuk *checks* and *balances*, dengan berbagai fungsi keamanan dan komponen-komponen yang terkait untuk menunjukan syarat-syarat keamanan.

2.3. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Information security management system (ISMS) adalah sekumpulan kebijakan-kebijakan yang berhubungan dengan manajemen keamanan informasi. Konsep kunci dari ISMS adalah agar organisasi merancang, menerapkan, dan memelihara rangkaian yang berkaitan dari proses dan sistem untuk secara efektif mengelola aksesibilitas informasi, kemudian memastikan *confidentiality, integrity and availability* dari aset-aset informasi dan meminimalkan resiko-resiko keamanan informasi [WIKI-ISMS].

ISMS yang paling diketahui umum diterangkan di ISO 27001 dan ISO 17799. Standar ISMS ini pertama kali dipublikasikan sebagai British Standard, BS 7799, yang terbagi dalam dua bagian [HALL2008]:

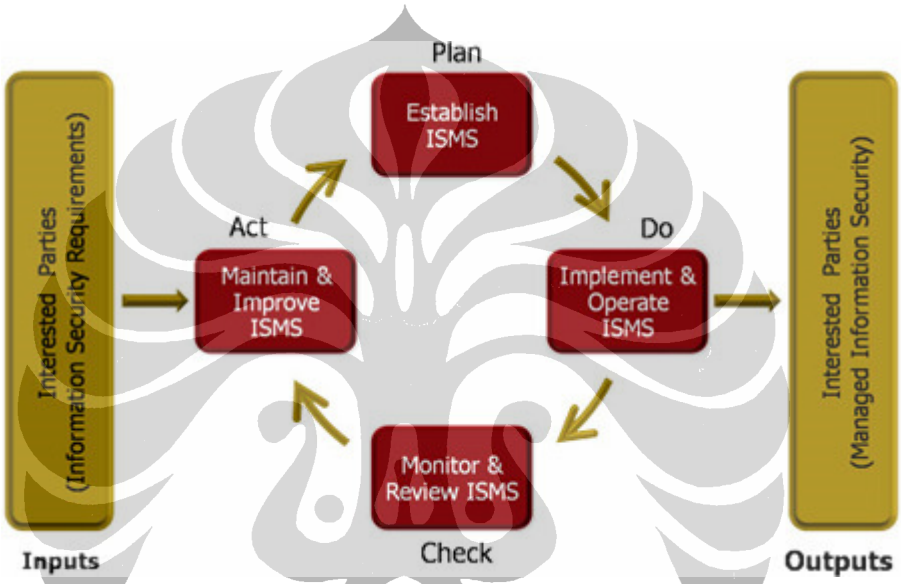
- *Code of practice* : BS 7799-1 dipublikasikan tahun 1995, kemudian dirilis sebagai BS7799:1999 setelah revisi mayor. Kemudian setelah revisi minor dokumen ini diterima sebagai standar internasional untuk Manajemen Keamanan Informasi ISO 17799:2000, dan dipublikasi ulang tahun 2005 sebagai ISO/IEC 17799:2005 (Direncanakan akan diubah menjadi ISO 27002).
- *Management system* : awalnya dipublikasikan sebagai BS 7799-2 tahun 1998, telah ditambahkan untuk menyediakan panduan dalam membuat dan syarat-syarat untuk Sistem Manajemen Keamanan Informasi. Kemudian direvisi untuk memasukkan lingkaran PDCA dan dipublikasikan sebagai BS7799-2:2002. Setelah direvisi lagi, telah diterima sebagai standar internasional ISO/IEC 27001:2005.



Gambar 2.6. Sejarah Perkembangan BS7799 menjadi ISO 27001 dan ISO 27002 [ATSE2009]

2.4. ISO 27001:2005

Standar internasional ini telah dipersiapkan untuk menyediakan sebuah model untuk pembangunan, penerapan, pengerjaan, pengawasan, peninjauan, pemeliharaan, peningkatan sebuah Information Security Management System (ISMS). Standar ini mengadopsi model *Plan-Do-Check-Act (PDCA)* yang diterapkan untuk menyusun seluruh proses ISMS seperti pada Gambar 2.7 [ISO27001].



Gambar 2.7. Model PDCA yang diterapkan pada proses-proses ISMS [ISO27001]

Secara ringkas, proses-proses pada tiap fase PDCA di atas dijelaskan di Tabel 2.1 di bawah ini [ISO27001].

Tabel 2.1. Pemetaan proses-proses ISMS terhadap Fase-fase PDCA

Plan (establish the ISMS)	Membangun kebijakan, objektif, proses, dan prosedur ISMS yang berhubungan dengan pengelolaan resiko dan peningkatan keamanan informasi untuk memberikan hasil-hasil yang sesuai dengan kebijakan dan objektif yang menyeluruh dari suatu organisasi.
Do (implement and operate the ISMS)	Menerapkan dan mengoperasikan kebijakan, kontrol, proses, dan prosedur ISMS.
Check (monitor and review the ISMS)	Menilai dan, jika dapat dilakukan, mengukur performa proses terhadap kebijakan, objektif, dan pengalaman praktis ISMS dan melaporkan hasilnya ke manajemen sebagai tinjauan.

Act (maintain and improve the ISMS)	Mengambil tindakan perbaikan dan pencegahan, berdasarkan hasil audit ISMS internal dan tinjauan manajemen atau informasi lain yang relevan, untuk mencapai peningkatan yang berkesinambungan dari ISMS.

2.4.1. Fase 1: Plan (Establish the ISMS) [ISO 27001]

Pada fase *Plan* ini, langkah-langkah yang dilakukan adalah:

1. Menentukan ruang lingkup ISMS
2. Menentukan kebijakan-kebijakan ISMS dalam arti karakteristik bisnis, organisasi tersebut, lokasinya, aset-aset dan teknologi yang:
   a) berisi *framework* untuk menetapkan *objectives* dan membangun sebuah *sense* yang menyeluruh dari arah dan prinsip-prinsip untuk tindakan dengan memperhitungkan keamanan informasi;
   b) memuat ke dalam *account business* dan syarat-syarat legal atau regulasi, dan kewajiban-kewajian keamanan kontraktual;
   c) menyesuaikan dengan konteks manajemen resiko strategik organisasi dimana pembangunan dan perawatan ISMS akan diletakkan;
   d) membangun kriteria untuk resiko yang akan dievaluasi; dan
   e) telah disetujui oleh manajemen.
3. Menentukan pendekatan yang sistematis untuk mengukur resiko
   a) Identifikasi metodologi pengukuran resiko yang sesuai dengan ISMS, dan keamanan informasi bisnis yang dikenali, syarat-syarat legal dan regulasi.
   b) Mengembangkan kriteria untuk menerima resiko dan identifikasi level-level resiko yang dapat diterima.
4. Identifikasi resiko-resiko.
   a) Identifikasi aset-aset di dalam ruang lingkup ISMS, dan para pemilik dari aset-aset tersebut.
   b) Identifikasi ancaman-ancaman pada aset-aset tersebut.
   c) Identifikasi *vulnerabilities* yang mungkin diekploitasi oleh ancaman-ancaman.

d) Identifikasi dampak-dampak hilangnya *confidentiality, integrity,* dan *availability* yang terjadi pada aset-aset.

5. Mengukur (analisa dan evaluasi) resiko-resiko
   a) Mengukur dampak-dampak bisnis pada organisasi yang mungkin akibat dari kegagalan-kegagalan keamanan, memasukkan ke dalam catatan konsekuensi-konsekuensi dari kehilangan *confidentiality, integrity,* atau *availability* aset-aset tersebut.
   b) Mengukur kemungkinan realistis dari kegagalan-kegagalan keamanan yang terjadi dalam ancaman dan *vulnerabilities* umum, dan dampak-dampak yang dihubungkan dengan aset-aset tersebut, dan kontrol-kontrol yang diimplementasikan saat ini.
   c) Memperkirakan level-level resiko.
   d) Menentukan apakah resiko-resiko tersebut bisa diterima atau membutuhkan perlakuan yang menggunakan kriteria untuk menerima resiko-resiko yang sudah terbentuk.
6. Identifikasi dan evaluasi opsi-opsi untuk memperlakukan resiko-resiko.
   Tindakan-tindakan yang mungkin mencakup:
   a) Menerapkan kontrol-kontrol yang sesuai;
   b) Menerima dengan sadar dan objektif resiko-resiko, menyediakan kebijakan-kebijakan organisasi yang memenuhi dengan jelas dan kriteria untuk menerima resiko-resiko;
   c) Menghidari resiko-resiko; dan
   d) Memindahkan resiko-resiko bisnis yang berhubungan ke pihak lain, seperti penjamin asuransi, supplier.
7. Pilih *control objectives* dan kontrol-kontrol.
8. Persiapkan *statement of Applicability*
   Statement of Applicability harus dipersiapkan yang memuat hal-hal berikut:
   a) *control objectives* dan kontrol-kontrol yang dipilih pada 7) dan alasan-alasan pemilihannya; dan
   b) pengecualian dari *control objectives* dan control-kontrol dalam Annex A [ISO27001] dan justifikasi untuk pengecualiannya.

9. Mendapatkan persetujuan manajemen.

2.4.2. Fase 2: Do (Implement and Operate the ISMS)

Langkah-langkah yang dilakukan pada fase *Do* ini adalah:

1. Memformulasikan sebuah rencana tindakan terhadap resiko
2. Menerapkan rencanan tindakan terhadap resiko tersebut
3. Menerapkan seluruh *control objectives* dan *control* yang dipilih
4. Menerapkan program pelatihan dan kesadaran
5. Mengelola pengoperasian

2.4.3. Fase 3: Check (Monitor and review the ISMS)

Langkah-langkah yang dilakukan pada fase *Check* ini adalah:

1. Mengeksekusi prosedur-prosedur pengawasan
2. Melakukan tinjauan berkala terhadap efektivitas ISMS tersebut
3. Meninjau tingkat resiko yang tertinggal dan resiko yang dapat diterima
4. Melakukan audit ISMS internal
5. Melakukan tinjauan manajemen terhadap ISMS secara berkala
6. Mencatat semua kejadian yang memiliki dampak terhadap performa ISMS

2.4.4. Fase 4: Act (Maintain and Improve the ISMS)

Langkah-langkah yang dilakukan pada fase *Act* ini adalah:

1. Menerapkan perbaikan yang diidentifikasikan
2. Mengambil pencegahan yang sesuai serta tindakan perbaikan
3. Mengkomunikasikan hasilnya kepada seluruh pihak yang terkait
4. Memastikan bahwa perbaikan telah mencapai tujuan-tujuan yang dimaksud

2.5. ISO 17799:2005

Latar belakang disusunnya ISO 17799, standar untuk manajemen keamanan sistem informasi, adalah karena diperlukan suatu cara bagaimana data atau informasi tersebut dikelola, dipelihara dan diekspos.

Awalnya adalah BS 7799 part 1 pada tahun 1995, *the Code of Practice for Information Security Management*. 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. Kemudian tahun 2005 diperbaharui menjadi ISO/IEC 17799:2005, perubahan yang terjadi dari tahun 2000 ke 2005 seperti pada Tabel 2.2.

Tabel 2.2. Perubahan ISO 17799:2000 ke ISO 17799:2005

2005		**2000**
Security Policy	↔	Security Policy
Organization of Information Security	↔	Organizational Security
Asset Management	↔	Asset Classification and Control
Human Resource Security	↔	Personnel Security
Physical and Environmental Security	↔	Physical and Environmental Security
Communications and Operations Management	↔	Communication and Operations Management
Access Control	↔	Access Control
Information Systems Acquisition Development and Maintenance	↔	System Development and Maintenance
Information Security Incident Management	↔	
Business Continuity Management	↔	Business Continuity Management
Compliance	↔	Compliance

ISO 17799:2005 mendefinisikan 133 buah kontrol keamanan yang terstruktur di bawah 11 *clauses* untuk memudahkan praktisi keamanan informasi mengidentifikasi hal-hal yang dibutuhkan untuk mengamankan bisnis dan organisasi mereka. Secara ringkas 11 *clauses* pada ISO 17799:2005 adalah seperti pada Tabel 2.3 [ISO17799].

Tabel 2.3. Sebelas *Clauses* dari ISO 17799:2005

Security Policy	Mempersiapkan arahan dan dukungan manajemen untuk keamanan informasi yang sesuai dengan kebutuhan bisnis dan aturan-aturan dan regulasi yang relevan.
Organization of Information Security	Mengelola keamanan informasi di dalam organisasi. Memelihara keamanan dari informasi organisasi dan fasilitas pemrosesan informasi yang diakses, diproses, dikomunikasikan, atau dikelola oleh pihak luar.
Asset Management	Mencapai dan memelihara proteksi yang sesuai dari aset-aset organisasi. Memastikan bahwa informasi mendapat tingkat keamanan yang sesuai.
Human Resources Security	Memastikan bahwa para pegawai, kontraktor, dan pengguna pihak ketiga: • memahami tanggung jawab mereka dan sesuai dengan peran yang dipertimbangkan untuk mereka • menyadari ancaman dan urusan keamanan informasi • meninggalkan organisasi atau pergantian pegawai dengan cara yang tertib.
Physical and Environmental Security	Mencegah akses fisik yang tidak terautorisasi, kerusakan, atau interferensi pada bangunan dan informasi organisasi. Mencegah kehilangan, kerusakan, pencurian, atau kompromi dari aset dan terhentinya aktivitas organisasi.
Communications and Operations Management	Mengembangkan kontrol-kontrol untuk prosedur operasional, manajemen penyampaian layanan pihak ketiga, perencanaan sistem, proteksi *malware*, backup, manajemen keamanan jaringan, penanganan media, pertukaran informasi, layanan *e-commerce*, dan pengawasan.
Access Control	Mengembangkan kontrol-kontrol pada syarat-syarat bisnis untuk akses pengguna, tanggung jawab pengguna, kontrol akses jaringan, kontrol akses OS, kontrol akses aplikasi, dan kontrol akses informasi.
Information Systems Acquisition, Development, and Maintenance	Mengembangkan kontrol-kontrol untuk pemrosesan yang benar dalam aplikasi, fungsi kriptografi, keamanan file sistem, keamanan proses *support*, dan manajemen *vulnerability*.
Information Security Incident Management	Memastikan kejadian-kejadian dan kelemahan keamanan informasi yang berhubungan dengan sistem informasi dikomunikasikan dalam cara yang memperbolehkan tindakan perbaikan tepat waktu dilakukan.

	Memastikan pendekatan yang konsisten dan efektif diterapkan pada manajemen insiden-insiden keamanan informasi.
Business Continuity Management	Menggagalkan interupsi-interupsi pada aktivitas-aktivitas bisnis untuk mencegah proses bisnis yang kritikal dari akibat kegagalan mayor dari sistem informasi atau bencana dan untuk memastikan pemulihannya yang tepat waktu.
Compliance	Mencegah pelanggaran dari segala aturan, hukum, regulasi, atau kewajiban kontraktual, dan segala syarat-syarat keamanan. Memastikan penyesuaian sistem dengan kebijakan dan standar keamanan organisasi. Memaksimalkan keefektifan dan meminimalkan inteferensi kepada dan dari proses audit sistem informasi.

Berikut ini pembahasan dari *control objectives* yang terdapat di masing-masing *Clauses* dari ISO 17799:2005 tersebut.

2.5.1. Security Policy

2.5.1.1. Information Security Policy

Bertujuan untuk menyediakan arah manajemen dan dukungan untuk keamanan informasi. Manajemen harus memberikan arah yang jelas dan memperlihatkan dukungan dan komitmen terhadap informasi melalui pemeliharaan keamanan informasi dan organisasi.

2.5.2. Organization of Information Security

2.5.2.1. Internal Organization

Bertujuan untuk mengatur keamanan informasi dan organisasi. Sebuah kerangka manajemen harus dibuat untuk memulai dan mengontrol implementasi keamanan informasi dalam organisasi.

2.5.2.2. External Parties

Bertujuan untuk menjaga keamanan dari fasilitas pemrosesan informasi dan aset informasi diakses oleh pihak ketiga. Akses oleh pihak ketiga terhadap fasilitas pemrosesan informasi sebuah organisasi harus dikontrol. Ketika sebuah bisnis membutuhkan akses dari pihak ketiga, sebuah pengujian risiko harus dilakukan untuk menentukan implikasi keamanan

dan kontrol yang perlu dilakukan. Kontrol harus disetujui dan didefinisikan dalam kontrak dengan pihak ketiga.

2.5.3. Asset Management

2.5.3.1. Responsibilities for Assets

Bertujuan untuk memberikan perlindungan yang baik terhadap aset organisasi. Setiap aset informasi utama harus dicatat untuk menjamin perlindungan yang sesuai sudah diberikan terhadap aset tersebut. Pemilik harus mengidentifikasikan setiap aset utama dan tanggung jawab perawatannya.

2.5.3.2. Information classification

Bertujuan untuk menjamin aset informasi mendapatkan perlindungan yang sesuai. Informasi harus diklasifikasikan untuk mengindikasikan kebutuhan, prioritas dan tingkat perlindungannya. Informasi memiliki beragam tingkat sensitifitas dan kekritisannya. Beberapa jenis informasi bisa saja membutuhkan perlindungan tambahan atau perlakuan khusus. Klasifikasi informasi harus digunakan untuk mendefinisikan tingkat perlindungan yang sesuai, dan kebutuhan perlakuan khusus.

2.5.4. Human Resource Security

2.5.4.1. Prior to Employment

Bertujuan untuk memastikan bahwa para pegawai, kontraktor, dan pengguna pihak ketiga memahami tanggungjawab mereka, dan sesuai dengan peran yang dipertimbangkan untuk mereka, dan untuk mengurangi resiko pencurian, penipuan, atau penyalahgunaan fasilitas-fasilitas. Tanggungjawab keamanan harus disampaikan sebelum mempekerjakan di dalam rincian kerja yang memadai dan perjanjian dan kondisi-kondisi pengerjaan.

2.5.4.2. During Employment

Bertujuan untuk memastikan bahwa para pegawai, kontraktor, dan pengguna pihak ketiga sadar akan ancaman-ancaman keamanan informasi dan perhatian, tanggungjawab dan pertanggungjawaban mereka, dan

diperlengkapi untuk mendukung kebijakan keamanan organisasi dalam perjalanan pekerjaan normal mereka, dan untuk mengurangi resiko kesalahan manusia.

2.5.4.3. Termination of change of employment

Bertujuan untuk memastikan para pegawai, kontraktor, dan pengguna pihak ketiga meninggalkan organisasi atau pergantian pengerjaan dilakukan dengan cara yang tertib. Tanggungjawab harus ditempatkan untuk memastikan pegawai, kontraktor, atau pengguna pihak ketiga meninggalkan organisasi dikelola, dan pengembalian seluruh perangkat dan penghapusan seluruh hak akses diselesaikan.

2.5.5. Physical and Environmental Security

2.5.5.1. Secure Areas

Bertujuan untuk mencegah akses fisik yang tidak teraoutorisasi, kerusakan, dan interferensi pada gedung dan informasi organisasi.

2.5.5.2. Equipment security

Bertujuan untuk mencegah, kerugian, kerusakan, pencurian, atau kompromi pada aset-aset dan interupsi pada aktivitas-aktivitas organisasi. Perangkat harus diproteksi dari ancaman fisik dan lingkungan.

2.5.6. Communication and Operations Management

2.5.6.1. Operational Procedures and responsibilities

Bertujuan untuk menjamin operasi fasilitas pengolahan informasi berjalan dengan benar dan aman. Tanggungjawab dan prosedur untuk pengaturan dan operasi dari semua fasilitas pengolahan informasi harus dibuat. Termasuk pembuatan instruksi operasi dan prosedur penanganan insiden yang sesuai.

2.5.6.2. Third Party Service Delivery Management

Bertujuan untuk menerapkan dan memelihara level yang sesuai dari keamanan informasi dan *service delivery* sejalan dengan perjanjian *service delivery* dengan pihak ketiga. Organisasi harus memeriksa penerapan dari perjanjian, mengawasi kepatuhan pada perjanjian dan mengelola

perubahan untuk memastikan bahwa layanan yang diberikan sesuai dengan seluruh syarat-syarat yang disetujui dengan pihak ketiga.

2.5.6.3. System Planning and Acceptance

Untuk mengurangi risiko kegagalan sistem. Perencanaan yang matang dan persiapan dibutuhkan untuk menjamin ketersediaan kapasitas dan sumber daya yang cukup. Proyek dari kebutuhan kapasitas di masa mendatang harus dibuat, untuk mengurangi risiko dari sistem yang kelebihan beban, kebutuhan dari sistem baru harus dibuat, didokumentasikan dan dilakukan tes untuk penerimaan dan penggunaan.

2.5.6.4. Protection against Malicious and Mobile Code

Bertujuan untuk menjaga integritas dari *software* dan informasi. Pencegahan dibutuhkan untuk mencegah dan mendeteksi adanya *malicious software. Software* dan fasilitas pengolahan informasi rawan terhadap *malicious software*, seperti virus komputer, *network worms, trojan horses,* dan *logic bomb.* Pengguna harus dibuat waspada terhadap *malicious software* dan ketika diperlukan manajer harus mengenalkan kontrol khusus untuk mendeteksi dan mencegah datangnya *malicious software* tersebut. Terutama sangat penting melakukan antisipasi untuk mendeteksi dan mecegah virus di komputer.

2.5.6.5. Back-Up

Bertujuan untuk menjaga integritas dan ketersediaan dari pengolahan informasi dan layanan komunikasi. Prosedur rutin harus dibuat untuk menjalankan strategi *backup* yang disetujui, mengambil salinan data yang di-*backup* dan mengulangi restorasi, mencatat kejadian-kejadian dan kesalahan dan ketika dibutuhkan mengawasi lingkungan peralatan.

2.5.6.6. Network Security Management

Bertujuan untuk menjamin perlindungan terhadap informasi di jaringan dan perlindungan terhadap infrastruktur pendukung. Manajemen keamanan jaringan yang dapat merentangkan batasan-batasan organisasi membutuhkan perhatian khusus. Kontrol tambahan dapat juga dibutuhkan untuk melindungi data-data yang sensitif yang lewat melalui jaringan publik.

2.5.6.7. Media Handling

Bertujuan untuk mencegah kerusakan aset dan berhentinya aktifitas bisnis. Media harus dikontrol dan dilindungi secara fisik. Prosedur operasi yang sesuai harus dibuat untuk melindungi dokumen, media komputer, data yang keluar masuk dan dokumentasi sistem dari kerusakan, pencurian, dan akses yang tidak sah.

2.5.6.8. Exchange of Information

Bertujuan untuk mencegah kehilangan, modifikasi atau penyalahgunaan dari pertukaran informasi antar organisasi. Pertukaran informasi dan *software* antara organisasi harus dikontrol, dan harus sesuai dengan aturan yang relevan. Pertukaran harus dilakukan berdasarkan kesepakatan. Prosedur dan standar untuk melindungi informasi dan media dalam pengiriman harus dibuat. Implikasi bisnis dan keamanan yang berhubungan dengan EDI (*electronic data interchange), electronic commerce,* dan *e-mail* harus dikontrol.

2.5.6.9. Electronic Commerce Services

Bertujuan untuk memastikan keamanan layanan *electronic commerce* dan penggunaan keamanannya. Implikasi keamanan ini berhubungan dengan penggunaan layanan *electronic commerce*, termasuk transaksi-transaksi *on-line*, dan syarat-syarat untuk pengontrolan harus dipertimbangkan. Integritas dan ketersediaan informasi secara elektronik yang dipublikasikan melalui sistem yang tersedia untuk umum harus dipertimbangkan.

2.5.6.10. Monitoring

Bertujuan untuk mendeteksi aktivitas-aktivitas pemrosesan informasi yang tidak terautorisasi. Sistem harus dimonitor dan kejadian keamanan informasi harus dicatat. Log-log operator dan *fault logging* harus digunakan untuk memastikan masalah-masalah sistem informasi teridentifikasi. Suatu organisasi harus patuh dengan seluruh syarat-syarat legal yang relevan yang bisa diterapkan untuk pengawasannya dan pencatatan aktivitas-aktivitas.

2.5.7. Access Control

2.5.7.1. Business Requirement for Access Control

Bertujuan untuk mengontrol akses terhadap informasi. Akses terhadap informasi dan proses bisnis harus dikontrol dengan dasar kebutuhan bisnis dan keamanan.

2.5.7.2. User Access Management

Bertujuan untuk mencegah akses yang tidak sah ke dalam sistem informasi. Prosedur formal harus ditempatkan untuk mengontrol alokasi hak akses terhadap sistem informasi dan layanan. Prosedur tersebut harus mencakup semua tingkat dari siklus hidup akses pengguna, mulai dari pendaftaran pengguna baru sampai deregistrasi pengguna yang tidak lagi membutuhakan akses ke dalam sistem informasi dan layanan. Perhatian khusus perlu diberikan untuk mengontrol hak akses khusus yang memungkinkan seorang pengguna untuk mengambil alih kontrol sistem.

2.5.7.3. User Responsibilities

Bertujuan untuk mencegah akses pengguna yang tidak sah. Kerjasama dari pengguna yang sah sangat penting untuk keefektifan keamanan. Pengguna harus disadarkan terhadap tanggung jawabnya untuk menjaga kontrol akses yang efektif, terutama yang berkaitan dengan penggunaan *password* dan keamanan perangkat pengguna.

2.5.7.4. Network Access control

Bertujuan untuk mengamankan layanan yang terhubung dengan jaringan. Akses terhadap layanan yang terhubung jaringan baik itu internal maupun eksternal harus dikontrol. Hal ini perlu untuk memastikan bahwa pengguna yang memiliki akses ke dalam jaringan dan layanan jaringan tidak mengkompromikan keamanan dari jaringan tersebut dengan cara menjamin:

- Interface yang sesuai antar jaringan di organisasi dan jaringan yang dimiliki oleh organisasi lain atau jaringan publik.
- Mekanisme otentikasi yang sesuai untuk pengguna dan perangkat.
- Kontrol terhadap akses pengguna ke dalam sistem informasi.

2.5.7.5. Operating System Access Control

Bertujuan untuk mencegah akses yang tidak sah ke dalam sistem komputer. Fasilitas keamanan pada level sistem operasi harus digunakan untuk membatasi akses ke sumber daya komputer. Fasilitas ini harus mampu untuk melakukan hal-hal sebagai berikut:

- Mengidentifikasi dan mengecek ulang identitas dan jika perlu letak terminal dan lokasi dari setiap pengguna yang sah.
- Mencatat akses ke dalam sistem, baik yang sukses dan gagal.
- Menyediakan otektikasi yang sesuai, apabila sistem manajemen *password* digunakan, sistem tersebut harus menjamin *password* yang baik.
- Membatasi waktu akses dari pengguna, ketika dibutuhkan.

2.5.7.6. Application access control

Bertujuan untuk mencegah akses tidak sah terhadap informasi yang disimpan dalam sistem informasi. Fasilitas keamanan harus bisa digunakan untuk membatasi akses dalam sistem aplikasi. Akses lojik ke dalam *software* dan informasi harus dibatasi terhadap pengguna yang sah.

Sistem aplikasi harus:

- Mengontrol akses pengguna terhadap informasi dan fungsi sistem aplikasi, sesuai dengan kebijakan akses kontrol bisnis.
- Menyediakan perlindungan dari akses yang tidak sah terhadah utiliti dan *software* sistem operasi yang mampu untuk mengambil alih sistem atau kontrol aplikasi.
- Tidak mengancam keamaman dari sistem yang lain yang menggunakan bersama-sama sumber daya informasi.
- Dapat menyediakan akses informasi khusus kepada pemilik, atau sekumpulan pengguna tertentu.

2.5.7.7. Mobile Computing and Teleworking

Bertujuan untuk menjamin kemanan informasi ketika menggunakan fasilitas *mobile computing* dan *teleworking*. Perlindungan yang diperlukan harus seimbang dengan risiko yang ditimbulkan dari cara kerja ini. Ketika menggunakan *mobile computing*, risiko bekerja dalam lingkungan yang

tidak terlindungi harus dipertimbangkan dan perlindungan yang sesuai harus diterapkan. Pada kasus *teleworking*, organisasi tersebut harus mengaplikasikan perlindungan terhadap tempat *teleworking* dan menjamin pengaturan yang sesuai dilakukan untuk cara kerja ini.

2.5.8. Information Systems Acquisition Development and Maintenance

2.5.8.1. Security Requirements of Information Systems

Bertujuan untuk menjamin bahwa keamanan dibangun di dalam system informasi. Hal ini termasuk infrastruktur, aplikasi bisnis, dan aplikasi yang dibangun oleh pengguna. Desain dan implementasi dari proses bisnis yang mendukung aplikasi atau layanan dapat bersifat vital untuk keamanan. Kebutuhan keamanan harus diidentifikasi dan disetujui dalam pembangunan sistem informasi.

2.5.8.2. Correct Processing in Applications

Bertujuan untuk mencegah kehilangan, modifikasi atau penyalahgunaan data pengguna dalam sistem aplikasi. Kontrol yang sesuai dan catatan audit harus dirancang ke dalam sistem aplikasi, termasuk aplikasi yang ditulis oleh pengguna. Hal ini seharusnya termasuk validasi dari input data, pengolahan internal dan keluaran data.

2.5.8.3. Cryptographic controls

Bertujuan untuk menjaga kerahasiaan, otentikasi dan integritas dari informasi. Sistem dan teknik kriptografi harus digunakan untuk pengamanan informasi yang dianggap berada dalam risiko dan juga untuk yang tidak mendapatkan perlindungan cukup.

2.5.8.4. Security of System Files

Bertujuan untuk menjamin bahwa proyek teknologi informasi dan aktifitas pendukungnya dilakukan dengan memperhatikan faktor keamanan. Akses ke *file-file* pada sistem harus dikontrol. Memelihara integritas sistem harus menjadi tanggung jawab dari fungsi pengguna atau grup pengembang yang memiliki sistem aplikasi atau *software.*

2.5.8.5. Security in Development and Support Processes

Bertujuan untuk memelihara keamanan dari *software* sistem aplikasi dan informasi. Proyek dan lingkungan pendukungnya harus dikontrol secara ketat. Para manajer yang bertanggung jawab terhadap sistem aplikasi harus juga bertanggung jawab terhadap keamanan proyek dan lingkungan pendukungnya. Mereka harus menjamin bahwa semua perubahan sistem yang diajukan sudah diperiksa dan dicek, supaya tidak terjadi pelanggaran keamanan pada sistem atau lingkungan operasi.

2.5.8.6. Technical Vulnerability Management

Bertujuan untuk mengurangi resiko yang dihasilkan exploitasi *vulnerabilities* teknis yang terpublikasi. Manajemen *vulnerabilities* teknikal harus diterapkan dengan efektif, sistematik, dan berulang-ulang dimana pengukuran yang dilakukan untuk menguji keefektipannya.

2.5.9. Information Security Incident Management

2.5.9.1. Reporting Information Security Events and Weaknesses

Bertujuan untuk memastikan kejadian-kejadian keamanan informasi dan kelemahan yang terkait dengan sistem informasi dikomunikasikan dengan cara yang memperbolehkan tindakan perbaikan tepat waktu dilakukan.

2.5.9.2. Management of Information Security Incidents and Improvements

Bertujuan untuk memastikan pendekatan yang konsisten dan efektif diterapkan pada manajemen kejadian-kejadian keamanan informasi. Tanggungjawab dan prosedur-prosedur harus ditempatkan untuk menangani kejadian-kejadian keamanan informasi dan kelemahan-kelemahan secara efektif ketika hal tersebut dilaporkan.

2.5.10. Business Continuity Management

2.5.10.1. Information Security Aspects of Business Continuity Management

Bertujuan untuk mengantisipasi berhentinya aktifitas bisnis dan untuk melindungi proses bisnis yang kritis dari efek bencana atau kesalahan yang

besar. Sebuah proses manajemen kelangsungan bisnis harus diimplementasikan untuk mengurangi gangguan yang diakibatkan oleh bencana dan kegagalan keamanan sampai ke level yang merupakan kombinasi dari pencegahan dan kontrol pemulihan. Konsekuensi dari bencana, kegagalan keamanan dan hilangnya layanan harus dianalisa. Rencana pemulihan harus dibangun dan diimplementasikan untuk menjamin bahwa proses bisnis dapat dipulihkan dalam waktu yang singkat. Rencana ini harus dipelihara dan dilatih, sehingga menjadi bagian integral dari semua proses manajemen. Manajemen kelangsungan bisnis harus meliputi kontrol untuk mengidentifikasikan dan mengurangi resiko, membatasi konsekuensi dari insiden yang merusak, dan menjamin pemulihan operasi berjalan tepat waktu.

2.5.11. Compliance

2.5.11.1. Compliance with Legal Requirements

Bertujuan untuk mencegah pelanggaran terhadap hukum pidana dan hukum perdata, regulasi dan obligasi kontrak serta kebutuhan keamanan. Perancangan, operasi, penggunaan, dan manajemen sistem informasi harus mengikuti hukum, regulasi, dan kebutuhan dari kontrak keamanan. Saran pada kebutuhan hukum tertentu harus dicari dari penasehat hukum organisasi atau pratisi hukum yang memiliki kualifikasi.

2.5.11.2. Compliance with Security Policies and Standards and Technical compliance

Bertujuan untuk menjamin kesesuaian dari sistem dengan kebijakan dan standar keamanan organisasi. Keamanan sistem informasi harus diperiksa secara berkala. Pemeriksaan ini harus dilakukan sesuai dengan kebijakan keamanan dan *platform* teknis dan sistem informasi harus diaudit untuk kesesuaian dengan standar implementasi keamanan.

BAB 4
PROFIL ORGANISASI

4.1. SEKILAS PANDANG ORGANISASI

Departemen Komunikasi dan Informatika (Depkominfo) terbentuk tahun 2005, sebelumnya merupakan Kementerian Komunikasi dan Informasi. Sesuai dengan Perpres RI No. 9 Tahun 2005 Depkominfo bertugas melaksanakan urusan pemerintahan di bidang komunikasi dan informatika. Depkominfo berada di bawah Kementerian Koordinator bidang Perekonomian.

Semboyan Depkominfo adalah "Menuju Masyarakat Informasi Indonesia".

4.2. VISI

Visi Depkominfo adalah:

"Terwujudnya masyarakat informasi yang sejahtera melalui penyelenggaraan komunikasi dan informatika yang efektif dan efisien dalam kerangka Negara Kesatuan Republik Indonesia."

4.3. MISI

Misi Depkominfo adalah:

1. Meningkatkan kapasitas layanan informasi dan pemberdayaan potensi masyarakat dalam rangka mewujudkan masyarakat berbudaya informasi.
2. Meningkatkan daya jangkau infrastruktur pos, komunikasi dan informatika untuk memperluas aksesibilitas masyarakat terhadap informasi dalam rangka mengurangi kesenjangan informasi.
3. Mendorong peningkatan aplikasi layanan publik dan industri aplikasi telematika dalam rangka meningkatkan nilai tambah layanan dan industri aplikasi.

4. Mengembangkan standardisasi dan sertifikasi dalam rangka menciptakan iklim usaha yang konstruktif dan kondusif di bidang industri komunikasi dan informatika.
5. Meningkatkan kerjasama dan kemitraan serta pemberdayaan lembaga komunikasi dan informatika pemerintah dan masyarakat.
6. Mendorong peranan media massa dalam rangka meningkatkan informasi yang beretika dan bertanggung jawab serta memberikan nilai tambah pembangunan bangsa.
7. Meningkatkan kualitas penelitian dan pengembangan dalam rangka menciptakan kemandirian dan daya saing bidang komunikasi dan informatika.
8. Meningkatkan kapasitas Sumber Daya Manusia (SDM) bidang komunikasi dan informatika dalam rangka meningkatkan literasi dan profesionalisme.
9. Meningkatkan peran serta aktif Indonesia dalam berbagai forum internasional di bidang komunikasi dan informatika dalam rangka meningkatkan citra positif bangsa dan negara.
10. Meningkatkan kualitas pengawasan menuju terselenggaranya kepemerintahan yang baik *(good governance)*.

4.4. TUGAS POKOK DAN FUNGSI

Tugas & Fungsi Departemen Komunikasi dan Informatika adalah sebagai berikut:

Tugas :

Membantu Presiden dalam menyelenggarakan sebagian urusan pemerintahan di bidang komunikasi dan informatika.

Fungsi :

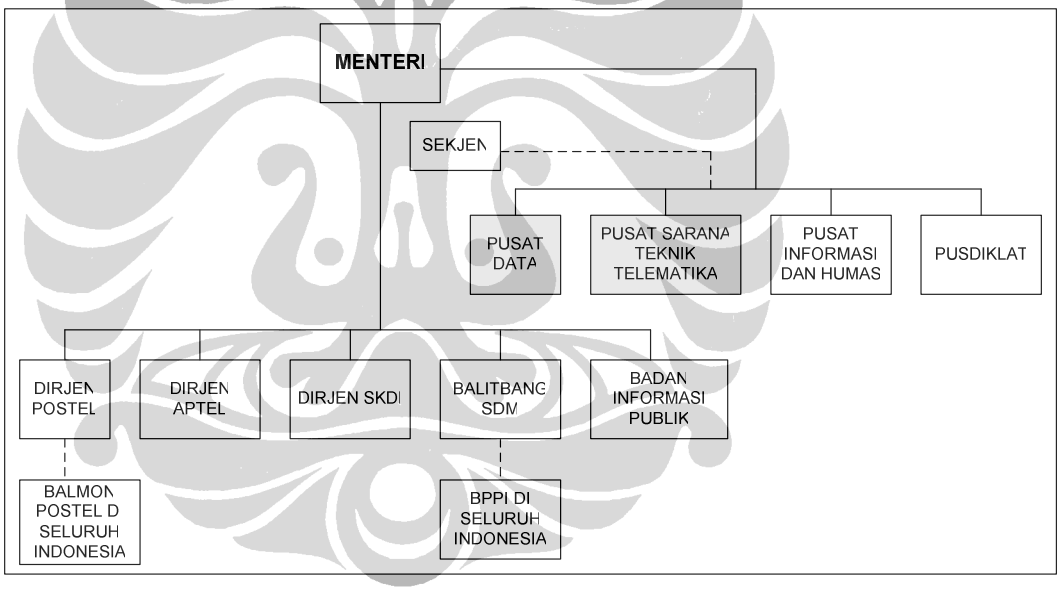
1. Perumusan kebijakan nasional, kebijakan pelaksanaan, dan kebijakan teknis di bidang komunikasi dan informatika yang meliputi pos,

telekomunikasi, penyiaran, teknologi informasi dan komunikasi, layanan multimedia dan diseminasi informasi.

2. Pelaksanaan urusan pemerintahan sesuai dengan bidang tugasnya.
3. Pengelolaan barang milik/kekayaan negara yang menjadi tanggung-jawabnya.
4. Pengawasan atas pelaksanaan tugasnya.
5. Penyampaian hasil evaluasi, saran, dan pertimbangan di bidang tugas dan fungsinya kepada Presiden.

4.5. STRUKTUR ORGANISASI

Berikut adalah gambar struktur organisasi Depkominfo:



Gambar 4.1. Struktur Organisasi Depkominfo

Selain unit dan satuan kerja pada Gambar 4.1, Depkominfo memiliki Unit Pelayanan Teknis (UPT) sebagai perpanjangan tangan untuk melakukan tupoksi Depkominfo. UPT tersebut adalah:

- BPPI (Balai Pengkajian dan Pengembangan Informasi)
- Balmon (Balai Monitoring) spektrum frekuensi radio dan orbit satelit

UPT-UPT ini tersebar di seluruh Indonesia, dan rencananya seluruh UPT akan terhubung secara *online* dengan kantor Pusat Depkominfo di Jakarta.

4.6. STRUKTUR ORGANISASI UNIT TI

Dari Gambar 4.1, ada dua unit kerja di bawah Sekjen yang menangani TI di lingkungan Depkominfo, yaitu: Pusat Data dan Pusat Sarana Teknik Telematika.

4.6.1. Pusat Data (Pusdat)

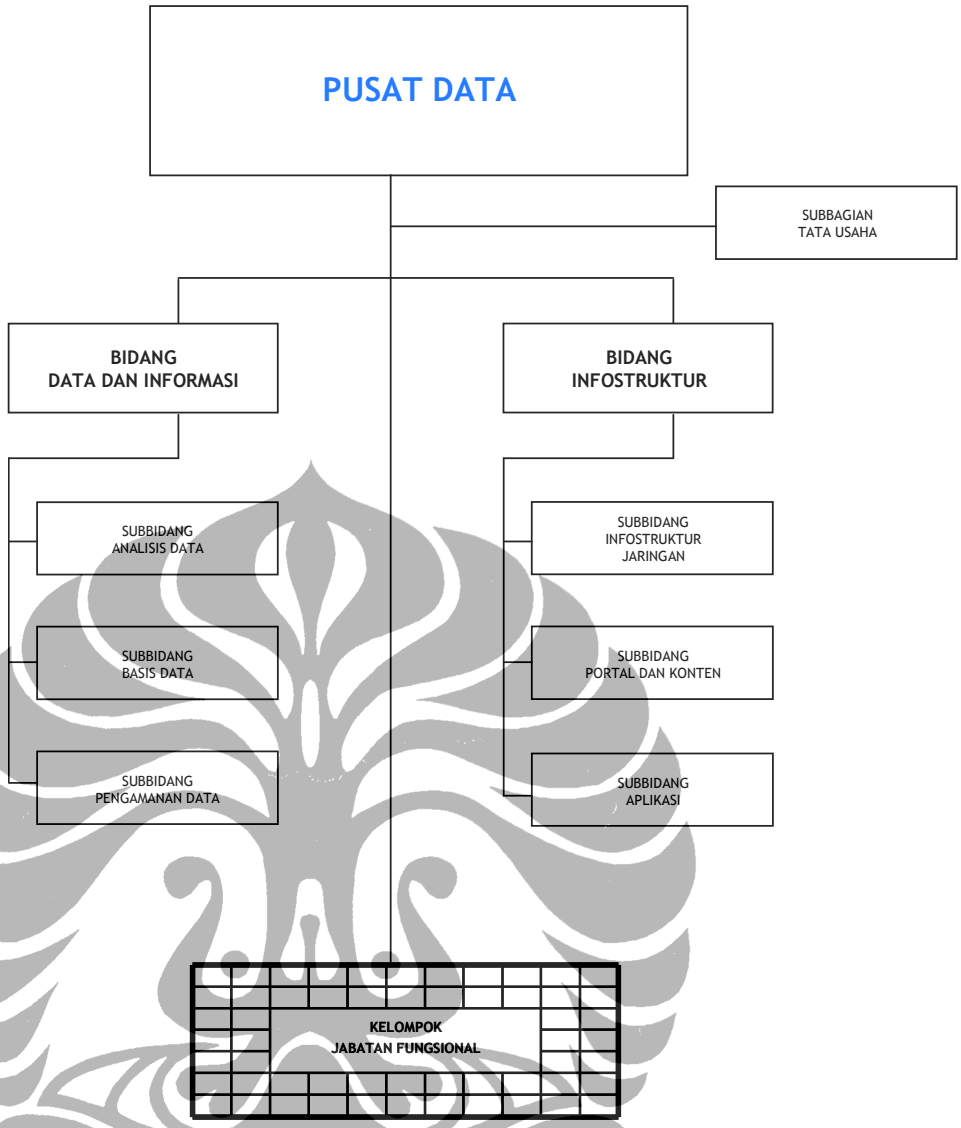
Sesuai dengan Permen Kominfo No. 25 Tahun 2008, Pusat Data adalah unsur pelaksana tugas tertentu departemen berada di bawah serta bertanggung jawab kepada Menteri melalui Sekretaris Jenderal.

Pusat Data mempunyai tugas melaksanakan layanan pengelolaan, pengembangan dan pemanfaatan data departemen berdasarkan kebijakan yang ditetapkan oleh Menteri.

Pusat Data menyelenggarakan fungsi:

1. Pelayanan, penyediaan dan pengelolaan sistem jaringan komunikasi data, analisis data dan sistem informasi departemen;
2. Pelayanan, pemeliharaan dan pengembangan sistem jaringan komunikasi data, serta pengelolaan data dan pelayanan sistem informasi departemen;
3. Pelaksanaan urusan tata usaha pusat.

Adapun struktur organisasi Pusat Data adalah seperti pada Gambar 4.2. dari gambar tersebut, di bawah Bidang Data dan Informasi terdapat Subbidang Pengamanan Data yang mempunyai tugas melakukan penyiapan bahan sistem pengamanan dan pengorganisasian data.



Gambar 4.2. Struktur Organisasi Pusat Data

4.6.2. Pusat Sarana Teknik Telematika (Pusteka)

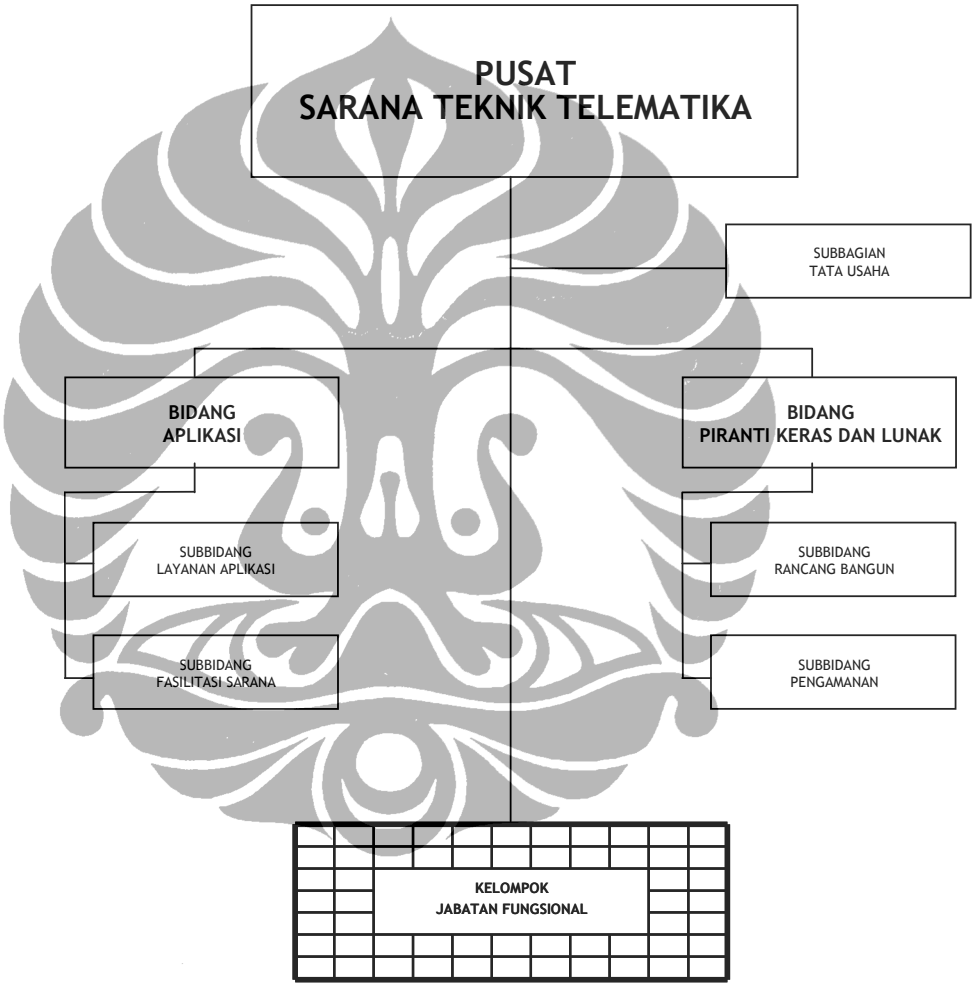
Berdasarkan Permen Kominfo No. 25 Tahun 2008, Pusat Sarana Teknik Telematika adalah unsur pelaksana tugas tertentu departemen berada di bawah serta bertanggung jawab kepada Menteri melalui Sekretaris Jenderal.

Pusat Sarana Teknik Telematika mempunyai tugas melaksanakan layanan pengelolaan, pengembangan dan pemanfaatan sarana teknik telematika departemen berdasarkan kebijakan yang ditetapkan oleh Menteri.

Pusat Sarana Teknik Telematika menyelenggarakan fungsi:

1. Pelayanan aplikasi *interface* dan fasilitasi sarana teknik telematika;
2. Pelayanan dan pengembangan sistem jaringan *interface* dan piranti keras telematika;
3. Pelaksanaan urusan ketatausahaan pusat.

Adapun struktur organisasi Pusat Sarana Teknik Telematika adalah seperti pada Gambar 4.3.



Gambar 4.3. Struktur Organisasi Pusat Sarana Teknik Telematika

Dari struktur organisasi tersebut (Gambar 4.3), di bawah Bidang Piranti Keras dan Lunak terdapat Subbidang Pengamanan yang mempunyai tugas melakukan penyiapan bahan fasilitasi dan advokasi pengamanan sarana teknik telematika.

Dari struktur organisasi Pusat Data dan Pusat Sarana Teknik Telematika, Keamanan Informasi di lingkungan Depkominfo ditangani bersama-sama oleh Pusat Sarana Teknik Telematika melalui Subbidang Pengamanan Data (Pusat Data) dan Pusat Data melalui Subbidang Pengamanan.