Modul 6: Keamanan Jaringan dan Keamanan Informasi dan Privasi

Sesi 0: Gambaran Modul 6
dan
Sesi 1: Kebutuhan Keamanan Informasi, Memahami Tren Keamanan Informasi, dan Meningkatkan Keamanan

Pemikiran

Apakah isi Modul 6 dan kepada siapa ditujukan?

- Target Peserta
  - Pembuat kebijakan dan pejabat pemerintah sehingga mereka memahami isu-isu terkait keamanan informasi
- Penekanan Utama
  - Gambaran kebutuhan keamanan informasi
  - Isu-isu dan tren keamanan informasi
  - Formulasi strategi keamanan informasi

Struktur Modul

Modul 6 terdiri dari 6 sesi:

- Sesi 1: Kebutuhan Keamanan Informasi, Tren Keamanan Informasi, dan Peningkatan Keamanan
- Sesi 2: Aktivitas Keamanan Informasi
- Sesi 3: Metodologi Keamanan Informasi
- Sesi 4: Perlindungan Privasi
- Sesi 5: Pembentukan Dan Operasi CSIRT
- Sesi 6: Daur Hidup Kebijakan Keamanan Informasi

Modul 6:
Keamanan Jaringan dan Keamanan Informasi dan Privasi

Sesi 1: Kebutuhan Keamanan Informasi, Tren Keamanan Informasi, dan Peningkatan Keamanan

Tujuan Pembelajaran

- Memahami konsep informasi dan keamanan informasi, dan mengenali kebutuhan akan keamanan informasi
- Memahami domain keamanan informasi dan mana saja yang ditekankan di standar internasional
- Mengenali target serangan dengan memahami tren terkini dalam ancaman keamanan
- Mengenali metode-metode yang ada untuk menghadapi ancaman

Konsep Informasi

- **Apakah informasi?**

Dari perspektif Keamanan Informasi

- Informasi diartikan sebagai sebuah ‘aset’; merupakan sesuatu yang memiliki **nilai** dan karenanya harus dilindungi
- **Nilai** secara intrinsik melibatkan subyektivitas yang membutuhkan penilaian dan pengambilan keputusan
- Oleh karena itu:

Keamanan adalah ilmu pengetahuan dan seni.

Konsep Informasi

Nilai Informasi

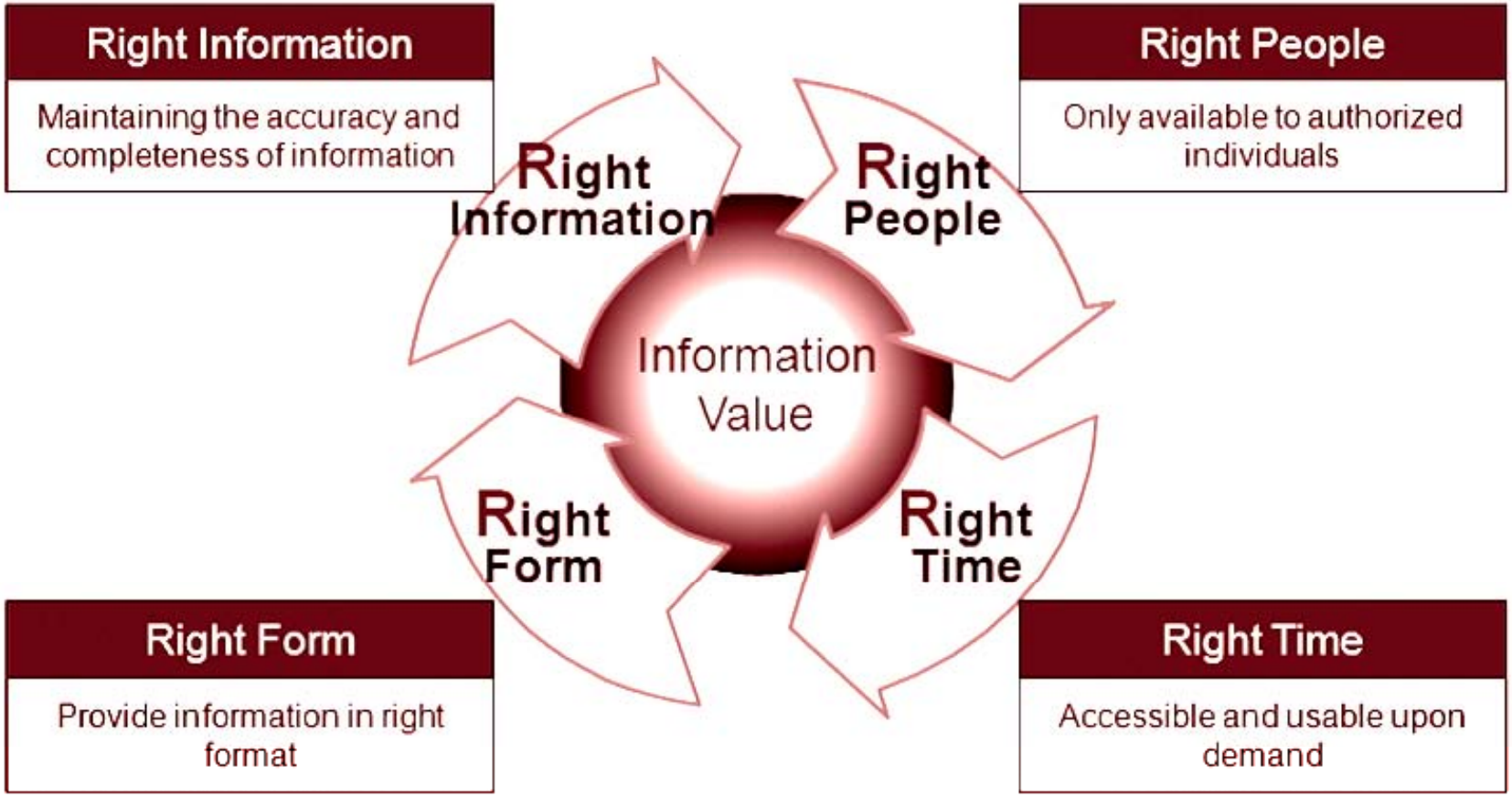
Karakteristik	Aset informasi	Aset nyata
Bentuk-pemeliharaan	Tidak memiliki bentuk fisik dan bersifat fleksibel	Memiliki bentuk fisik
Variabel nilai	Bernilai lebih tinggi ketika digabung dan diproses	Total nilai adalah jumlah dari tiap nilai
Berbagi	Reproduksi yang tak terbatas, dan orang-orang dapat berbagi nilainya	Reproduksi tidak mungkin; dengan reproduksi, nilai aset berkurang
Ketergantungan-medium	Perlu disampaikan melalui medium	Dapat disampaikan secara independen (karena bentuk fisiknya)

Konsep Informasi

- **Risiko terhadap aset informasi**
- Peningkatan perilaku tidak etis yang timbul dari anonimitas
  - TIK dapat digunakan untuk memelihara anonimitas, yang mempermudah seseorang untuk melakukan tindakan tidak etis dan kriminal, termasuk perolehan informasi secara ilegal
- Konflik kepemilikan dan kontrol informasi
- Kesenjangan informasi dan kesejahteraan diantara kelas dan negara
- Pertumbuhan keterbukaan informasi disebabkan oleh majunya jaringan
  - Kelemahan satu bagian jaringan dapat berakibat buruk pada bagian lain

Konsep Informasi

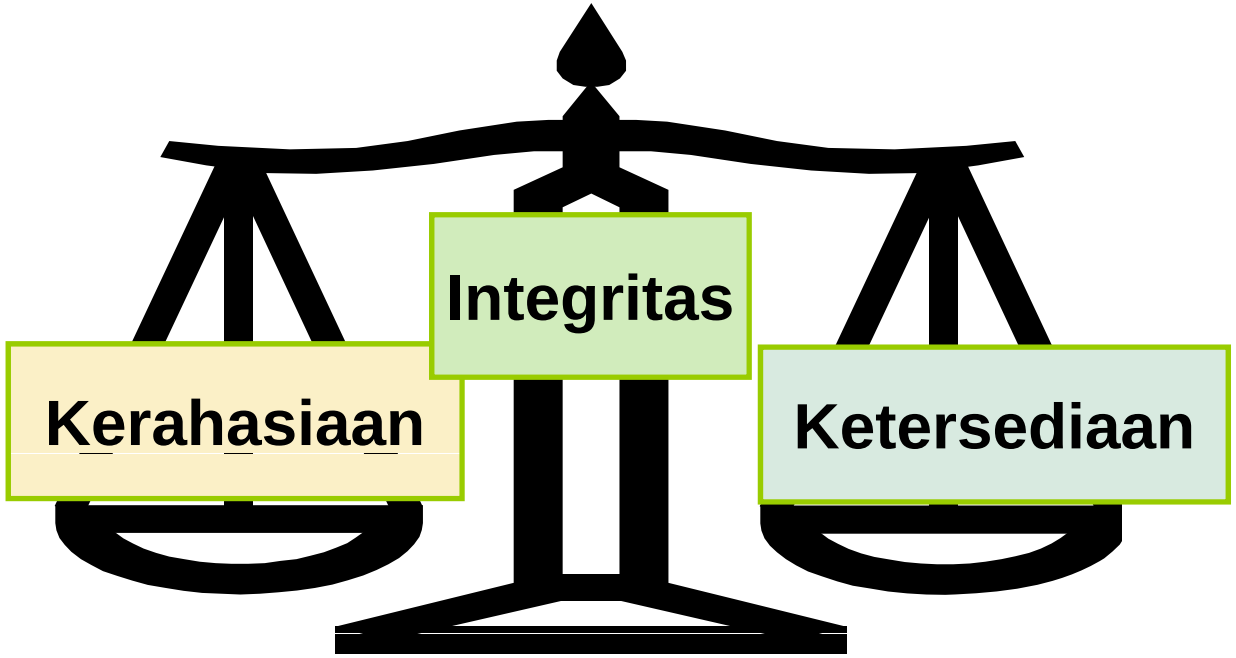
➢ 4R keamanan informasi



Konsep Informasi

➢ Penerapan Keamanan Informasi

- ❖ Cara menerapkan 4R adalah dengan menjamin **kerahasiaan**, **integritas**, dan **ketersediaan.**



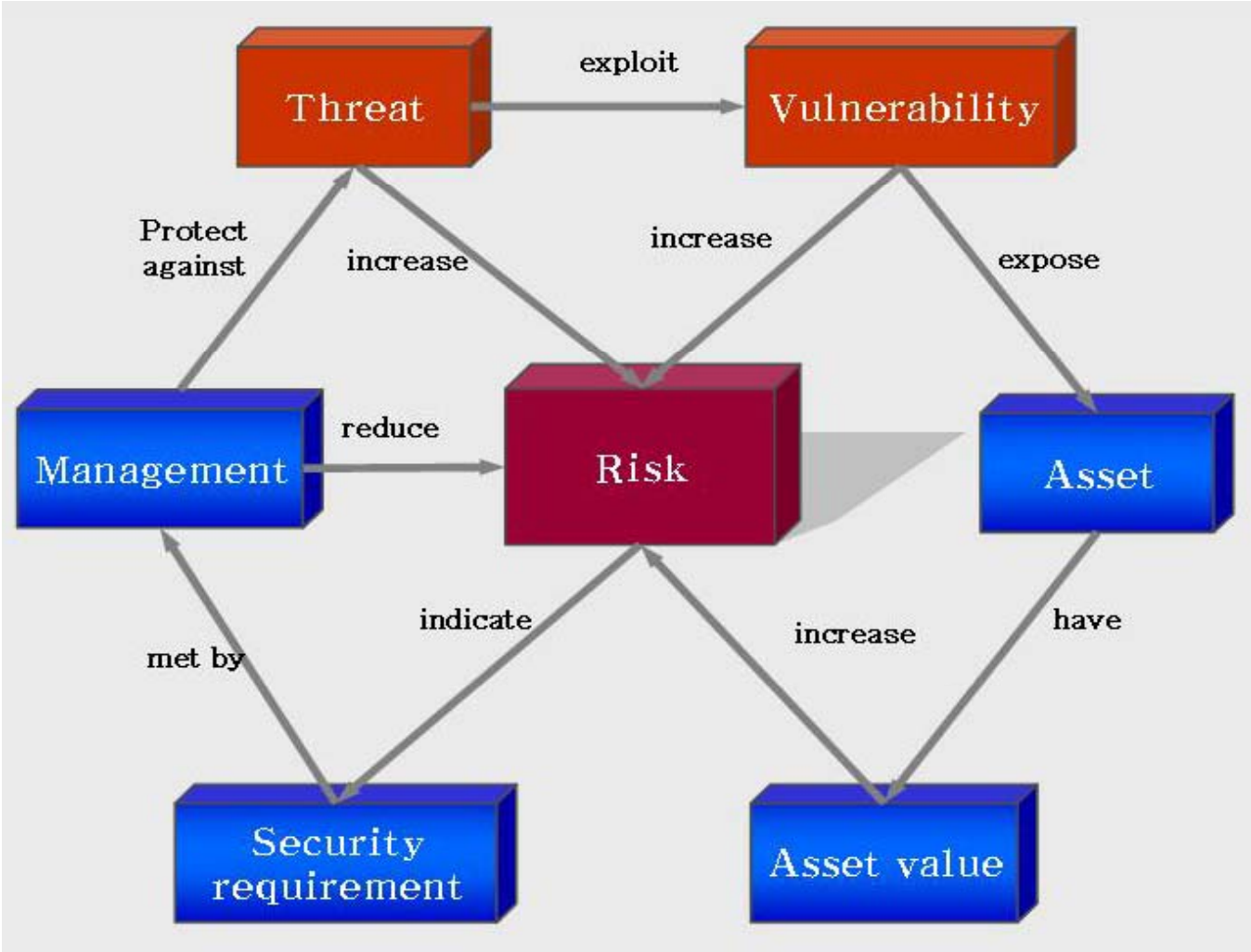
Konsep Informasi

➢ Karakteristik Keamanan Informasi

Kerahasiaan	Menjamin informasi tidak dibuat tersedia atau terbuka untuk individu, entitas, atau proses yang tidak berwenang.
Integritas	Integritas menjaga akurasi dan kelengkapan aset-aset.
Ketersediaan	Menjamin bahwa informasi dapat diakses dan digunakan oleh entitas yang berwenang ketika dibutuhkan.

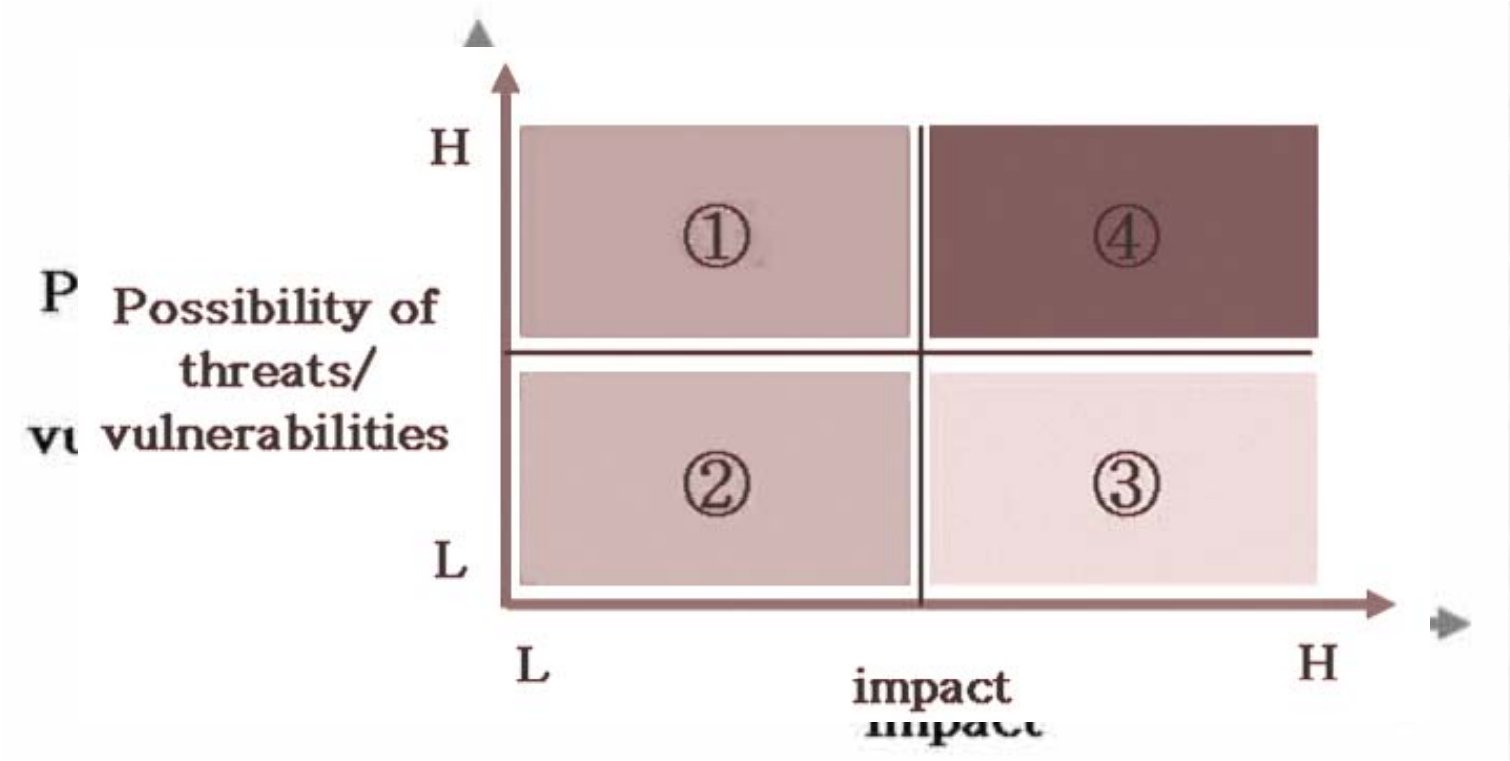
Konsep Informasi

- **Hubungan antara Risiko dan Aset Informasi**



Konsep Informasi

- **Metode-metode manajemen risiko**



Standar Kegiatan Keamanan Informasi

- **ISO [International Standards Organization]**

  ISO/IEC27001 disusun oleh ISO/IEC dan fokus kepada keamanan administratif

- **CISA [Certified Information Systems Auditor]**

  CISA fokus pada kegiatan audit dan pengendalian sistem informasi

- **CISSP [Certified Information Systems Security Professional]**

  CISSP fokus utamanya pada keamanan teknis

Tren Ancaman Keamanan Informasi

Analisis tren ancaman keamanan

- Analisis tren ancaman keamanan dapat dipahami sebagai pencarian pola untuk mengidentifikasi bagaimana ancaman keamanan berubah dan berkembang.

Proses Analisis Tren Keamanan:

- Penetapan pola dasar
- Deteksi perubahan pola – sebuah anomali atau penyimpangan dari norma
- Menentukan spesifikasi dari anomali

Tren Ancaman Keamanan Informasi

Otomasi alat penyerangan

- Saat ini, penyusup menggunakan alat otomatis untuk mengumpulkan informasi tentang kelemahan sistem atau untuk langsung menyerang.

Alat-alat ini memudahkan membuat serangan:

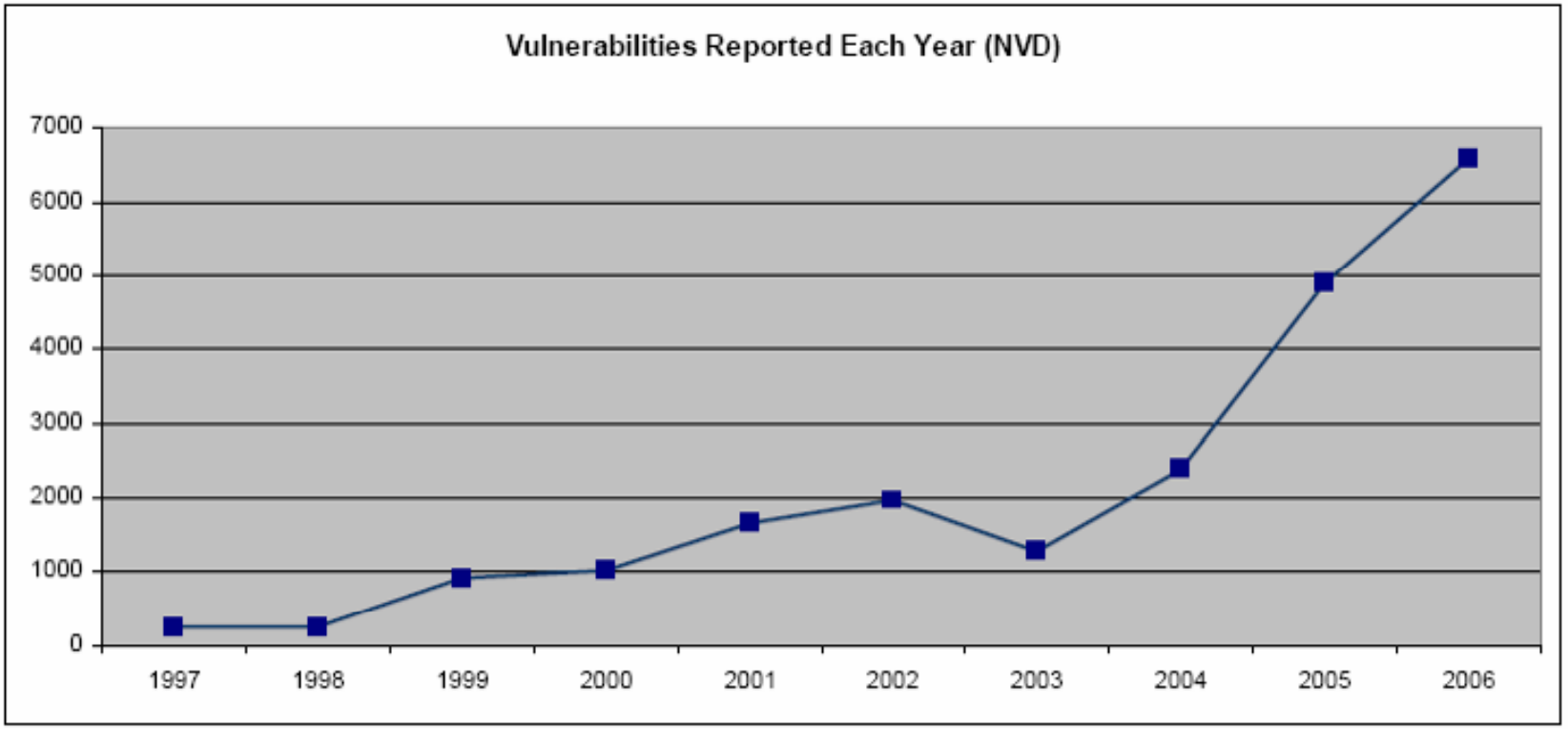
- Bahkan orang yang tidak mempunyai pengetahuan akan teknologi *hacking* dapat melakukan serangan.
- Alat-alat ini mudah digunakan.
- Alat-alat ini menyebabkan kerusakan kritis.

Tren Ancaman Keamanan Informasi

- **Alat penyerangan yang sulit dideteksi**
- Beberapa alat penyerangan menggunakan pola penyerangan baru yang tak terdeteksi oleh alat deteksi saat ini. Sebagai contoh, teknik anti-forensik digunakan untuk menyembunyikan sifat dari alat penyerangan.
- Alat polimorfik berubah bentuk setiap saat digunakan. Beberapa alat ini menggunakan protokol umum seperti *hypertext transfer protocol* (HTTP), sehingga sulit membedakan mereka dari lalu-lintas jaringan normal.

Tren Ancaman Keamanan Informasi

- Penemuan kerentanan yang lebih cepat



❖***Sumber: McAfee***

Tren Ancaman Keamanan Informasi

- **Peningkatan ancaman asimetrik dan konvergensi metode serangan**
  - *Ancaman asimetrik adalah kondisi dimana penyerang memiliki keunggulan terhadap yang bertahan*
  - *Konvergensi metode serangan adalah konsolidasi berbagai metode serangan oleh penyerang untuk menciptakan jaringan global yang mendukung aktivitas pengrusakan terkoordinasi*
  - Sifat asimetrik keamanan meningkatkan kompleksitas dari tantangan keamanan dan pengelolaannya

Tren Ancaman Keamanan Informasi

- **Meningkatnya ancaman dari serangan infrastruktur**

Serangan Infrastruktur

- Ags 2008 – Serangan Internet terhadap Situs *web* Georgia
- Apr 2007 – Serangan *Cyber* terhadap Estonia
- Sep 2005 – Kontroversi Kartun Muhammad (Jyllands-Posten)
- Mei 2005 – Malaysia-Indonesia
- Apr 2001 – Sino-AS

Tren Ancaman Keamanan Informasi

➢ Perubahan tujuan penyerangan

FBI sees rise in computer crime - Security - MSNBC.com - Windows Internet Explorer

http://www.msnbc.msn.com/id/27216425/print/1/displaymode/1098/

MSNBC.com

FBI sees rise in computer crime

Organized crime drawn by ease of reaching millions of potential victims

By Randall Mikkelsen
Reuters
updated 11:21 a.m. ET Oct. 16, 2008

WASHINGTON - Computer spying and theft of personal information have risen notably in
said on Wednesday.

FBI Assistant Director Shawn Henry told reporters that organized-crime groups are draw

He said as many as two dozen countries have taken an "aggressive interest" in penetra

He declined to specify countries, but U.S. intelligence agencies have voiced concern over

As one possible example of Russia's electronic spying prowess, Georgia accused Moscow
it carried out a military offensive.

U.S. federal agents are stepping up efforts to fight computer crime, and working with for
said.

"Over the past year the malicious activity has become much more prevalent," Henry said.

An attack method growing in popularity is "botnets," in which malicious software spreads
data theft or shutting down a system, Henry said.

Another method, "Spearfishing," when hackers get a copy of a company's e-mail list, the
he said.

He said computer crime has invaded Wall Street, but had nothing to do with the current

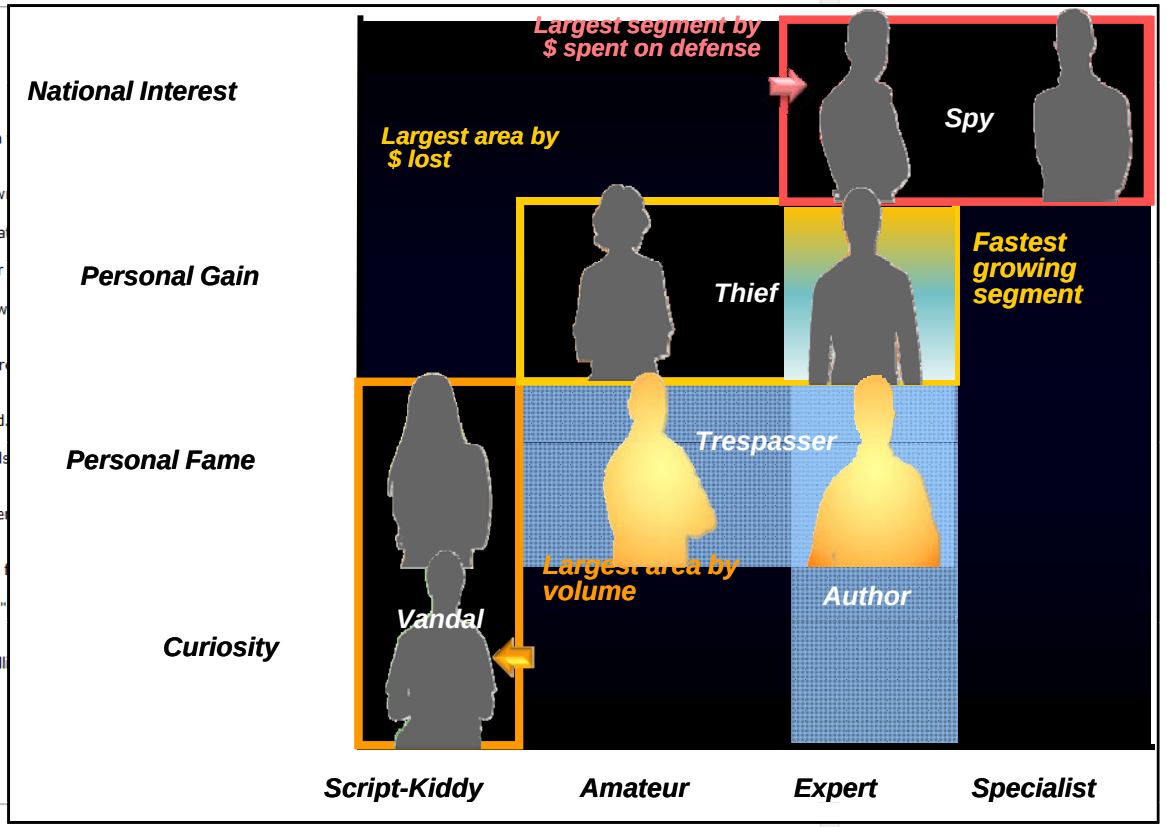
Individual investment companies have, however, lost tens of millions of dollars through "
the price of low-liquidity stocks and dump them from their own accounts.

Internet Crime Complaint Center, which the FBI helps run, has recorded more than 1 mill
Henry said.

Copyright 2008 Reuters. Click for restrictions.

URL: http://www.msnbc.msn.com/id/27216425/

MSN Privacy . Legal
© 2008 MSNBC.com



Jenis-jenis Serangan

- **Hacking**
  - Tindakan memperoleh akses ke komputer atau jaringan komputer untuk mendapatkan atau mengubah infomasi tanpa otorisasi yang sah
  - Dapat dikelompokkan dalam *hacking* 'iseng', kriminal atau politis

Serangan *Hacking*

- Ags 2008 – Serangan Internet terhadap Situs *web* Georgia
- Apr 2007 – Serangan *Cyber* terhadap Estonia
- Sep 2005 – Kontroversi Kartun Muhammad (Jyllands-Posten)
- Mei 2005 – Malaysia-Indonesia
- Apr 2001 – Sino-AS

Jenis-jenis Serangan

Denial of Service

- Serangan *Denial-of-service* (DoS) mencegah pengguna yang sah dari penggunaan layanan ketika pelaku mendapatkan akses tanpa izin ke mesin atau data. Ini terjadi karena pelaku ‘membanjiri’ jaringan dengan volume data yang besar atau sengaja menghabiskan sumber daya yang langka atau terbatas, seperti *process control blocks* atau koneksi jaringan yang tertunda.

Jenis-jenis Serangan

- ***Malicious Code* (Kode Berbahaya)**
  - Program yang menyebabkan kerusakan sistem ketika dijalankan
  - Termasuk *Trojan horse*, virus, dan *worm*

Jenis-jenis Serangan

- ***Social Engineering***
  - Sekumpulan teknik untuk memanipulasi orang sehingga orang tersebut membocorkan informasi rahasia

Peningkatan Keamanan

- **Pengamanan Administratif**
  - Strategi, kebijakan, dan pedoman keamanan informasi
    - ✓Strategi keamanan informasi
    - ✓Kebijakan keamanan informasi
    - ✓Pedoman keamanan informasi
    - ✓Standar keamanan informasi
    - ✓*IT Compliance*

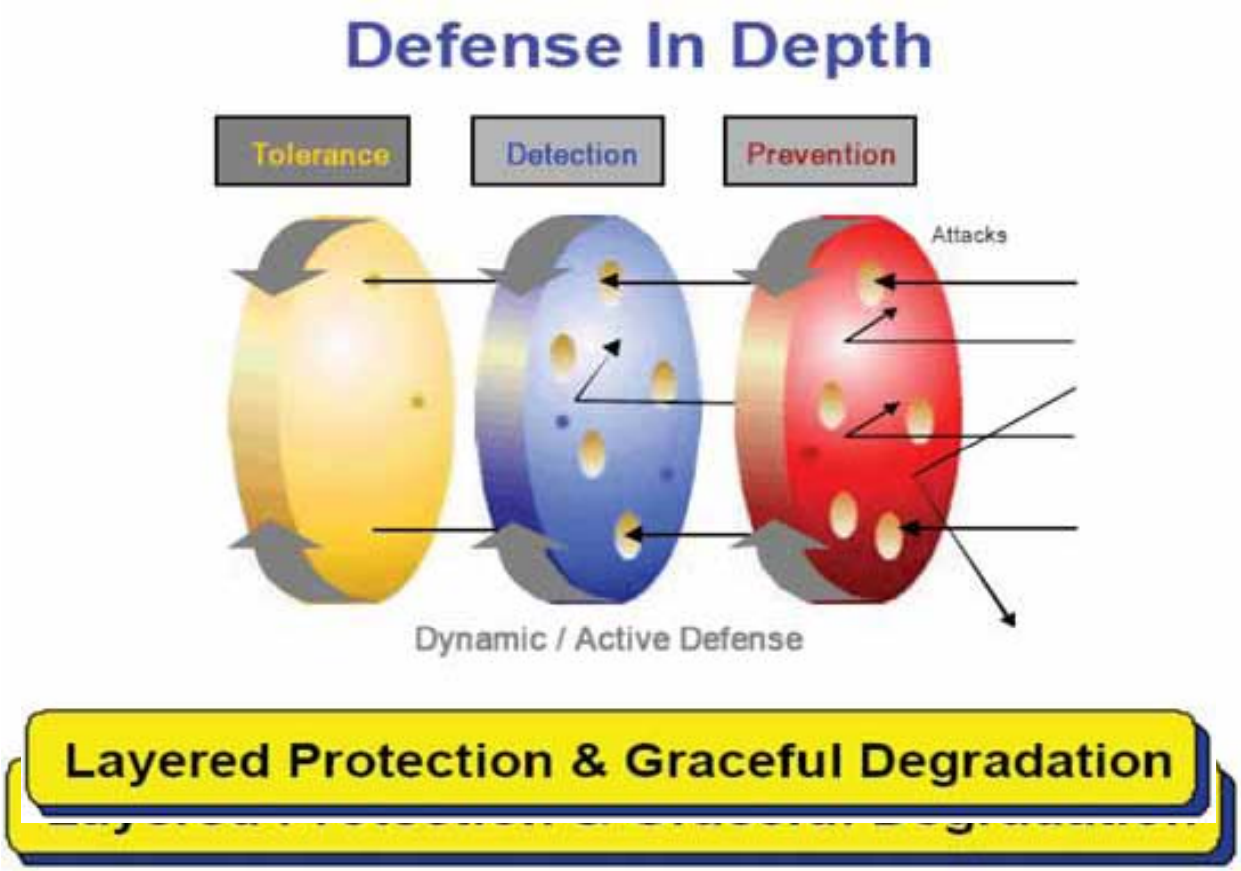
Peningkatan Keamanan

- **Pengamanan Administratif – lanjutan**
  - Proses dan operasi keamanan informasi
    - ✓Program pendidikan dan pelatihan keamanan informasi
    - ✓Penguatan promosi melalui berbagai kegiatan
    - ✓Pengamanan dukungan

Peningkatan Keamanan

➢ Pengamanan dengan Teknologi

- ❖ Model *Defense-in-Depth* (DID)



Peningkatan Keamanan

- **Pengamanan dengan Teknologi**
  - ***Teknologi Pencegah***
    - ✓Kriptografi

      Proses pengkodean informasi dari bentuk aslinya (disebut *plaintext*) menjadi sandi, bentuk yang tidak dapat dipahami
    - ✓*One-Time Passwords* (OTP)

      OTP hanya dapat digunakan sekali. *Password* statis lebih mudah disalahgunakan oleh *password loss*, *password sniffing*, dan *brute-force cracks*, dan sejenisnya. OTP digunakan untuk mencegahnya.

Peningkatan Keamanan

- **Pengamanan dengan Teknologi**
  - ***Teknologi pencegah*** (lanjutan)
    - ✓*Firewall*

      Firewalls mengatur beberapa aliran lalu lintas antara jaringan komputer dari t*rust level* yang berbeda.
    - ✓Alat penganalisis kerentanan

      Ada 3 jenis alat penganalisis kerentanan:
      - Alat penganalisis kerentanan jaringan
      - Alat penganalisis kerentanan *server*
      - Alat penganalisis kerentanan *web*

Peningkatan Keamanan

➢ Pengamanan dengan Teknologi

❖ *Teknologi deteksi*

- ✓ Anti-Virus

  Program komputer untuk mengidentifikasi, menetralisir atau mengeliminasi kode berbahaya

- ✓ IDS (*Intrusion Detection System*)

  IDS mengumpulkan dan menganalisis informasi dari berbagai area dalam sebuah komputer atau jaringan untuk mengidentifikasi kemungkinan penerobosan keamanan

- ✓ IPS (*Intrusion Prevention System*)

  IPS mengidentifikasi potensi ancaman dan bereaksi sebelum mereka digunakan untuk menyerang

Peningkatan Keamanan

➢ Pengamanan dengan Teknologi

❖ *Teknologi terintegrasi*

- ✓ESM (*Enterprise Security Management*)

  Sistem ESM mengatur, mengontrol dan mengoperasikan solusi keamanan informasi seperti IDS dan IPS mengikuti kebijakan yang ditetapkan

- ✓ERM (*Enterprise Risk Management*)

  Sistem ERM adalah membantu memprediksi seluruh risiko yang terkait dengan organisasi, termasuk area di luar keamanan informasi, dan mengatur langkah mengatasinya secara otomatis

Tugas 1

- Nilailah tingkat kesadaran keamanan informasi diantara anggota organisasi Anda.

- Sebutkan langkah-langkah yang diambil oleh organisasi Anda dalam mengimplementasikan keamanan informasi. Klasifikasikan langkah-langkah tersebut ke dalam 4 metode keamanan informasi.

- Temukan contoh langkah keamanan informasi dalam domain administratif, fisik, dan teknis di organisasi Anda atau organisasi lain di negara atau wilayah Anda.

Tugas 2

- Jawablah pertanyaan berikut:
  - Ancaman keamanan informasi apa yang mudah menyerang organisasi Anda? Mengapa?
  - Solusi teknologi keamanan informasi mana yang tersedia di organisasi Anda?
  - Apakah organisasi Anda memiliki kebijakan, strategi dan pedoman keamanan informasi?
    - ✓ Jika ya, seberapa cukupkah hal-hal tersebut terhadap ancaman yang mudah menyerang organisasi Anda?
    - ✓ Jika tidak, apa yang akan Anda rekomendasikan untuk organisasi Anda terkait kebijakan, strategi dan pedoman keamanan informasi?

Modul 6: Keamanan Jaringan dan Keamanan Informasi dan Privasi

Sesi 2: Aktivitas Keamanan Informasi

Tujuan Pembelajaran

- Memahami aktivitas keamanan informasi di AS, UE, Korea dan Jepang

- Memahami aktivitas keamanan informasi dari organisasi internasional dan peran organisasi standar internasional terkait dengan keamanan informasi.

Konten

A. Aktivitas keamanan informasi nasional
   a. *AS*
   b. *UE*
   c. *Republik Korea*
   d. *Jepang*

B. Aktivitas keamanan informasi internasional
   a. Aktivitas keamanan informasi dari organisasi internasional
   b. Organisasi internasional berdasarkan subyek tertentu

Aktivitas Keamanan Informasi Nasional

- **AS**
  - Setelah serangan teroris pada 11 September 2001 (9/11), AS mendirikan *Department of Homeland Security* (DHS) untuk memperkuat keamanan nasional tidak hanya terhadap ancaman fisik tetapi juga terhadap *cyberthreats*. Pada Februari 2003, AS merilis '*National Strategy to Secure Cyberspace*'.
  - AS melakukan aktivitas keamanan informasi yang efektif dan komprehensif melalui sistem *Information Security Officer* (ISO).

Aktivitas Keamanan Informasi Nasional

- Strategi keamanan informasi AS
  - *National Strategy for Homeland Security*
  - *National Strategy for the Physical Security of Critical Infrastructures and Key Assets*
  - *National Strategy to Secure Cyberspace*

Aktivitas Keamanan Informasi Nasional

- ***Memperketat Hukum Keamanan Informasi***
  - *Cyber Security Enhancement Act*
    - ✓CSEA (*Cyber Security Enhancement Act*) of 2002 mencakup bab dua dari *Homeland Security Law*
    - ✓Memberikan amandemen pedoman pidana untuk beberapa kejahatan komputer seperti, pengecualian pengungkapan darurat, pengecualian kejujuran, larangan iklan Internet ilegal, dan perlindungan privasi

Aktivitas Keamanan Informasi Nasional

- ***Memperketat Hukum Keamanan Informasi***
  - *Federal Information Security Management Act*

    Tujuan utamanya adalah:

    ✓ Untuk memberikan kerangka kerja komprehensif untuk meningkatkan efisiensi kontrol keamanan informasi dari operasi dan aset; dan

    ✓ Untuk mengembangkan kontrol dan rencana pemeliharaan yang tepat untuk melindungi informasi/sistem informasi, dan menyediakan mekanisme untuk meningkatkan manajemen program keamanan informasi.

Aktivitas Keamanan Informasi Nasional

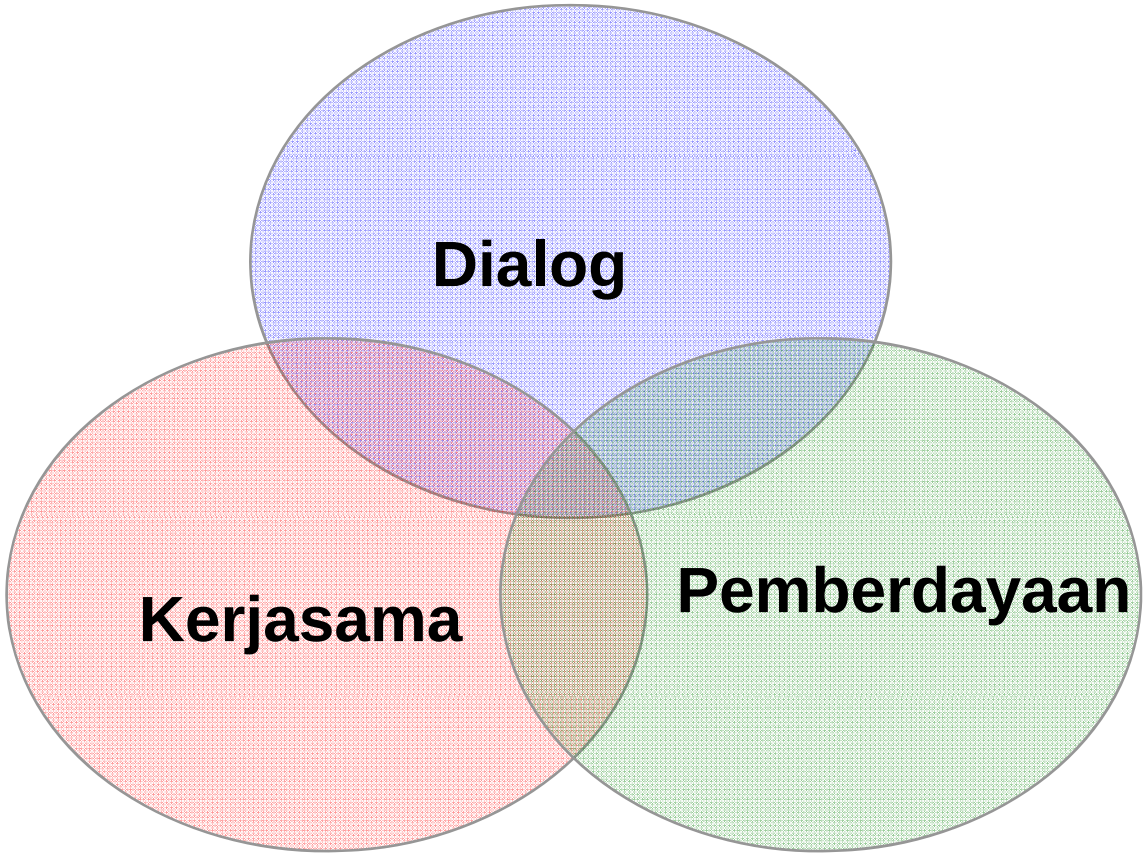
- **UE**
  - '*eEurope 2002 actionplan*' dan '*eEurope 2005*‘ untuk menjalankan ‘*Renewed Lisbon Strategy*’ dimana UE akan lebih cepat dibanding AS pada 2010
  - Visi ENISA menekankan kemitraan dan hubungan erat antar negara anggota, institusi riset, dan vendor peranti lunak/perangkat keras untuk mewujudkan budaya keamanan
  - Menekankan ‘kerja sama dan kemitraan’ sebagai basis kesuksesan 'i2010‘, yang mengejar pertumbuhan berkelanjutan dengan memanfaatkan TI

Aktivitas Keamanan Informasi Nasional

- **Strategi keamanan informasi UE**
  - Menurut '*2006 Communication*' (31 Mei 2006), pendekatan trisula untuk isu keamanan dibangun untuk mencakup:
    - ✓Langkah keamanan informasi dan jaringan
    - ✓Kerangka kerja pengaturan komunikasi elektronik (termasuk isu privasi dan keamanan data)
    - ✓Memerangi *cybercrime*

Aktivitas Keamanan Informasi Nasional

- **Strategi keamanan informasi UE**



Aktivitas Keamanan Informasi Nasional

- **Strategi keamanan informasi UE**
  - *Council of Europe Convention on Cybercrime*

Aktivitas Keamanan Informasi Nasional

- **Strategi keamanan informasi UE**
  - Visi ENISA

    "untuk membantu meningkatkan keamanan informasi dan jaringan dalam Komunitas [Uni Eropa] dan mendorong bertumbuhnya budaya keamanan informasi dan jaringan untuk kepentingan masyarakat, konsumen, serta organisasi bisnis dan sektor publik."
  - Menekankan kemitraan dan hubungan erat antar negara anggota, institusi riset, dan vendor peranti lunak/perangkat keras untuk mewujudkan budaya keamanan
  - Fokus pada pembuatan undang-undang dan solusi politik

Aktivitas Keamanan Informasi Nasional

➢ Aksi Jangka Panjang ENISA

Aktivitas Keamanan Informasi Nasional

- **Republik Korea**
  - Meskipun Republik Korea adalah salah satu neg ara paling maju di dunia dalam hal teknologi Inte rnet, mereka baru-baru saja menanggapi perl unya menjaga keamanan informasi.

Aktivitas Keamanan Informasi Nasional

- Strategi keamanan informasi
  - Di tahun 2004, pemerintah Korea melalui *Ministry of Information and Communication* (MIC) mengeluarkan *Information Security Roadmap* jangka menengah dan jangka panjang dengan tujuan untuk membangun BCN (*Broadband Convergence Network*).
  - Juga untuk mengembangkan teknologi keamanan terhadap penyalinan ilegal *next-generation mobile equipment*.
  - MIC juga berusaha mengenalkan *Privacy Impact Assessment* (PIA) dan membangun sarana untuk *adult certification* menggunakan nomor registrasi penduduk.

Aktivitas Keamanan Informasi Nasional

- Strategi keamanan informasi
  - Tujuan khusus *Information Security Roadmap* adalah untuk:

(1) menjamin keamanan infrastruktur jaringan;

(2) memastikan kehandalan layanan dan perangkat TI baru; dan

(3) mempromosikan dasar keamanan informasi di Republik Korea.

Aktivitas Keamanan Informasi Nasional

- **Jepang**
  - Jepang punya tujuan untuk menjadi ‘negara maju dalam keamanan informasi’ dan telah menetapkan sekumpulan tujuan rinci, prinsip dasar dan proyek di bidang keamanan informasi.

  - ISPC (*Information Security Policy Council*) dan NISC (*National Information Security Center*) adalah organisasi inti yang mengawasi semua pekerjaan keamanan informasi di Jepang.

Aktivitas Keamanan Informasi Nasional

- Strategi keamanan informasi
  - Strategi keamanan informasi Jepang terdiri dari dua bagian:
    - ✓*First National Strategy on Information Security*
    - ✓*Secure Japan YYYY*

Aktivitas Keamanan Informasi Nasional

- ***First Strategy on Information Security***
  - Pihak pelaksana:
    - ✓ Pemerintah pusat dan lokal
    - ✓ Infrastruktur penting
    - ✓ Bisnis
    - ✓ Individu
  - Kebijakan praktis:
    - ✓ Memajukan teknologi keamanan informasi
    - ✓ Memajukan kerjasama dan kolaborasi internasional
    - ✓ Pengembangan sumber daya manusia
    - ✓ Pengawasan kejahatan dan langkah perlindungan

Aktivitas Keamanan Informasi Nasional

Secure Japan YYYY

- adalah rencana tahunan keamanan informasi. *Secure Japan* 2007 berisi 159 langkah implementasi keamanan informasi dan arah rencana untuk 24 prioritas.

SJ2008 mencakup hal berikut:

1) Mempelajari langkah terobosan terhadap keterbatasan sistem promosi yang ada saat ini, kerangka kerja dari ukuran dan level teknologi
2) Sejumlah langkah perlu diambil dengan tepat
3) Memajukan usaha sehingga kebijakan keamanan informasi dapat menghasilkan dampak (hasil) sosial

Aktivitas Keamanan Informasi Internasional

- **PBB**
  - WSIS (*World Summit on the Information Society*)

    WSIS adalah salah satu konferensi yang disponsori PBB

  - Konferensi ini mengadopsi deklarasi prinsip dan rencana aksi untuk pertumbuhan masyarakat informasi yang efektif serta pengurangan ‘kesenjangan informasi’.

  - Rencana aksi menyatakan aksi-aksi berikut:
    - ✓ Peran pemerintah dan semua *stakeholder* dalam mendukung TIK untuk pembangunan
    - ✓ Infrastruktur informasi dan komunikasi sebagai pondasi penting untuk masyarakat informasi yang inklusif

Aktivitas Keamanan Informasi Internasional

PBB – lanjutan

- Rencana aksi menyatakan aksi-aksi berikut (cont'd):
  - ✓ Akses informasi dan pengetahuan
  - ✓ Pembangunan kapasitas
  - ✓ Membangun kepercayaan dan keamanan dalam penggunaan TIK
  - ✓ [Menciptakan] lingkungan yang mendukung
  - ✓ Aplikasi TIK dalam semua aspek kehidupan
  - ✓ Keragaman budaya, bahasa dan konten lokal
  - ✓ Media
  - ✓ Sisi etika dalam Masyarakat Informasi
  - ✓ Kerjasama regional dan internasional

Aktivitas Keamanan Informasi Internasional

- **PBB – lanjutan**
  - IGF (*Internet Governance Forum*)

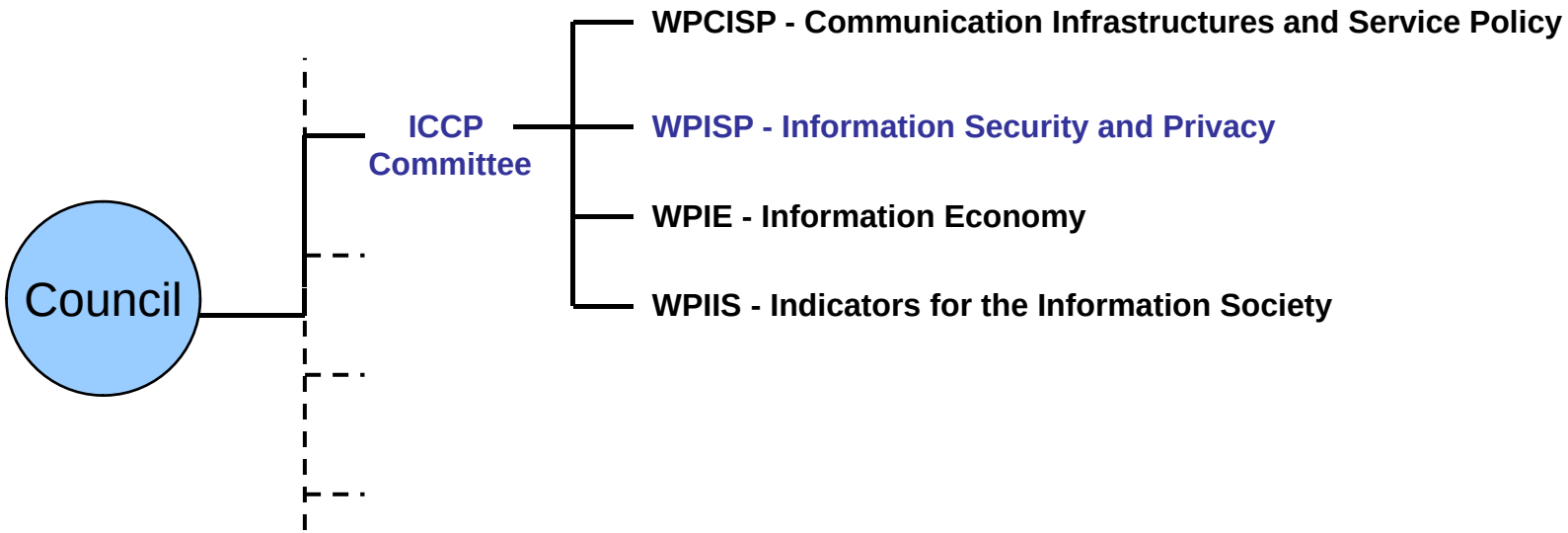
    adalah organisasi pendukung PBB untuk menangani Tata Kelola Internet.
  - Forum IGF kedua, yang diadakan di Rio de Janeiro pada tanggal 12-15 November 2007, berfokus pada isu keamanan informasi.
  - Peserta IGF mencapai kesepakatan bahwa keamanan Internet adalah faktor kunci untuk menegakkan integritas dan kerahasiaan TIK.
  - Isu-isu utama yang juga didiskusikan di pertemuan adalah *cyberterrorism*, *cybercrime*, dan keamanan anak-anak di Internet.

Aktivitas Keamanan Informasi Internasional

OECD

- WPISP (*Working Party on Information Security and Privacy*) bekerja dibawah bantuan *Committee for Information, Computer and Communications Policy* (ICCP).

WPISP dalam struktur OECD



Aktivitas Keamanan Informasi Internasional

- **OECD – lanjutan**
  - **Hasil kerja WPISP dalam hal Keamanan Informasi**
    - ✓ Di tahun 2002, OECD mengeluarkan "*Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*"
    - ✓ Survei kebijakan keamanan informasi nasional
    - ✓ *Workshop* internasional untuk berbagi pengalaman dan praktik terbaik
    - ✓ "*Culture of Security Web Site*": direktori sumber daya kebijakan keamanan informasi nasional
    - ✓ Kebijakan keamanan informasi untuk infrastruktur informasi penting dan *e-government* (sedang berlangsung)

Aktivitas Keamanan Informasi Internasional

- **OECD – lanjutan**
  - **Hasil kerja WPISP terkait privasi**
    - ✓ "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*" OECD (1980)
    - ✓ "*Privacy Online: OECD Guidance on Policy and Practice*" (2002)
    - ✓ *Privacy Law Enforcement Cooperation*

Aktivitas Keamanan Informasi Internasional

- **OECD – lanjutan**

  Hasil kerja lainnya:

  - *OECD Guidelines on Cryptography Policy* (1998)
  - *E-Authentication*
  - *OECD Task Force on Spam* (2005-2006)
  - "*Biometric-Based Technologies*" (2004)
  - Pekerjaan lain yang masih berlangsung
    - ✓ *Digital Identity Management*
    - ✓ Malware
    - ✓ *Radio frequency identification* (RFID) yang bersifat pervasif, sensor dan jaringan
    - ✓ Kerangka kerja umum untuk implementasi keamanan informasi dan privasi

Aktivitas Keamanan Informasi Internasional

- **APEC**
  - *APEC's Telecommunication and Information Working Group* (TEL) melakukan kegiatan keamanan informasi dan terdiri dari tiga kelompok pengarah:
    - Kelompok Pengarah Liberalisasi,
    - Kelompok Pengarah Pengembangan TIK, dan
    - Kelompok Pengarah Keamanan dan Kemakmuran.

Aktivitas Keamanan Informasi Internasional

- **ITU**

  WSIS (*World Summit on the Information Society*)

  - Diajukan oleh Tunisia di *ITU Plenipotentiary* 1998
  - Diadopsi saat *UN Summit 2001* (*UN General Assembly*)
  - Fase pertama, Jenewa, 10-12 December 2003
  - Fase kedua, Tunis, 16-18 November 2005
  - Kemitraan *Multi-stakeholder*

Aktivitas Keamanan Informasi Internasional

➢ ITU – lanjutan

- ❖ Kegiatan *Cybersecurity*:
  - ✓ITU-T - *WSIS Action Line C.5*
  - ✓ITU-D - ITU *Global Cyber-security Agenda*
  - ✓ITU-R - ITU *Cyber-security Gateway*

Aktivitas Keamanan Informasi Internasional

- **ITU – lanjutan**
  - ITU-D

    ITU-D disusun untuk membantu menyebarkan akses ke TIK yang adil, berkesinambungan, dan terjangkau sebagai cara merangsang pertumbuhan sosial dan ekonomi yang lebih luas.

  - ITU-D mengawasi program kerja *Cybersecurity* ITU yang disusun untuk membantu negara mengembangkan teknologi untuk keamanan *cyberspace* tingkat tinggi.

Aktivitas Keamanan Informasi Internasional

ITU – lanjutan

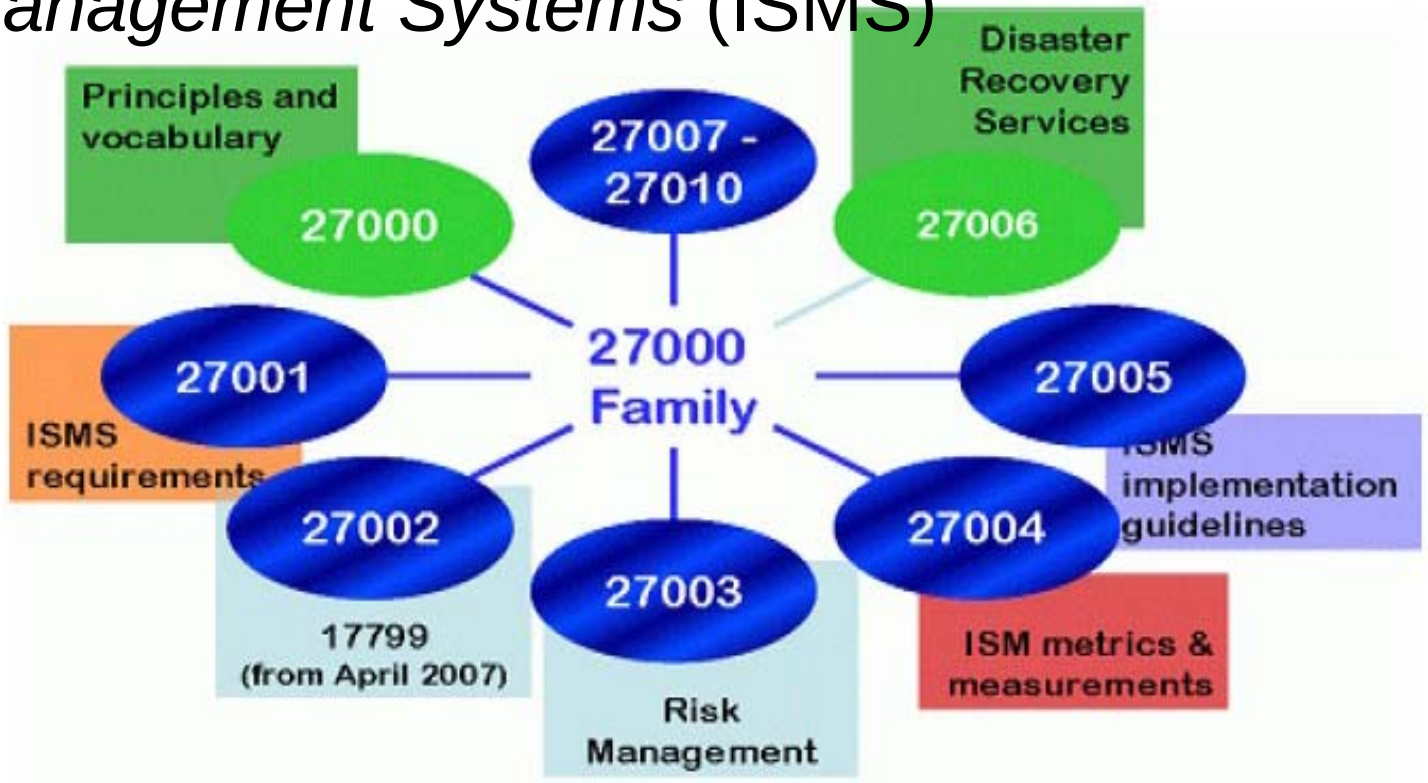
Kegiatan ITU-T pada *cybersecurity* (dalam *ICT security standards roadmap*)

- Bagian 1 berisi informasi tentang organisasi yang bekerja pada standar keamanan TIK
- Bagian 2 adalah basisdata standar keamanan saat ini dan termasuk juga standar keamanan ITU-T, ISO/IEC JTC 1, IETF, IEEE, ATIS, ETSI dan OASIS
- Bagian 3 berisi daftar standar
- Bagian 4 mengidentifikasi kebutuhan yang akan datang dan mengajukan standar-standar baru
- Bagian 5 berisi Praktik Terbaik Keamanan

Aktivitas Keamanan Informasi Internasional

- **ISO/IEC**

  27000 - ISMS: *Information Technology – Security Techniques – Information Security Management Systems* (ISMS)



Aktivitas Keamanan Informasi Internasional

- **ISO/IEC 15408 – *Common Criteria***
  - *Common Criteria* untuk Evaluasi Keamanan TI

Tujuan: Menjamin bahwa proses spesifikasi, implementasi, dan evaluasi dari produk keamanan komputer telah dilakukan dengan teliti dan mengikuti standar

Ringkasan

A. Aktivitas keamanan informasi nasional
   a. *AS*
   b. *UE*
   c. *Republik Korea*
   d. *Jepang*

B. Aktivitas keamanan informasi internasional
   a. Aktivitas keamanan informasi dari organisasi internasional
   b. Organisasi internasional berdasarkan subyek tertentu

Aktivitas Keamanan Informasi Internasional

- Pertanyaan
  - Dari beberapa kegiatan keamanan informasi yang dilakukan oleh organisasi internasional di Bagian ini, manakah yang telah di adopsi di negara Anda? Bagaimana mereka diimplementasikan?

Tugas

- Apa kemiripan diantara kegiatan keamanan informasi yang dilaksanakan oleh negara-negara yang dijelaskan dalam Bagian ini? Apa perbedaannya?
- Apakah ada aktivitas keamanan informasi oleh negara yang telah disebutkan sebelumnya yang tidak dapat diterapkan di negara Anda atau tidak relevan?
  - ✓ Jika ya, yang mana dan mengapa mereka tidak dapat diterapkan atau tidak relevan?

Modul 6: Keamanan Jaringan dan Keamanan Informasi dan Privasi

Sesi 3: Metodologi Keamanan Informasi

Tujuan Pembelajaran

- Memahami aspek administratif, fisik, dan teknis dari Metodologi Keamanan Informasi

- Memahami metode-metode keamanan informasi yang diterapkan di negara maju

Konten

- Metodologi Keamanan Informasi
  - Aspek Administratif
  - Aspek Fisik
  - Aspek Teknis ~ *Common Criteria*

- Contoh Menurut Negara
  - Amerika (NIST)
  - Inggris (BS7799)
  - Jepang (ISMS Ver. 2.0 (BS7799 Bagian 2: 2002))
  - Republik Korea (ISO/IEC27001 dan/atau KISA ISMS)
  - Jerman (*IT Baseline Protection Qualification*)
  - Lainnya

Metodologi Keamanan Informasi

- Aspek Administratif
  - ISO/IEC 27001 (BS7799)

    ISO27001 berisi kebutuhan untuk implementasi dan pengelolaan ISMS dan standar-standar umum yang digunakan untuk standar keamanan berbagai organisasi serta manajemen keamanan yang efektif

Kontrol di ISO/IEC27001

Domain	***Item***
A5.	Kebijakan keamanan
A6.	Organisasi keamanan informasi
A7.	Manajemen aset
A8.	Keamanan sumber daya manusia
A9.	Keamanan fisik dan lingkungan
A10.	Manajemen komunikasi dan operasi
A11.	Kontrol akses
A12.	Pengadaan, pengembangan dan pemeliharaan sistem informasi
A13.	Manajemen insiden keamanan informasi
A14.	Manajemen keberlangsungan bisnis
A15.	Kepatuhan (*compliance*)

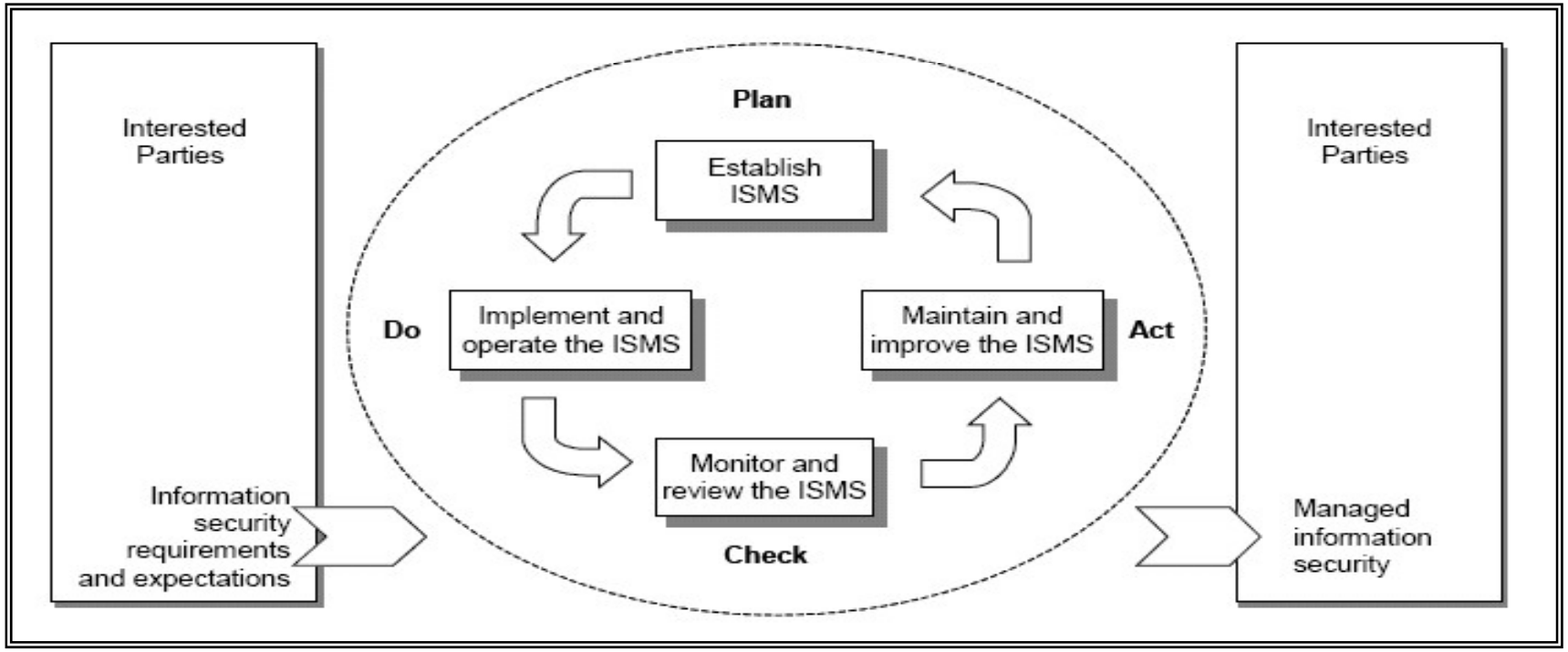
Sumber: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

Metodologi Keamanan Informasi

- Aspek Administratif
  - Model Proses ISO/IEC 27001 (BS7799)

    ISO/IEC27001 mengadopsi model proses *Plan-Do-Check-Act*, yang digunakan untuk mengatur struktur seluruh proses ISMS.

Model PDCA yang diterapkan ke Proses ISMS



Sumber: ISO/IEC JTC 1/SC 27

Metodologi Keamanan Informasi

- Aspek Administratif
  - ISO/IEC 27001 (BS7799)
    - ✓ **Analisis kesenjangan**

      Proses pengukuran tingkat keamanan informasi saat ini dan menetapkan arah masa depan keamanan informasi
    - ✓ **Kajian risiko**

      Terdiri dari dua bagian: kajian nilai aset dan kajian ancaman dan kerentanan
    - ✓ **Penerapan kontrol**

      Diperlukan keputusan untuk menerapkan kontrol yang sesuai untuk masing-masing nilai aset. Risiko perlu dibagi ke dalam risiko yang dapat diterima dan risiko yang tidak dapat diterima mengikuti kriteria 'Tingkatan Jaminan'.

Metodologi Keamanan Informasi

- Aspek Administratif
  - Sertifikasi ISO/IEC 27001 (BS7799)

    Setiap negara memiliki badan sertifikasi ISO/IEC27001. Jumlah sertifikasi tiap negara sebagai berikut:

Jumlah Sertifikasi Tiap Negara

Negara	Jumlah	Negara	Jumlah	Negara	Jumlah
Jepang	**2351**	Filipina	**12**	Vietnam	**3**
India	**382**	Swiss	**12**	Argentina	**2**
Inggris	**365**	UEA	**12**	Belgia	**2**
Taiwan	**170**	Arab Saudi	**10**	Bulgaria	**2**
Cina	**102**	Perancis	**10**	Denmark	**2**
Jerman	**85**	Iceland	**8**	Lithuania	**2**
Hungaria	**61**	Pakistan	**7**	Oman	**2**
Korea	**59**	Swedia	**7**	Peru	**2**
AS	**59**	Thailand	**7**	Portugal	**2**
Australia	**53**	Yunani	**6**	Qatar	**2**

Sumber: http://www.iso27001certificates.com/

Metodologi Keamanan Informasi

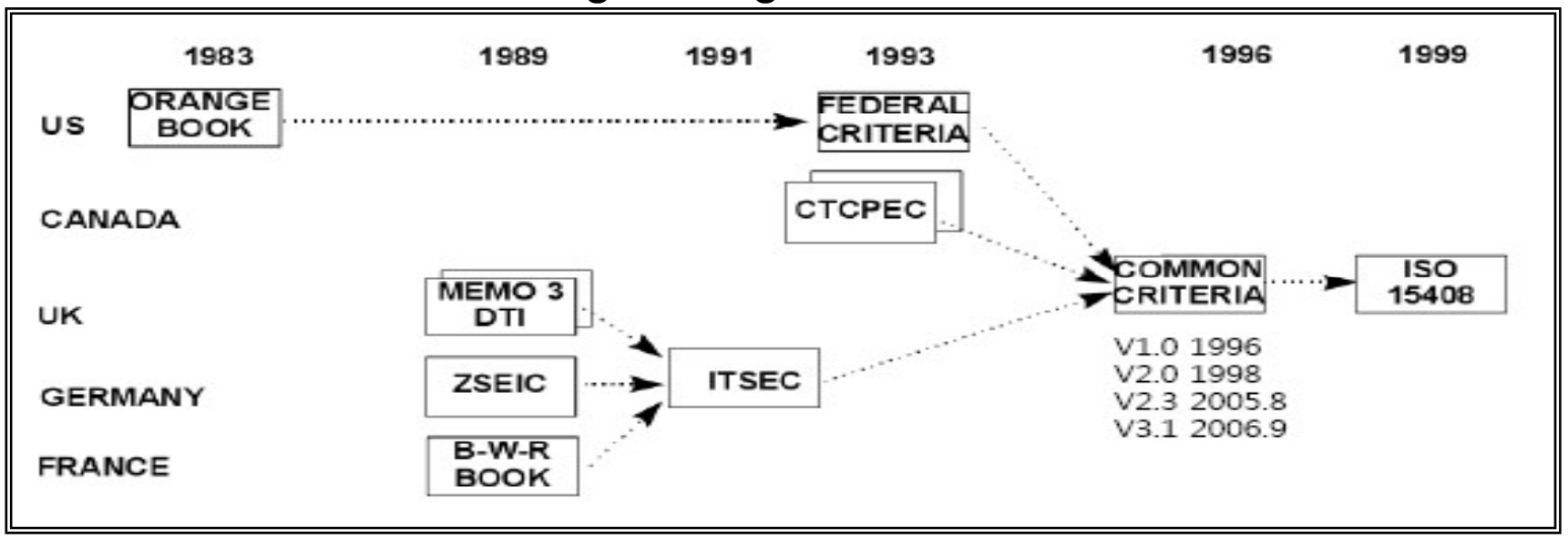
- Aspek Fisik
  - FEMA 426 di AS
  - FEMA (*Federal Emergency Management Agency*) 426 merupakan standar ISMS fisik di Amerika Serikat dan digunakan di banyak negara sebagai metodologi. FEMA 426 memberikan pedoman untuk melindungi gedung terhadap serangan teroris.
  - Seri terkait:
    - ✓FEMA 427: untuk bangunan komersial
    - ✓FEMA 428: untuk sekolah
    - ✓FEMA 429: untuk asuransi
    - ✓FEMA 430: untuk arsitek

Metodologi Keamanan Informasi

- Aspek Teknis
  - CC (*Common Criteria*)

    CC adalah standar internasional untuk level kebutuhan keamanan diantara negara. CC berisi kebutuhan untuk keamanan TI untuk produk atau sistem dalam kategori kebutuhan fungsional dan kebutuhan penjaminan

Proses Pengembangan Sertifikasi CC



Metodologi Keamanan Informasi

- Aspek Teknis
  - CC's *Security Functional Requirements* (SFRs)

    SFR menetapkan semua fungsi keamanan untuk TOE (*Target of Evaluation*) untuk mendapatkan sertifikasi CC

Isi Kelas dalam SFR

Kelas		Rincian
FAU	Audit keamanan	Fungsi-fungsi seperti proteksi data audit, format *record* dan seleksi peristiwa, serta perangkat analisis, alarm pelanggaran dan analisis *real-time*
FCO	Komunikasi	Menggambarkan kebutuhan secara spesifik bagi TOE yang digunakan untuk pengiriman informasi
FCS	Dukungan kriptografi	Menetapkan penggunaan manajemen kunci kriptografi dan operasi kriptografi
FDP	Proteksi data pengguna	Menetapkan kebutuhan terkait dengan perlindungan data pengguna
FIA	Identifikasi dan otentikasi	Menanggapi kebutuhan fungsi untuk menetapkan dan memverifikasi identitas pengguna yang diklaim

Metodologi Keamanan Informasi

- Aspek Teknis
  - CC's *Security Functional Requirements* (SFR) – lanjutan

Kelas		Rincian
FMT	Manajemen keamanan	Menentukan manajemen dari berbagai aspek *TOE Security Functions* (TSF): atribut keamanan, data dan fungsi TSF
FPR	Privasi	Berisi kebutuhan yang dapat ditarik untuk memenuhi kebutuhan privasi pengguna, sekaligus tetap menjaga sistem sefleksibel mungkin untuk memelihara kontrol yang cukup bagi operasional sistem
FPT	Proteksi TSF	Berisi kebutuhan fungsional yang terkait dengan integritas dan manajemen mekanisme dari TSF dan integritas data TSF
FRU	Utilisasi sumber daya	Berisi ketersediaan sumber daya yang dibutuhkan seperti pemrosesan kapabilitas dan/atau kapasitas penyimpanan
FTA	Akses TOE	Menentukan kebutuhan fungsional untuk pengontrolan sesi-sesi pengguna
FTP	Jalur/saluran yang dipercaya	Memberikan kebutuhan untuk jalur komunikasi yang dipercaya antara pengguna dan TSF

Metodologi Keamanan Informasi

- Aspek Teknis
  - *Security Assurance Requirement* (SAR)

    Filosofi CC membutuhkan artikulasi ancaman keamanan dan komitmen terhadap kebijakan keamanan organisasional melalui tindakan keamanan yang tepat dan cukup

Isu Kelas dalam SAR

Kelas		Rincian
APE	Evaluasi *Protection Profile* (PP)	Ini dibutuhkan untuk menunjukkan bahwa PP sudah baik dan konsisten dan, jika PP berdasar pada satu atau lebih PP atau paket lainnya, bahwa PP merupakan perwujudan yang benar dari PP dan paket yang digunakan.
ASE	Evaluasi *Security Target* (ST)	Ini dibutuhkan untuk menunjukkan bahwa ST sudah baik dan konsisten dan, jika ST berdasar pada satu atau lebih PP lainnya atau pada paket, bahwa ST merupakan perwujudan yang benar dari PP dan paket yang digunakan.
ADV	Pengembangan	Ini memberikan informasi tentang TOE. Pengetahuan yang didapat digunakan sebagai dasar untuk melakukan analisis kerentanan dan pengujian TOE, seperti dijelaskan dalam kelas kelas ATE dan AVA.
AGD	Dokumen pedoman	Untuk persiapan dan operasi TOE yang aman, perlu digambarkan semua aspek yang relevan untuk penanganan TOE yang aman. Kelas tersebut juga menanggapi kemungkinan salah konfigurasi atau penanganan TOE yang tidak diharapkan.

Metodologi Keamanan Informasi

- Aspek Teknis
  - *Security Assurance Requirement* (SAR)

Kelas		Rincian
ALC	Dukungan daur-hidup	Dalam daur-hidup produk, termasuk didalamnya kemampuan manajemen konfigurasi (CM), ruang lingkup CM, penyampaian, kemanan pengembangan, perbaikan kerusakan, definisi, perangkat dan teknik daur-hidup, membedakan apakan TOE dibawah tanggung jawab pengembang atau pengguna.
ATE	Tes	Penekanan di kelas ini adalah pada konfirmasi bahwa TSF beroperasi sesuai dengan deskripsi desainnya. Kelas ini tidak berurusan dengan penetrasi pengujian.
AVA	Kajian kerentanan	Kajian kerentanan mencakup berbagai kerentanan dalam pengembangan dan operasi TOE.
ACO	Komposisi	Menetapkan kebutuhan penjaminan yang didesain untuk memberikan kenyaman bahwa TOE yang disusun akan beroperasi secara aman ketika mengandalkan fungsionalitas keamanan yang disediakan oleh komponen piranti lunak, *firmware* atau perangkat keras yang dievaluasi sebelumnya.

Metodologi Keamanan Informasi

- Aspek Teknis
  - Metode evaluasi CC menyangkut dua aspek:
    - ✓**Evaluasi PP** (*Protection Profile*)

      PP mendeskrispsikan sekumpulan kebutuhan keamanan yang bebas-dari-implementasi untuk kategori TOE dan berisi pernyataan masalah keamanan dimana produk yang *compliant* berusaha selesaikan.

    - ✓**Evaluasi ST** (*Security Target*)

      ST merupakan dasar persetujuan antara pengembang TOE, konsumen, pengevaluasi dan otoritas evaluasi atas apa yang ditawarkan TOE, dan ruang lingkup evaluasi.

Metodologi Keamanan Informasi

- Aspek Teknis
  - CCRA (*Common Criteria Recognition Arrangement*) berfungsi untuk memberikan persetujuan sertifikasi CC di berbagai negara

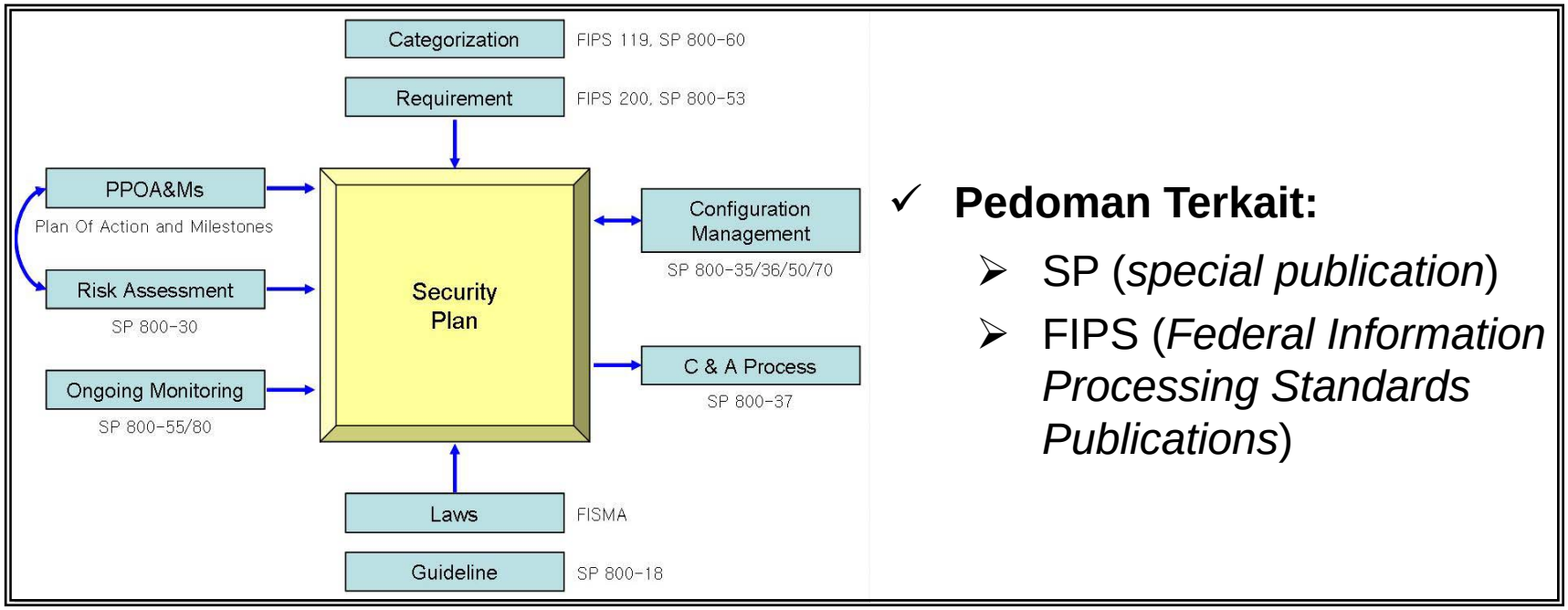
CAP dan CCP

- ✓ **Kualifikasi untuk CCRA :** Negara yang ingin menjadi anggota CCRA harus mengirimkan permohonan tertulis ke *Management Committee* (MC)
- ✓ **Anggota CCRA :**
  12 CAP (*Certificate Authorizing Participants*) dan
  12 CCP (*Certificate Consuming Participants*)

Studi Kasus Menurut Negara

- AS (NIST: *National Institute of Standards and Technology*)
  - NIST telah mengembangkan pedoman dan standar untuk memperkuat keamanan informasi dan sistem informasi yang dapat digunakan oleh institusi Federal

Masukan/Keluaran Proses Perencanaan Keamanan



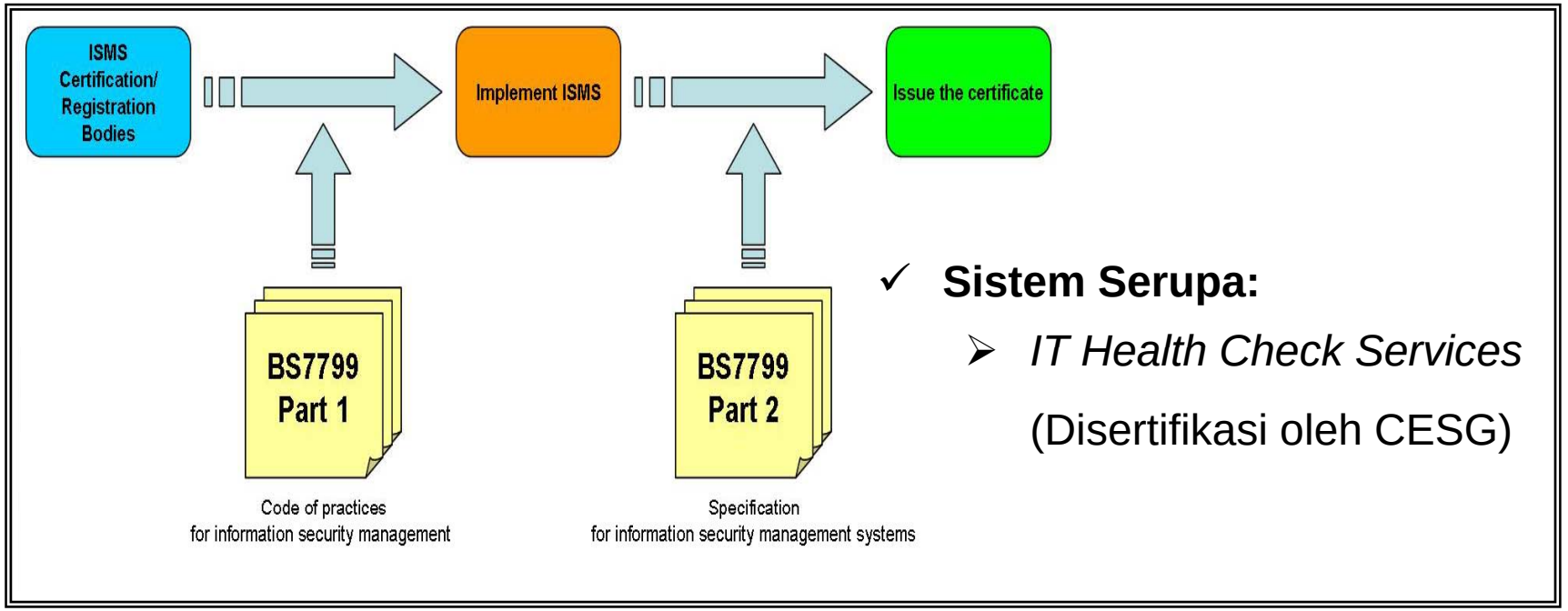
✓ **Pedoman Terkait:**

- SP (*special publication*)
- FIPS (*Federal Information Processing Standards Publications*)

Studi Kasus Menurut Negara

- Inggris (BS7799)
  - BSI menganalisis aktivitas keamanan organisasi di Inggris dan memberikan sertifikasi BS7799, yang sekarang telah dikembangkan menjadi ISO27001 (BS7799 bagian 2) dan ISO27002 (BS7799 bagian 1)

Proses Sertifikasi BS7799



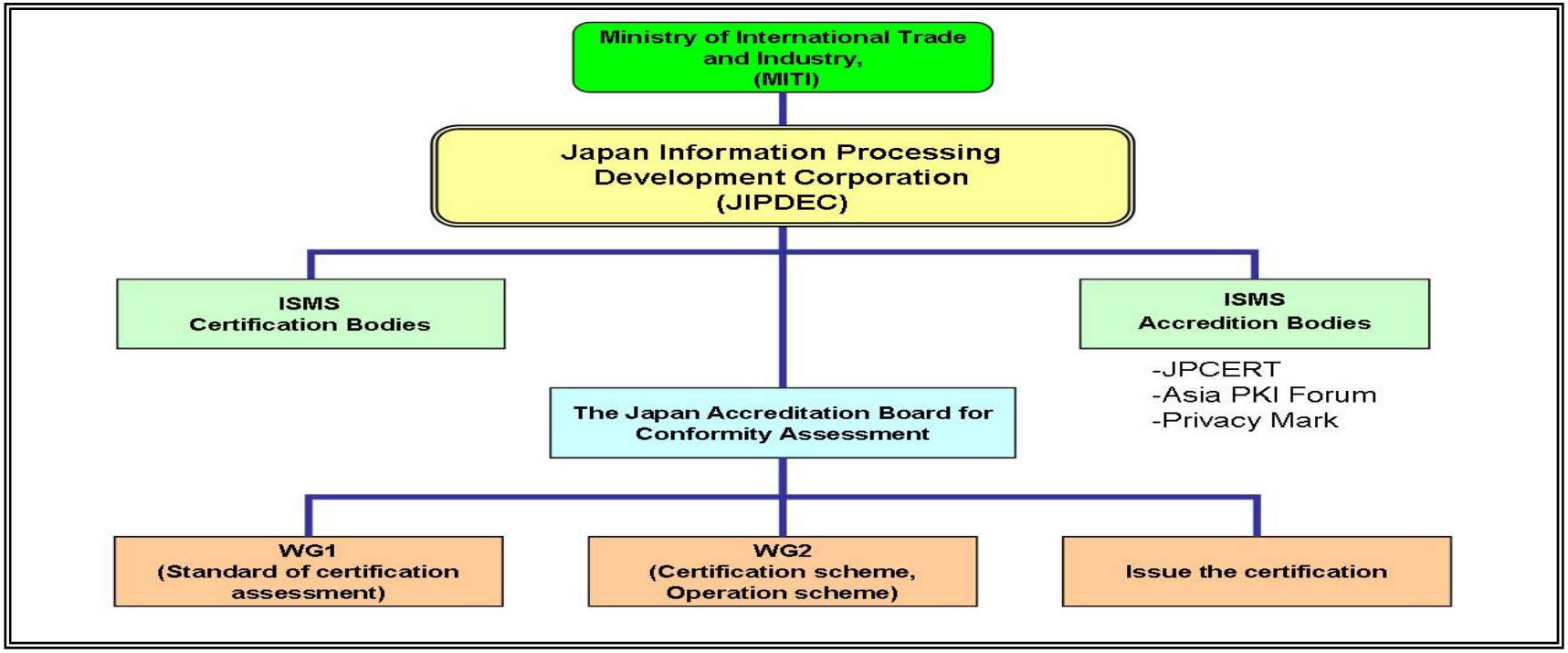
- ✓ **Sistem Serupa:**
  - *IT Health Check Services*

    (Disertifikasi oleh CESG)

Studi Kasus Menurut Negara

- Jepang (ISMS Ver. 2.0 (BS7799 Bagian 2: 2002))
  - ISMS Ver. 2.0 dari JIPDEC (*Japan Information Processing Development Corporation*) telah beroperasi di Jepang sejak April 2002 dan telah bergeser ke BS7799 Bagian 2: 2002.

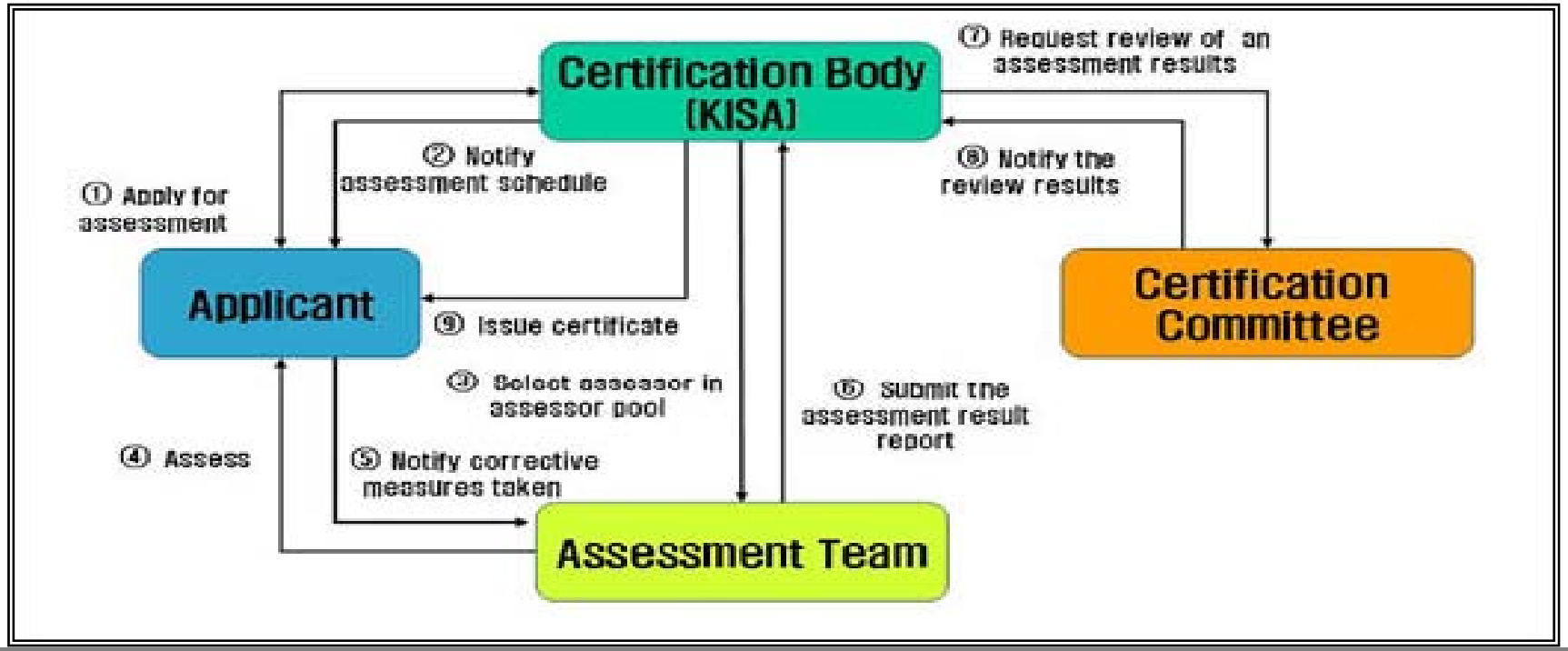
Sertifikasi ISMS di Jepang



Studi Kasus Menurut Negara

- Republik Korea (ISO/IEC27001 dan/atau KISA ISMS)
  - KISA (*Korea Information Security Agency*) menangani sertifikasi ISMS KISA, yaitu sistem manajemen sintetis yang mencakup rencana keamanan teknis/fisik

Sertifikasi ISMS KISA



Studi Kasus Menurut Negara

- Jerman (*IT Baseline Protection Qualification*)
  - BSI (*Bundesamt for Sicherheit in der Informationstechnik*) telah menyusun *IT Baseline Protection Qualification* berdasarkan standar internasional, *ISO Guide 25[GUI25]* dan standar Eropa, EN45001
  - Jenis-jenis sertifikasi meliputi:
    - ✓*IT Baseline Protection Certificate*
    - ✓*Self-declared (IT Baseline Protection higher level)*
    - ✓*Self-declared (IT Baseline Protection entry level)*

Studi Kasus Menurut Negara

- Lainnya

Tabel 9. Sertifikasi ISMS Negara Lain

	Lembaga Sertifikasi	Standar
Kanada	*Communications Security Establishment*	MG-4 Pedoman Sertifikasi dan Akreditasi untuk Sistem Teknologi Informasi
Taiwan	*Bureau of Standards, Meteorology and Inspection*	CNS 17799 & CNS 17800
Singapura	*Information Technology Standards Committee*	SS493 : Bagian 1 (Kerangka Kerja Standar Keamanan TI) & SS493 : Bagian 2 (Layanan Keamanan) sedang disusun

Ringkasan

- Metodologi Keamanan Informasi
  - Aspek Administratif
  - Aspek Fisik
  - Aspek Teknis ~ Kriteria Umum

- Contoh Menurut Negara
  - Amerika Serikat (NIST)
  - Inggris (BS7799)
  - Jepang (ISMS Ver. 2.0 (BS7799 Bagian 2: 2002))
  - Republik Korea (ISO/IEC27001 dan/atau KISA ISMS)
  - Jerman (*IT Baseline Protection Qualification*)
  - Lainnya

Modul 6: Keamanan Jaringan dan Keamanan Informasi dan Privasi

Sesi 4: Perlindungan Privasi

Tujuan Pembelajaran

- Memahami konsep privasi
- Tren kebijakan privasi di organisasi internasional dan beberapa negara
- Memberikan gambaran dan contoh Kajian Dampak Privasi (*Privacy Impact Assessment*).

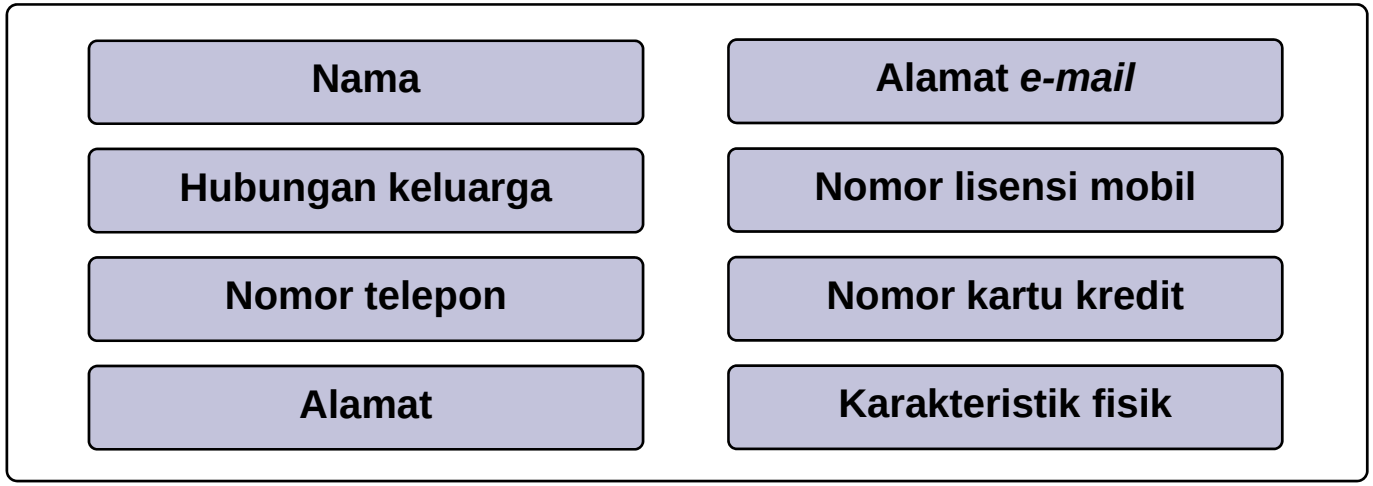
Konten

- Konsep Privasi
  - Apakah “Informasi Pribadi”?
  - Informasi Pribadi dan Privasi
  - Serangan Privasi
- Tren Kebijakan Privasi
  - OECD, UE, PBB
  - Republik Korea, AS, Jepang
- *Privacy Impact Assessment* (PIA)
  - Apakah PIA?
  - Proses PIA
  - Ruang lingkup penilaian PIA
  - Contoh-contoh PIA

Konsep Privasi

- Apakah “Informasi Pribadi”?
- Secara sempit, Informasi pribadi adalah informasi yang berkaitan dengan individu yang dapat diidentifikasi atau orang yang teridentifikasi. Termasuk di dalamnya informasi seperti nama, nomor telepon, alamat, *e-mail*, nomor lisensi mobil, karakteristik fisik (dimensi wajah, sidik jari, tulisan tangan, dan lain-lain), nomor kartu kredit, dan hubungan keluarga

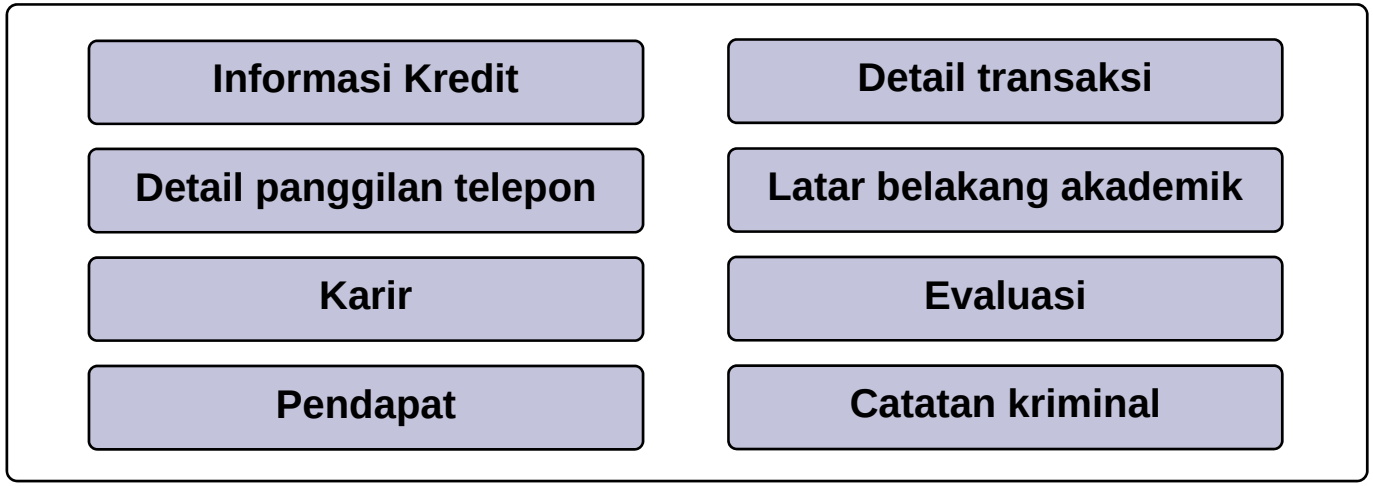
Informasi Pribadi, definisi sempit



Konsep Privasi

- Apakah “Informasi Pribadi”?
  - Dalam pengertian lebih luas, mencakup informasi pribadi seperti informasi kredit, detail transaksi, detail panggilan telepon, latar belakang akademik, karir, evaluasi/opini, dan catatan kriminal.

Informasi Pribadi, Definisi Luas



Konsep Privasi

- Informasi Pribadi dan Privasi
  - Akses, pengumpulan, analisis, dan penggunaan informasi pribadi yang tidak pantas berdampak pada perilaku pihak lain terhadap pribadi yang bersangkutan dan pada akhirnya berdampak negatif terhadap kehidupan sosial, harta benda, dan keselamatan-nya.
  - Oleh karena itu, informasi pribadi harus dilindungi dari akses, pengumpulan, penyimpanan, analisis dan penggunaan yang salah. Dalam hal ini, informasi pribadi adalah subyek perlindungan.

Konsep Privasi

- Informasi Pribadi dan Privasi
  - Ada lima cara untuk menjelaskan **hak untuk privasi**:
    1. Hak untuk bebas dari akses yang tidak diinginkan (misalnya akses fisik, akses melalui SMS)
    2. Hak untuk tidak membolehkan informasi pribadi digunakan dengan cara yang tidak diinginkan (misalnya penjualan informasi, pembocoran informasi, pencocokan)
    3. Hak untuk tidak membolehkan informasi pribadi dikumpulkan oleh pihak lain tanpa sepengetahuan atau seizin seseorang (misalnya melalui penggunaan CCTV dan *cookies*)
    4. Hak untuk memiliki informasi pribadi yang dinyatakan secara akurat dan benar (integritas)
    5. Hak untuk mendapatkan imbalan atas nilai informasi

Konsep Privasi

- Informasi Pribadi dan Privasi
  - Konsep Pasif
    - ✓"*The right to life has come to mean the right to enjoy life – the right to be let alone*."

      Samuel Warren & Louise Brandeis (1890)
    - ✓Hak untuk dibiarkan sendiri (tidak diusik)
    - ✓Hak alami terkait dengan martabat manusia
    - ✓Terkait dengan undang-undang yang melarang masuk tanpa izin
  - Konsep Aktif
    - ✓Kontrol mandiri terhadap informasi pribadi, atau
    - ✓Hak untuk melakukan koreksi terhadap efek yang dihasilkan dari informasi pribadi yang tidak benar

Tren dalam Kebijakan Privasi

- OECD
  - Pada tahun 1980, OECD mengadopsi "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*," yang juga dikenal sebagai "*OECD Fair Information Practices*."
  - Pada tahun 2002 "*Privacy Online: OECD Guidance on Policy and Practice*" diumumkan.
  - Pedoman tersebut diterapkan pada data pribadi (baik di sektor publik atau swasta) yang menimbulkan bahaya terhadap privasi dan kebebasan individu sebagai akibat dari cara informasi tersebut diproses, atau akibat dari sifat atau konteks dimana informasi tersebut digunakan.
  - Prinsip-prinsip OECD yang dinyatakan dalam Pedoman tersebut menyatakan hak dan kewajiban individu dalam konteks otomasi proses data pribadi, serta hak dan kewajiban mereka yang terlibat dalam proses tersebut.
  - Selain itu, prinsip-prinsip dasar yang digariskan dalam Pedoman tersebut juga dapat digunakan baik di tingkat nasional maupun internasional.

Tren dalam Kebijakan Privasi

- OECD
- Delapan prinsip dalam pedoman OECD terkait perlindungan privasi adalah
  - Prinsip pembatasan pengumpulan
  - Prinsip kualitas data
  - Prinsip pernyataan tujuan
  - Prinsip penggunaan terbatas
  - Prinsip penjagaan keamanan
  - Prinsip keterbukaan
  - Prinsip partisipasi individu
  - Prinsip akuntabilitas

Tren dalam Kebijakan Privasi

- OECD

1. Prinsip pembatasan pengumpulan

Perlu ada pembatasan dalam hal pengumpulan data pribadi. Data harus diperoleh dengan cara yang adil dan sah menurut hukum serta, jika diperlukan, sepengetahuan atau seizin subyek data.

2. Prinsip kualitas data

Data pribadi harus relevan dengan tujuan penggunaannya. Sesuai dengan penggunaan tersebut, data harus akurat, lengkap dan *up-to-date*.

Tren dalam Kebijakan Privasi

- OECD

3. Prinsip pernyataan tujuan

Tujuan pengumpulan data pribadi harus dinyatakan selambat-lambatnya pada saat pengumpulan data, dan penggunaan data sesudah itu hanya akan terbatas pada pemenuhan tujuan atau penggunaan lain yang tetap sesuai dengan tujuan, serta sebagaimana dinyatakan setiap terjadi perubahan tujuan.

4. Prinsip penggunaan terbatas

Data pribadi tidak boleh diungkapkan, dibuat menjadi tersedia atau digunakan untuk tujuan selain dari yang ditentukan sesuai dengan prinsip pernyataan tujuan kecuali dengan persetujuan dari subyek data atau otoritas hukum.

Tren dalam Kebijakan Privasi

- OECD

5. Prinsip penjagaan keamanan

Data pribadi harus dilindungi dengan penjagaan keamanan yang wajar terhadap risiko seperti kehilangan atau akses tanpa izin, perusakan, penggunaan, modifikasi atau penyingkapan data.

6. Prinsip keterbukaan

Harus ada kebijakan umum tentang keterbukaan pengembangan, praktik dan kebijakan terkait dengan data pribadi. Alat harus siap sedia untuk menentukan keberadaan dan sifat data pribadi, tujuan utama penggunaannya, serta identitas dan alamat dari pengendali data.

Tren dalam Kebijakan Privasi

- OECD

7. Prinsip partisipasi individu

Individu seharusnya memiliki hak untuk:

a. Mendapatkan konfirmasi dari pengendali data apakah mereka memiliki data yang berkaitan dengan dia;
b. Menerima komunikasi tentang data yang berhubungan dengan dia dalam waktu yang wajar, dengan biaya, jika ada, yang tidak berlebihan, dalam cara yang wajar, dan dalam bentuk yang mudah dimengerti oleh dia;
c. Diberikan alasan jika permintaan yang dibuat berdasarkan sub-paragraf (a) dan (b) ditolak, dan untuk dapat mengajukan keberatan atas penolakan, dan
d. Untuk mengajukan keberatan terhadap data yang berkaitan dengannya dan, jika keberatan tersebut berhasil, untuk meminta data dihapus, dikoreksi, dilengkapi atau diubah

8. Prinsip akuntabilitas

Pengendali data harus bertanggung jawab untuk mematuhi langkah-langkah yang memberikan efek pada prinsip-prinsip yang dinyatakan di atas

Tren dalam Kebijakan Privasi

- PBB
  - Sejak akhir tahun 1960-an, dunia telah memberi perhatian akan efek terhadap privasi atas pemrosesan informasi secara otomatis. UNESCO khususnya telah menunjukkan perhatian akan privasi dan perlindungan privasi sejak "*UN Guidelines for the Regulation of Computerized Personal Data File*" diadopsi oleh Majelis Umum pada tahun 1990.

  - Pedoman PBB diterapkan ke dokumen (kertas) serta *file* data komputerisasi di sektor publik atau swasta. Panduan tersebut menyatakan serangkaian prinsip terkait jaminan minimum yang harus disediakan untuk perundang-

Tren dalam Kebijakan Privasi

- Pedoman PBB yang berkaitan dengan perlindungan privasi
  - Prinsip sah dan keadilan
  - Prinsip akurasi
  - Prinsip pernyataan tujuan
  - Prinsip akses orang yang berkepentingan
  - Prinsip non-diskriminasi
  - Kekuatan untuk membuat pengecualian
  - Prinsip keamanan
  - Pengawasan dan sanksi
  - Aliran data antar-batas
  - Bidang penerapan

Tren dalam Kebijakan Privasi

- EU
  - *EU's Council of Ministers* mengadopsi *European Directive on the Protection of Individuals with Regard to Processing of Personal Data dan Free Movement of Such Data (EU Directive)* pada tanggal 24 Oktober 1995 yang menyediakan kerangka kerja pengaturan untuk menjamin keamanan dan pergerakan bebas data pribadi lintas batas nasional negara-negara anggota Uni Eropa (UE), dan juga untuk menetapkan dasar keamanan seputar informasi pribadi dimanapun data itu disimpan, dikirim atau diproses.
  - *EU Data Protection Directive* disusun sebagai usaha untuk menyatukan dan menyelaraskan dengan hukum masing-masing negara terkait perlindungan privasi. Artikel 1 dari *EU Directive* menyatakan bahwa "Negara Anggota harus melindungi hak-hak dasar dan kebebasan alami seseorang, dan khususnya hak mereka atas privasi, terkait dengan pemrosesan data pribadi."
  - Setiap negara anggota UE telah merevisi hukum yang ada atau menetapkan hukum perlindungan privasi baru untuk melaksanakan *EU Directive*.

Tren dalam Kebijakan Privasi

- EU
  - Contoh lain hukum UE mengenai perlindungan privasi:
    - ✓ Artikel 8 *European Convention on Human Rights*
    - ✓ *Directive 95/46/EC (Data Protection Directive)*
    - ✓ *Directive 2002/58/EC (the E-Privacy Directive)*
    - ✓ *Directive 2006/24/EC Article 5 (The Data Retention Directive)*

Tren dalam Kebijakan Privasi

- Republik Korea
  - Republik Korea memiliki pelanggan jaringan *broadband* terbanyak di dunia. Pada pertengahan tahun 2005, 25 persen populasi dan 75 persen rumah tangga telah berlangganan jaringan *broadband*. Jaringan komunikasi nirkabel dan jaringan *broadband* Republik Korea saat ini diakui sebagai salah satu yang terbaik di dunia. Karenanya, frekuensi kebocoran informasi pribadi di dalam negeri telah meningkat secara signifikan, sehingga membutuhkan kebijakan dan solusi teknologi.
  - Sayangnya, pemerintah Korea tidak bergerak cukup cepat terhadap hal ini. UU Perlindungan Privasi masih ditunda dalam *National Assembly* dan tidak ada hukum independen untuk proteksi

Tren dalam Kebijakan Privasi

- Republik Korea
  - Pemerintah Korea telah menetapkan "*Mid- and Long-term Information Security Roadmap for Realizing u-SafeKorea*" dan empat proyek prioritas utama sejak 2005 adalah:

1. menjamin keamanan infrastruktur utama;
2. menciptakan kepercayaan terhadap layanan baru TI;
3. menguatkan fungsi perlindungan informasi untuk mesin pertumbuhan yang baru; dan
4. membangun basis keamanan informasi di lingkungan baru *cyber*.

  - Prioritas keempat juga mencakup sub proyek yang disebut 'Penguatan Sistem Perlindungan Privasi'.
  - Beberapa hukum yang terkait dengan perlindungan privasi :
    - ✓ *Personal Information Protection Law in Public*
    - ✓ *Law on Telecom Networks and Information Protection*

Tren dalam Kebijakan Privasi

- Republik Korea
  - Contoh hukum Korea terkait Perlindungan Privasi
    - ✓*Personal Information Protection Law in Public*
    - ✓Undang-undang Peningkatan Pemanfaatan Jaringan Informasi dan Komunikasi dan Perlindungan Informasi
    - ✓Undang-undang Perlindungan Rahasia Komunikasi
    - ✓Undang-undang Perlindungan Informasi Lokasi

Tren dalam Kebijakan Privasi

- Amerika Serikat
  - AS telah mempercayakan kegiatan perlindungan privasi ke pasar mengingat terlalu banyak pembatasan oleh pemerintah telah menghambat aktivitas *e-commerce*.
  - *Privacy Act* tahun 1974 memberikan perlindungan privasi informasi di sektor publik sementara hukum yang berbeda mengatur privasi di sektor swasta.
  - Tidak ada organisasi yang menangani masalah perlindungan privasi di sektor swasta. Di sektor publik, *Office of Management and Budget* (OMB) berperanan dalam menetapkan kebijakan privasi pemerintah federal mengikuti *Privacy Act*

Tren dalam Kebijakan Privasi

- Amerika Serikat
  - Di sektor swasta, *Federal Trade Commission* diberi wewenang mengeksekusi hukum yang melindungi privasi *online* anak-anak, informasi kredit konsumen, dan praktik perdagangan yang wajar.

Tren dalam Kebijakan Privasi

- Amerika Serikat
  - Hukum AS yang terkait dengan perlindungan privasi adalah sebagai berikut :
    - ✓The Privacy Act (1974)
    - ✓CCPA (*Consumer Credit Protection Act*, 1984)
    - ✓ECPA (*Electric Communications Privacy Act*, 1986)
    - ✓Gramm-Leach-Bliley Act (1999)
    - ✓HIPAA (*Health Insurance Portability and Accountability Act*, 1996)
    - ✓SOX (*Sarbanes-Oxley Act*, 2002)
    - ✓COPPA (*Children's Online Privacy Protection Act*, 1998)

Tren dalam Kebijakan Privasi

- Jepang
  - Pada tahun 1982, Jepang menetapkan langkah perlindungan privasi berdasarkan delapan prinsip dasar OECD.
  - Di tahun 1988, hukum perlindungan privasi di sektor publik diumumkan dan memperlihatkan efek.
  - Di sektor swasta, *Guideline for the Protection of Privacy* dikeluarkan oleh Departemen Industri dan Perdagangan Internasional di tahun 1997.
  - Untuk meningkatkan kesesuaian hukum perlindungan privasi nasional dengan pedoman internasional, *Advanced Information and Telecommunications Society Promotion Headquarters* telah mendorong legislasi hukum perlindungan informasi pribadi.
  - Sebagai tambahan, *Data Protection Authority* telah ditunjuk sebagai lembaga independen yang akan memastikan ketaatan terhadap perlindungan privasi dan membantu individu dalam kasus pelanggaran privasi.

Tren dalam Kebijakan Privasi

- Jepang
  - Hukum Jepang yang terkait dengan perlindungan privasi adalah sebagai berikut :
    - ✓ *Act for the Protection of Computer Processed Personal Data Held by Administrative Organs*, 1988
    - ✓ *Regulations of Local Governments* (dikeluarkan pada tahun 1999 untuk 1.529 pemerintah lokal)
    - ✓ *Act for the Protection of Personal Information*, 2003
    - ✓ *Act on the Protection of Personal Information Held by Administrative Organs*, 2003
    - ✓ *Act for the Protection of Personal Information Retained by Independent Administrative Institutions*, 2003
    - ✓ *Board of Audit Law*, 2003

Tren dalam Kebijakan Privasi

- Pertanyaan
  - Di negara Anda, kebijakan dan hukum apa yang diterapkan untuk melindungi privasi informasi?
  - Apa masalah atau akibat yang timbul dari pengesahan dan/atau pelaksanaan kebijakan dan hukum tersebut?
  - Prinsip apa (lihat Pedoman OECD dan Pedoman PBB) yang Anda pikir dapat mendukung kebijakan dan hukum perlindungan privasi di negara Anda?

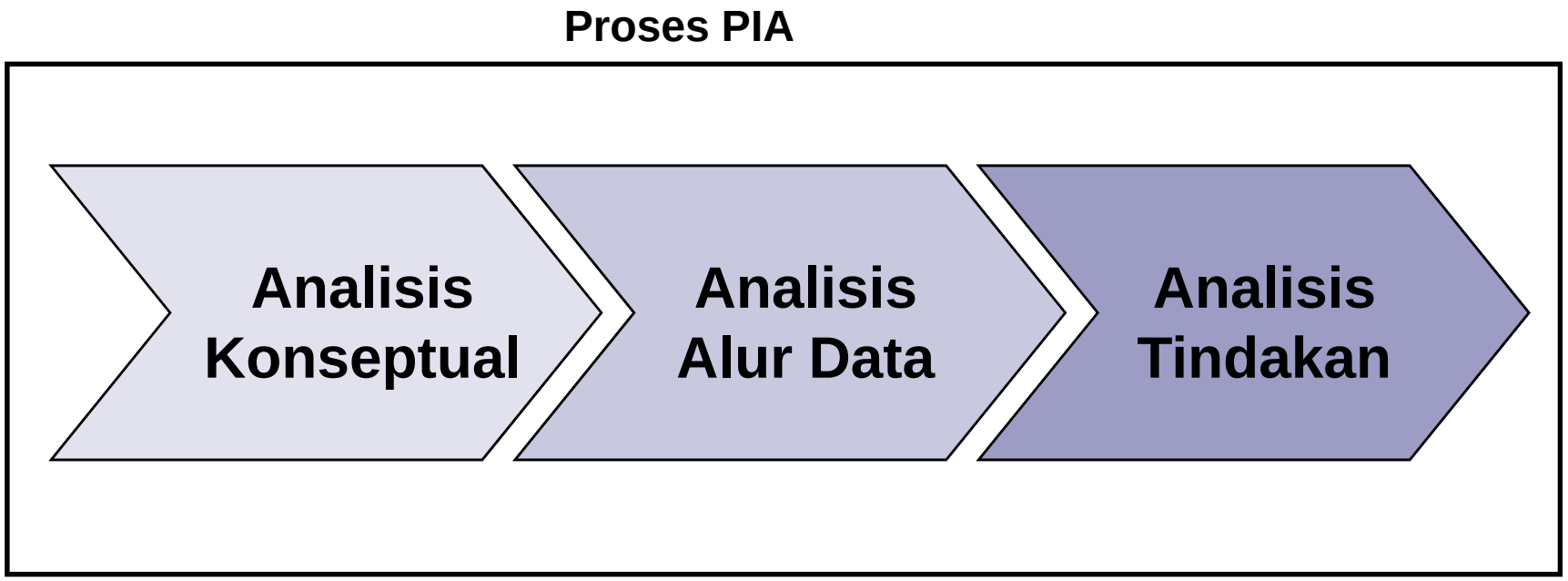
Privacy Impact Assessment (PIA)

- Apakah PIA?

  PIA adalah proses sistematis dari investigasi, analisis dan evaluasi efek privasi konsumen atau nasional dari penggunaan sistem informasi baru atau modifikasi sistem informasi yang ada. PIA berdasar pada ‘prinsip pencegahan awal’ – yaitu mencegah lebih baik daripada mengobati. PIA bukan hanya evaluasi terhadap sistem tetapi mempertimbangkan efek serius privasi dari pengenalan atau perubahan sistem baru.

Privacy Impact Assessment (PIA)

- Proses PIA



Privacy Impact Assessment (PIA)

- Lingkup penilaian PIA

  PIA dilakukan ketika :

  1. Membangun sistem informasi baru yang akan memegang dan mengelola informasi pribadi dalam jumlah besar;
  2. Menggunakan teknologi baru dimana privasi dapat terganggu;
  3. Memodifikasi sistem informasi yang ada yang memegang dan mengelola informasi pribadi; dan
  4. Mengumpulkan, menggunakan, menyimpan dan/atau menghancurkan informasi pribadi dimana risiko gangguan privasi dapat timbul.

Privacy Impact Assessment (PIA)

- Contoh PIA

Contoh PIA Menurut Negara

Dasar Hukum	
Amerika Serikat	*Section 208* dari *e-Government Act* tahun 2002 OMB memberikan persyaratan PIA dalam OMB-M-03-22
Kanada	Mengenalkan kebijakan dan pedoman PIA pada bulan Mei 2002 Mewajibkan eksekusi PIA pada basis hukum umum pada privasi
Australia / Selandia Baru	Dengan sukarela melaksanakan PIA (tanpa dasar hukum) *PIA Handbook* untuk mendukung PIA (2004, Selandia Baru), pe doman PIA (2004, Australia)

Ringkasan

- Konsep Privasi
  - Apakah “Informasi Pribadi”?
  - Informasi Pribadi dan Privasi
  - Serangan Privasi
- Tren dalam Kebijakan Privasi
  - OECD, UE, PBB
  - Republik Korea, AS, Jepang
- *Privacy Impact Assessment* (PIA)
  - Apakah PIA?
  - Proses PIA
  - Ruang lingkup penilaian PIA
  - Contoh-contoh PIA

Modul 6: Keamanan Jaringan dan Keamanan Informasi dan Privasi

Sesi 5 : Pembentukan dan Operasi CSIRT

Tujuan Pembelajaran

- Menjelaskan bagaimana membentuk dan mengoperasikan *Computer Security Incident Response Team* (CSIRT) nasional; dan

- Mempelajari berbagai model CSIRT

Konten

- Pengembangan dan Operasi CSIRT
  - Tinjauan
  - Model CSIRT dan Memilih Model CSIRT yang tepat
  - Pembentukan CSIRT
  - Operasi & Layanan CSIRT

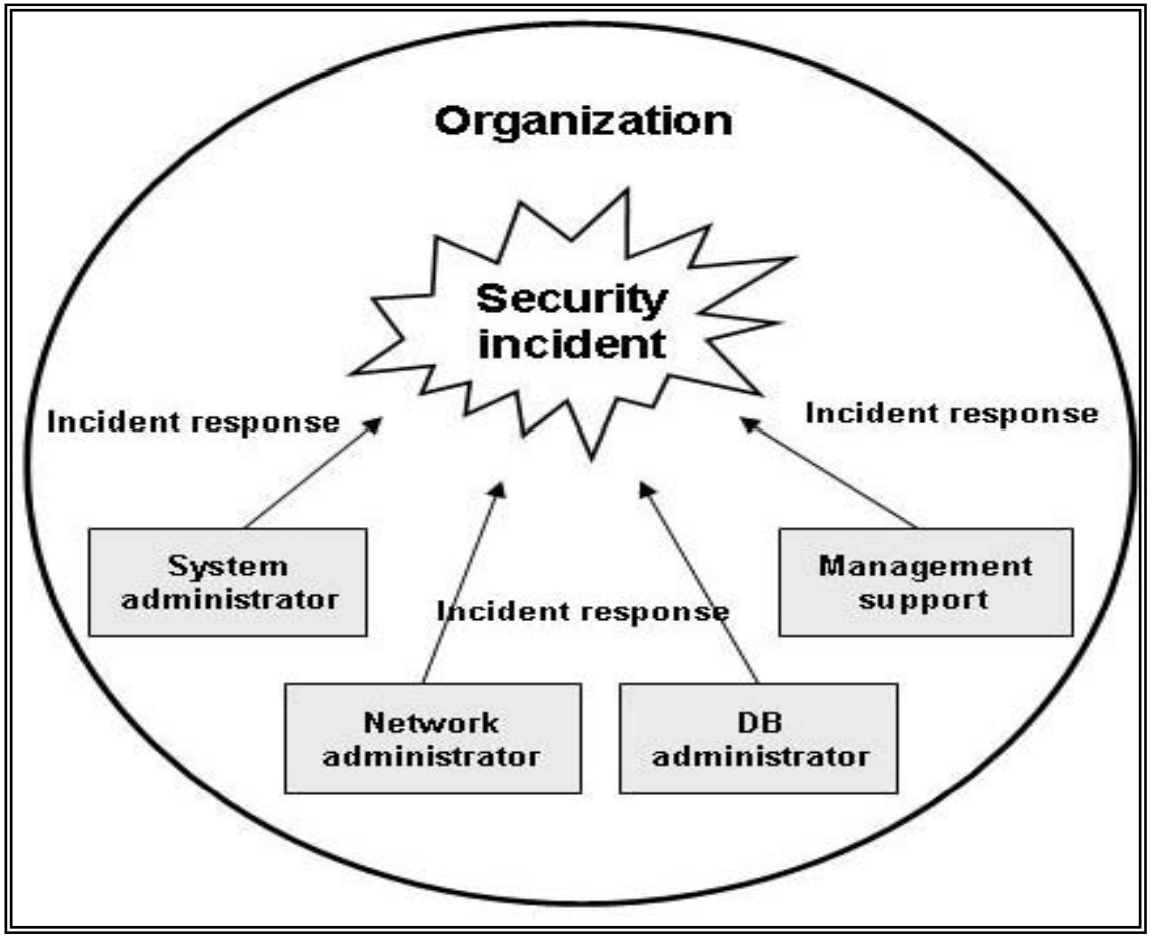
- Status CSIRT saat ini
  - CSIRT Internasional

Pengembangan dan Operasi CSIRT

- Definisi CSIRT
  - CSIRT merupakan sebuah organisasi, seperti organisasi formal atau adhoc lainnya, yang bertanggungjawab atas penerimaan, pemantauan dan penanganan laporan dan aktivitas insiden keamanan komputer

- Riwayat CSIRT
  - 1988, penyebaran pertama worm Morris
  - *Defence Advanced Research Projects Agency* (DARPA) membentuk *Software Engineering Institute (SEI)* dan kemudian membentuk CERT/CC.
  - Setiap negara di Eropa membentuk organisasi sejenis
  - *Forum of Incident Response and Security Teams* (FIRST) dibentuk pada tahun 1990

Model CSIRT

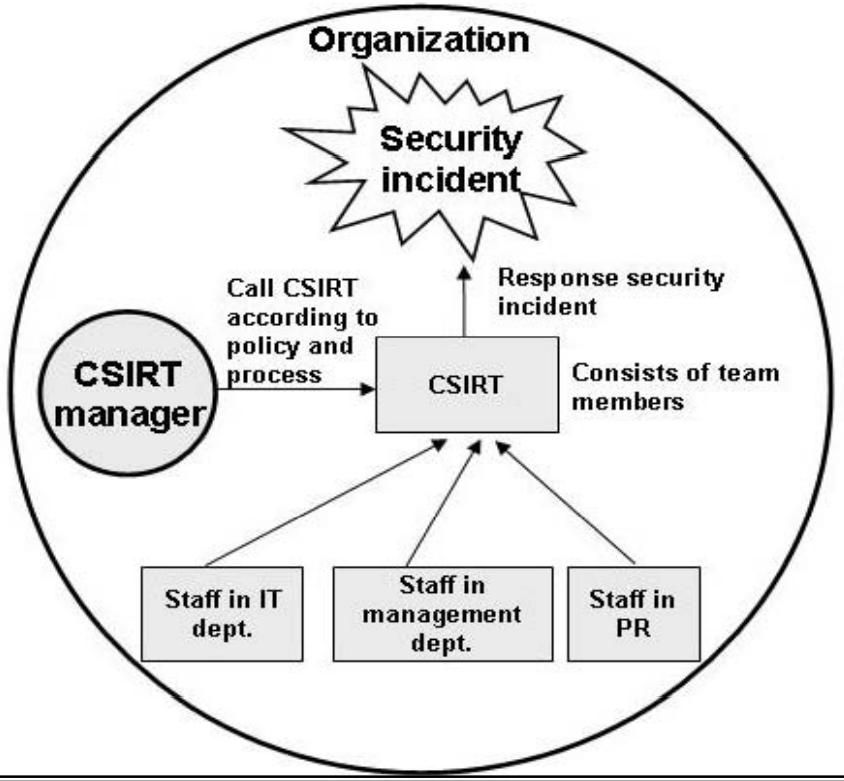


Model Tim Keamanan (menggunakan staf TI yang ada)

- Berlawanan dengan CSIRT yang umum
- Tidak ada organisasi sentral yang bertanggung jawab untuk menangani insiden keamanan komputer
- Tugas penanganan insiden dilakukan oleh administrator sistem dan jaringan, atau oleh spesialis sistem keamanan lainnya

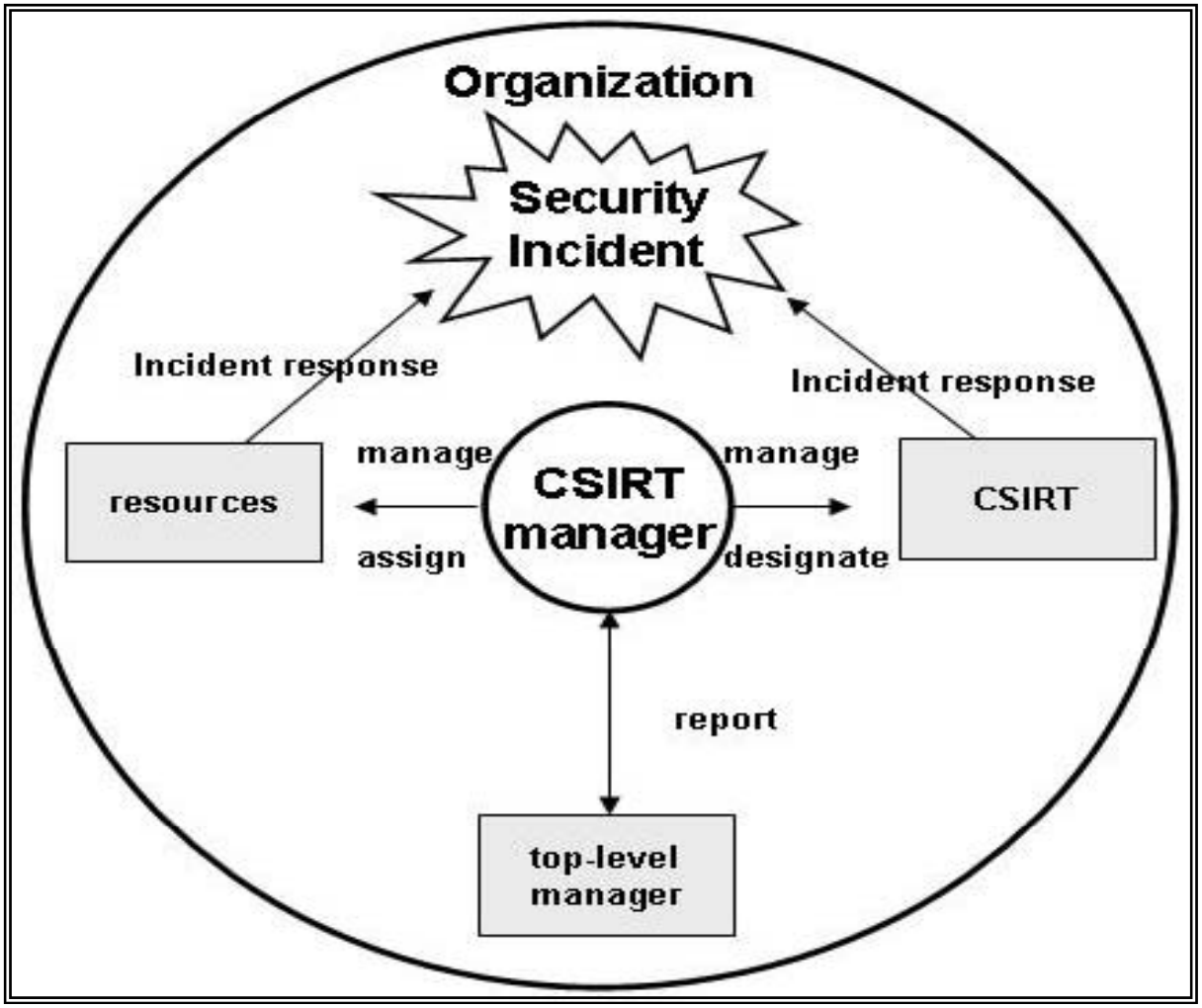
Model CSIRT

- Model CSIRT Terdistribusi Internal
  - Tim dalam model ini terdiri dari administrator CSIRT yang bertanggungjawab untuk pelaporan dan manajemen keseluruhan, dan staf dari divisi-divisi lain dari lembaga/perusahaan.



- ✓ **Perbandingan dengan model Tim Keamanan:**
- ❖ *Keberadaan kebijakan, prosedur, dan proses yang lebih formal untuk menangani insiden*
- ❖ *Ditetapkannya metode komunikasi dengan keseluruhan perusahaan terkait ancaman keamanan dan strategi penanganan; dan*
- ❖ *Manajer dan anggota tim CSIRT yang ditunjuk dan ditugaskan secara khusus untuk penanganan insiden*

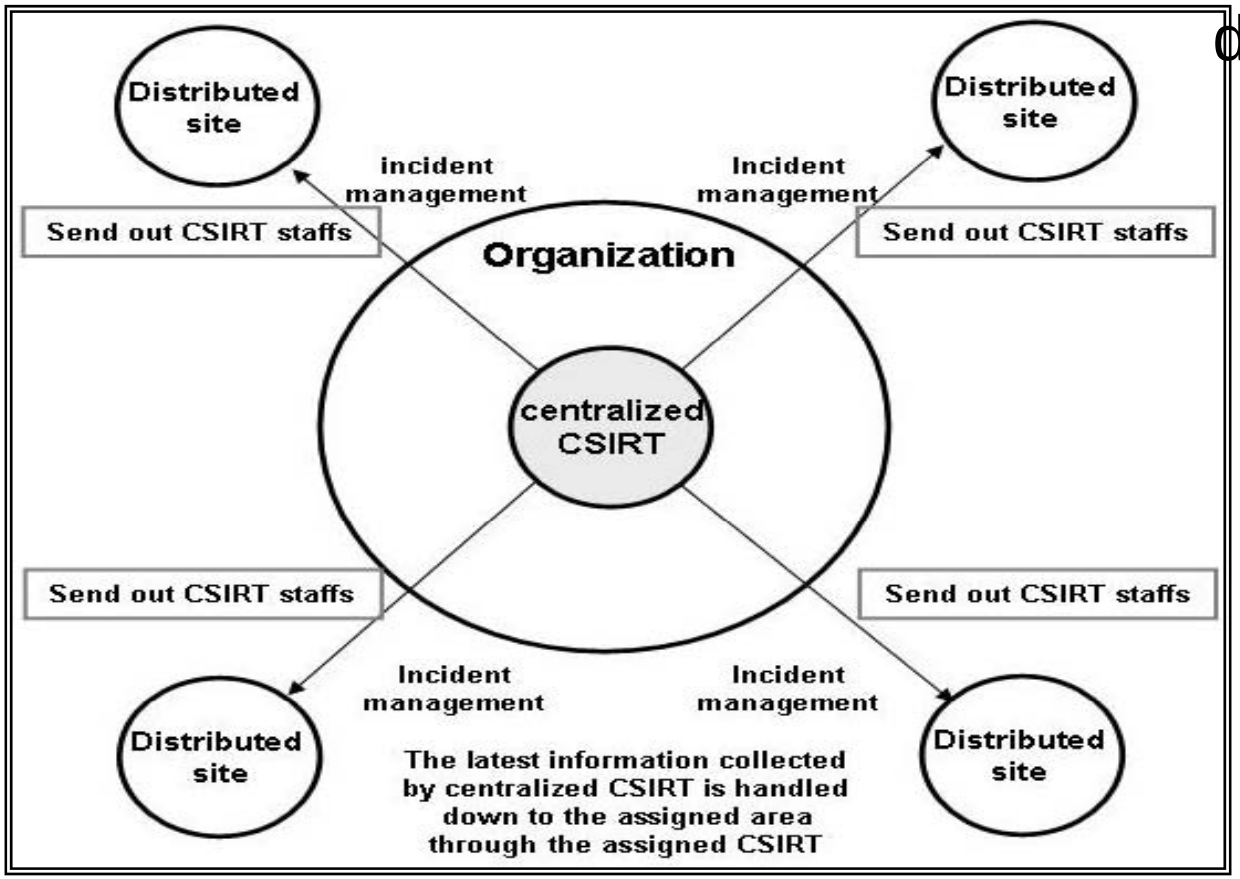
Model CSIRT



Model CSIRT Terpusat Internal

- Tim yang lokasinya terpusat mengendalikan dan mendukung organisasi
- CSIRT memiliki tanggung jawab menyeluruh terhadap pelaporan, analisis dan penanganan insiden
- Anggota tim menghabiskan seluruh waktu menangani seluruh insiden

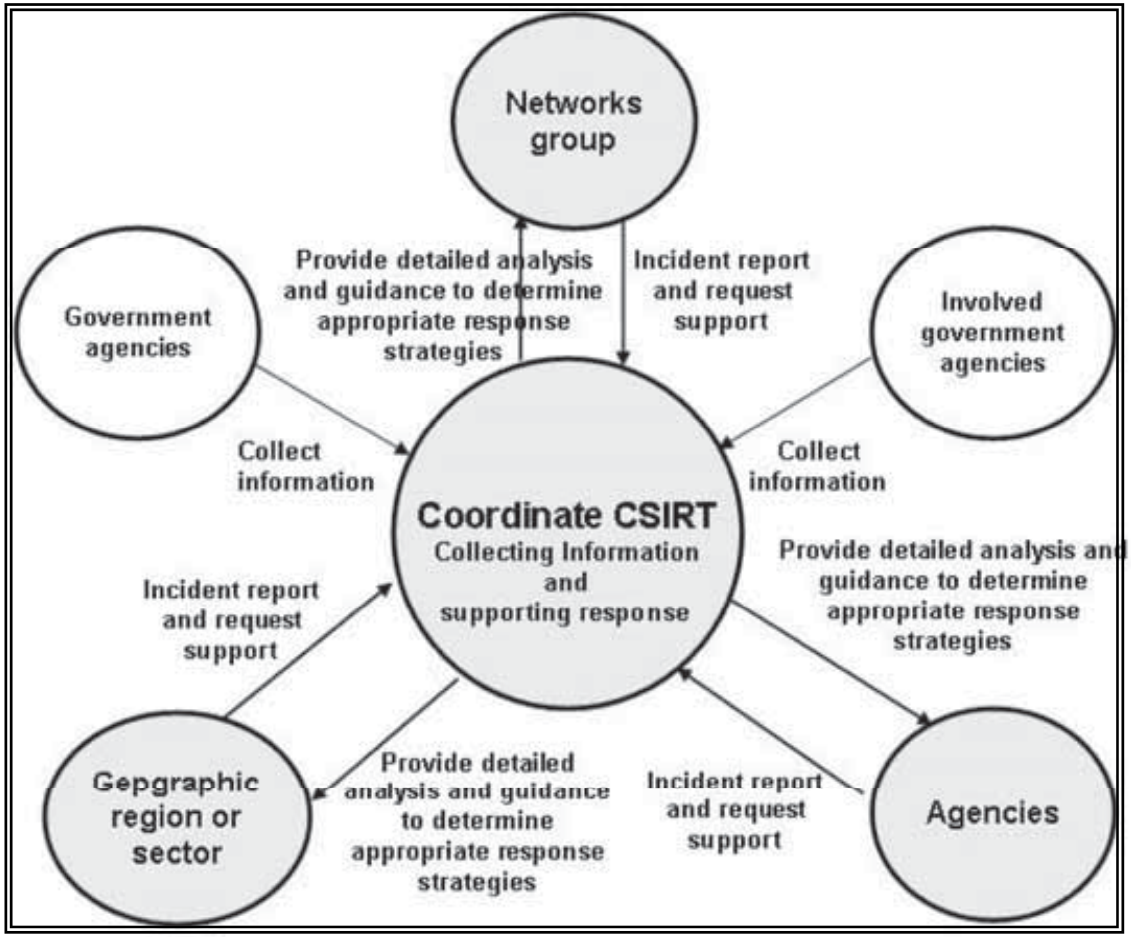
Model CSIRT



Model CSIRT Gabungan Terdistribusi dan Terpusat

- Dimana CSIRT terpusat tidak dapat mengendalikan dan mendukung keseluruhan organisasi, beberapa anggota tim didistribusikan ke lokasi/cabang/divisi organisasi untuk menyediakan tingkat pelayanan yang sama dalam area tanggung jawab mereka seperti yang disediakan pada CSIRT terpusat

Model CSIRT



Model CSIRT Terkoordinasi

- Anggota tim dalam CSIRT kombinasi dikelompokkan kedalam CSIRT independen berdasarkan pada beberapa karakteristik seperti konektivitas jaringan, batas geografis, dan lain-lain.
- Mereka dikendalikan oleh CSIRT terpusat.

Pembentukan CSIRT

- Lima tahapan dalam membentuk CSIRT
- Tahap 1 - tingkat kesadaran
  - *Stakeholder* mengembangkan pemahaman atas apa yang perlu dilakukan dalam membentuk CSIRT.

✓ **Isi Pendidikan Utama:**

1. *Pendorong dan motivator*
2. *Kebutuhan untuk mengembangkan kemampuan penanganan insiden oleh CSIRT*
3. *Mengidentifikasi orang-orang dalam CSIRT*
4. Mempelajari *sumber daya dan infrastruktur penting yang ada*
5. *Jenis-jenis saluran komunikasi yang perlu ditentukan untuk berkomunikasi*
6. *Hukum, peraturan dan kebijakan yang memengaruhi pengembangan CSIRT*
7. *Strategi pembiayaan*
8. *Teknologi dan infrastruktur informasi jaringan yang diperlukan CSIRT*
9. Mempelajari *teknologi dan infrastruktur informasi jaringan*
10. *Rencana dan interdependensi penanganan dasar yang akan digunakan*
11. *Sekumpulan layanan utama yang berpotensi*
12. *Praktik dan pedoman terbaik*

Pembentukan CSIRT

- Tahap 2 – Perencanaan CSIRT
  - **Berdasarkan pengetahuan dan informasi yang didapat selama Tahap 1**

✓ **Usulan Kegiatan**

1. *Identifikasi persyaratan dan kebutuhan CSIRT nasional*
2. *Mendefinisikan visi CSIRT nasional*
3. *Mendefinisikan misi tim nasional*
4. *Menentukan konstituen yang akan dilayani*
5. *Mengidentifikasi cara berkomunikasi*
6. *Mengidentifikasi jenis-jenis persetujuan, kepem impinan dan dukungan pemerintah*
7. *Mengidentifikasi jenis-jenis keahlian dan pengetahuan staf yang diperlukan*
8. *Mendefinisikan peran dan tanggungjawab*
9. *Menyusun proses manajemen insiden*
10. *Mengembangkan sekumpulan kriteria standar dan terminologi yang konsisten*
11. *Mendefinisikan hubungan CSIRT dengan mitra*
12. *Menentukan proses yang dibutuhkan untuk integrasi*
13. *Menyusun rencana CSIRT nasional*

Pembentukan CSIRT

- Tahap 3 – Implementasi CSIRT
  - Tim proyek menggunakan informasi dan rencana dari Tahap 1 dan 2 untuk mengimplementasikan CSIRT

✓ **Proses implementasi:**

1. Mendapatkan dana
2. Mengumumkan secara luas bahwa CSIRT nasional sedang dibentuk
3. Penyusunan mekanisme koordinasi dan komunikasi
4. Implementasi sistem informasi dan infrastruktur jaringan
5. Mengembangkan operasi dan proses untuk staf CSIRT
6. Pengembangan kebijakan dan prosedur internal
7. Implementasi proses interaksi CSIRT nasional dengan konstituennya
8. Merekrut personel
9. Mendidik dan melatih staf CSIRT

Pembentukan CSIRT

- Tahap 4 – Pengoperasian CSIRT
  - Layanan dasar yang harus disediakan oleh CSIRT nasional didefinisikan dan efisiensi operasional untuk memanfaatkan kemampuan manajemen insiden dievaluasi

✓	**Aktivitas tahap operasional:**
1.	Secara aktif melaksanakan berbagai layanan
2.	Mengembangkan dan melaksanakan mekanisme evaluasi efektivitas operasi CSIRT nasional
3.	Meningkatkan CSIRT nasional berdasarkan hasil evaluasi
4.	Memperluas misi, layanan dan staf yang tepat dan dapat bertahan untuk meningkatkan layanan
5.	Melanjutkan pengembangan dan peningkatan kebijakan dan prosedur CSIRT

Pembentukan CSIRT

➢ Tahap 5 – Kolaborasi

- ❖ CSIRT nasional perlu bertukar informasi dan pengalaman dalam menangani insiden melalui kerjasama jangka panjang dengan CSIRT domestik, CSIRT internasional, atau institusi lain.

✓ **Aktivitas kolaborasi**

1. *Berpartisipasi dalam kegiatan berbagi data dan informasi serta mendukung pengembangan standar berbagi data dan informasi*
2. *Berpartisipasi secara global dalam fungsi sebagai 'watch dan warning' untuk mendukung komunitas CSIRT*
3. *Meningkatkan kualitas kegiatan CSIRT dengan menyediakan pelatihan, workshop dan konferensi yang membahas tren serangan dan strategi penanganan*
4. *Kolaborasi dengan pihak lainnya dalam komunitas untuk mengembangkan dokumen dan pedoman praktik terbaik*
5. *Meninjau dan merevisi proses untuk manajemen insiden*

Operasi dan Layanan CSIRT

- Layanan Reaktif
  - Layanan inti CSIRT
  - Tujuan: menanggapi ancaman dan kelemahan
  - Ada 11 layanan reaktif (lihat slide berikutnya)
- Layanan Proaktif
  - Tujuan: meningkatkan proses keamanan dan infrastruktur dari lembaga konstituen sebelum insiden terjadi atau terdeteksi
- Layanan Manajemen Kualitas Keamanan
  - Tujuan: memberikan pengetahuan yang didapat dari penanganan insiden, kerentanan dan serangan dalam satu kesatuan

Operasi dan Layanan CSIRT

Kategori Layanan	Layanan		Tim Keamanan	Terdistribusi	Terpusat	Gabungan	Terkoordinasi
Reaktif	Siaga dan Peringatan		Tambahan	Inti	Inti	Inti	Inti
	Pena-nganan Insiden	Analisis Insiden	Inti	Inti	Inti	Inti	Inti
		Penanganan Insiden di Lokasi	Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
		Bantuan Penanganan Insiden	Tidak biasa	Inti	Inti	Inti	Inti
		Koordinasi Penanganan Insiden	Inti	Inti	Inti	Inti	Inti
	Pena-nganan Artefak	Analisis Kerentanan	Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
		Penanganan Kerentanan	Inti	Tambahan	Tidak biasa	Tambahan	Tambahan
		Koordinasi Penanganan Kerentanan	Tambahan	Inti	Inti	Inti	Inti
		Analisis Artefak	Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
		Penanganan Artefak	Inti	Tambahan	Tambahan	Tambahan	Tambahan
		Koordinasi Penanganan Artefak	Tambahan	Tambahan	Inti	Inti	Inti
Proaktif	Pemberitahuan		Tidak biasa	Inti	Inti	Inti	Inti
	Pengawasan Teknologi		Tidak biasa	Tambahan	Inti	Inti	Inti
	Audit atau Penilaian Keamanan		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Konfigurtasi dan pemeliharaan perangkat, aplikasi, infrastruktur, dan layanan keamanan		Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
	Pengembangan Perangkat Keamanan		Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
	Layanan Deteksi Penyusupan		Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
	Penyebaran Informasi Terkait Keamanan		Tidak biasa	Tambahan	Inti	Inti	Inti
Manajemen Kualitas Keamanan	Analisis Risiko		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Perencanaan Keberlangsungan Bisnis dan Pemulihan Bencana		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Konsultasi Keamanan		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Peningkatan Kesadaran		Tidak biasa	Tambahan	Tambahan	Tambahan	Inti
	Pendidikan/Pelatihan		Tidak biasa	Tambahan	Tambahan	Tambahan	Inti
	Evaluasi atau Sertifikasi Produk		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan

Status CSIRT International Saat Ini

- FIRST (*Forum of Incident Response Security Teams*)
  - Terdiri dari CERT, lembaga pemerintah dan perusahaan keamanan dari 41 negara
  - Tujuan: mengaktifkan kegiatan penanganan insiden dan perlindungan, serta memotivasi kerjasama antar anggota dengan memberikan mereka teknologi, pengetahuan dan perangkat untuk menangani insiden

✓ **Aktivitas FIRST**

1. *Pengembangan dan berbagi praktik terbaik*
2. *Memotivasi pengembangan kebijakan, layanan dan produk keamanan berkualitas baik*
3. *Mendukung dan mengembangkan pedoman keamanan komputer yang tepat*
4. *Membantu pemerintah, pengusaha dan lembaga pendidikan untuk membangun sebuah tim penanganan insiden dan memperluasnya*
5. *Memfasilitasi dalam berbagi teknologi, pengalaman dan pengetahuan diantara anggota untuk lingkungan elektronik yang lebih aman*

Status CSIRT International Saat Ini

- APCERT (Asia Pacific CERT) - http://www.apcert.org
  - Komite CERT di kawasan Asia - Pasifik
  - APCERT telah memiliki 14 anggota tetap dan 6 anggota asosiasi
  - Konsep terpenting dalam APCERT adalah hubungan saling percaya antara anggota untuk saling bertukar informasi dan bekerjasama.

✓ **Tujuan kegiatan APCERT**

1. *Meningkatkan kerjasama regional dan internasional Asia-Pasifik*
2. *Membangun langkah bersama untuk menangani insiden keamanan jaringan regional atau skala besar*
3. *Meningkatkan berbagi informasi dan pertukaran teknologi keamanan*
4. *Meningkatkan kerjasama penelitian terhadap masalah umum*
5. *Membantu CERT lainnya di kawasan*
6. *Memberikan saran dan solusi masalah hukum terkait dengan keamanan informasi dan penanganan insiden regional*

Status CSIRT International Saat Ini

- EGC (European Government CERT)
  - EGC adalah komite non-resmi yang berhubungan dengan CSIRT di negara-negara Eropa
  - Tujuan: Mengaktifkan kerjasama yang efektif dengan anggota dalam penanganan insiden

✓ **Peran dan Tanggung Jawab EGC**

1. Membangun langkah bersama untuk menangani insiden keamanan jaringan re gional atau skala besar
2. Meningkatkan berbagi informasi dan pertukaran teknologi terkait insiden keam anan dan ancaman kode berbahaya serta kerentanan
3. Mengidentifikasi area-area pengetahuan dan keahlian yang dapat dibagi
4. Mengidentifikasi area-area untuk kerjasama penelitian dan pengembangan
5. Mendorong formasi CSIRT pemerintah di negara-negara Eropa

Status CSIRT International Saat Ini

- ENISA (*European Network and Information Security Agency*)
  - Tujuan: meningkatkan keamanan jaringan dan keamanan informasi di Uni Eropa (UE)
  - Berkontribusi terhadap usaha internasional untuk mitigasi virus dan *hacking* serta pengawasan *online* terhadap ancaman

✓ **Peran ENISA**

1. *Memberikan dukungan untuk memastikan NIS diantara anggota ENISA atau UE*
2. *Membantu menstabilkan pertukaran informasi antara stakeholder; dan*
3. *Meningkatkan koordinasi fungsi yang terkait dengan NIS*

Rangkuman

- Pengembangan dan Operasi CSIRT
  - Tinjauan
  - Model CSIRT dan Memilih Model CSIRT yang tepat
  - Pembentukan CSIRT
  - Operasi & Layanan CSIRT

- Status CSIRT saat ini
  - CSIRT Internasional

Tugas

- Apakah ada CSIRT nasional di negara Anda?
  - Jika ya, jelaskan model apakah yang digunakan dan bagaimana mereka bekerja. Nilai seberapa efektif mereka dalam melaksanakan fungsinya.
  - Jika tidak, tentukan model CSIRT mana yang tepat untuk negara Anda dan jelaskan apa yang diperlukan untuk membentuk CSIRT nasional di negara Anda.

Modul 6: Keamanan Jaringan dan Keamanan Informasi dan Privasi

Sesi 6: Daur Hidup Kebijakan Keamanan Informasi

Tujuan Pembelajaran

- Mengetahui komponen utama yang harus diperhitungkan oleh pembuat kebijakan ketika menyusun kebijakan keamanan informasi nasional dan pelaksanaannya

- Termasuk proses persiapan, pembuatan, pelaksanaan, kontrol, dan umpan balik sebelum kebijakan informasi keamanan dibuat, dan pertimbangan pembuat kebijakan terhadapnya.

Konten

- Pengumpulan Informasi
- Analisis kesenjangan
- Merumuskan Kebijakan Keamanan Informasi
  - Menentukan arah kebijakan dan mendorongnya
  - Konstitusi organisasi keamanan informasi
  - Penetapan kerangka kerja kebijakan
  - Penyusunan dan/atau pengubahan hukum
  - Pengalokasian anggaran
- Implementasi/Pelaksanaan Kebijakan
- Peninjauan dan Evaluasi Kebijakan Keamanan Informasi

Daur Hidup Kebijakan Keamanan Informasi

Pengumpulan informasi

- Pengumpulan kasus dari luar negeri

  Dalam menemukan kasus yang relevan dari negara lain, penyusun kebijakan perlu memperhatikan kesamaan dalam:

  - Tingkat keamanan informasi nasional
  - Arah pembentukan kebijakan
  - Infrastruktur jaringan dan sistem
- Pengumpulan materi dalam negeri
  - Karena hukum, peraturan dan kebijakan cenderung fokus pada area tertentu, korelasi antara mereka mungkin tidak langsung terlihat jelas oleh penyusun kebijakan.
  - Karena itu, terdapat kebutuhan untuk mengumpulkan dan menganilisis serta mengevaluasi semua hukum, peraturan dan kebijakan yang terkait dengan keamanan informasi.

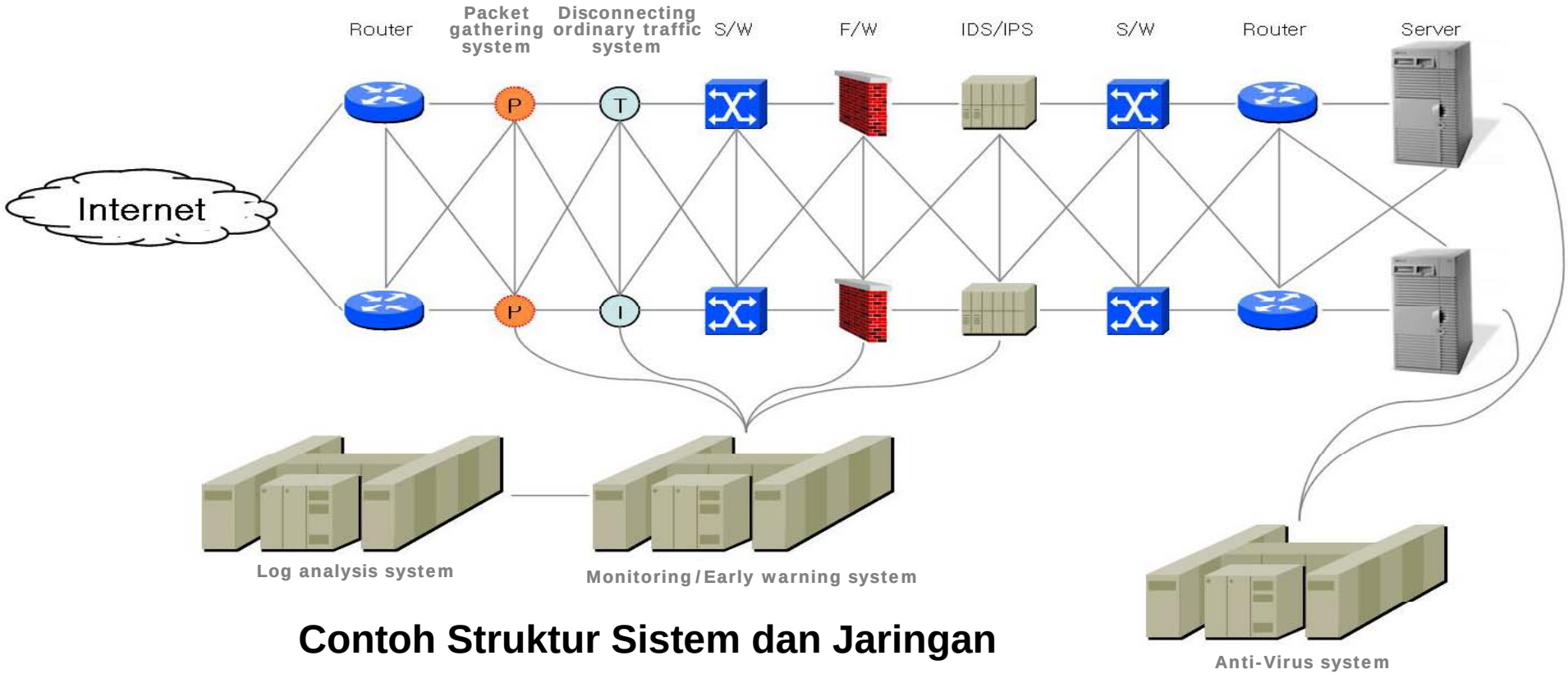
Analisis kesenjangan

- Analisis kesenjangan dapat dibagi menjadi dua fase:
  1. Memahami kemampuan dan kapasitas negara – yaitu sumber daya manusia dan organisasi, serta infrastruktur informasi dan komunikasi – dalam bidang umum keamanan informasi; dan

  2. Mengidentifikasi ancaman eksternal pada keamanan informasi.

Analisis kesenjangan

- Fase Pertama
  - **Memahami status infrastruktur informasi-komunikasi saat ini**



Contoh Struktur Sistem dan Jaringan

Analisis kesenjangan

- Fase kedua
  - Identifikasi ancaman keamanan informasi eksternal
  - Khususnya, penyusun kebijakan perlu memahami:
    - ✓Tingkat penetrasi ancaman pada keamanan informasi
    - ✓Jenis serangan terbaru dan yang paling umum
    - ✓Jenis-jenis ancaman dan tingkat kekuatan mereka di masa mendatang

Merumuskan Kebijakan Keamanan Informasi

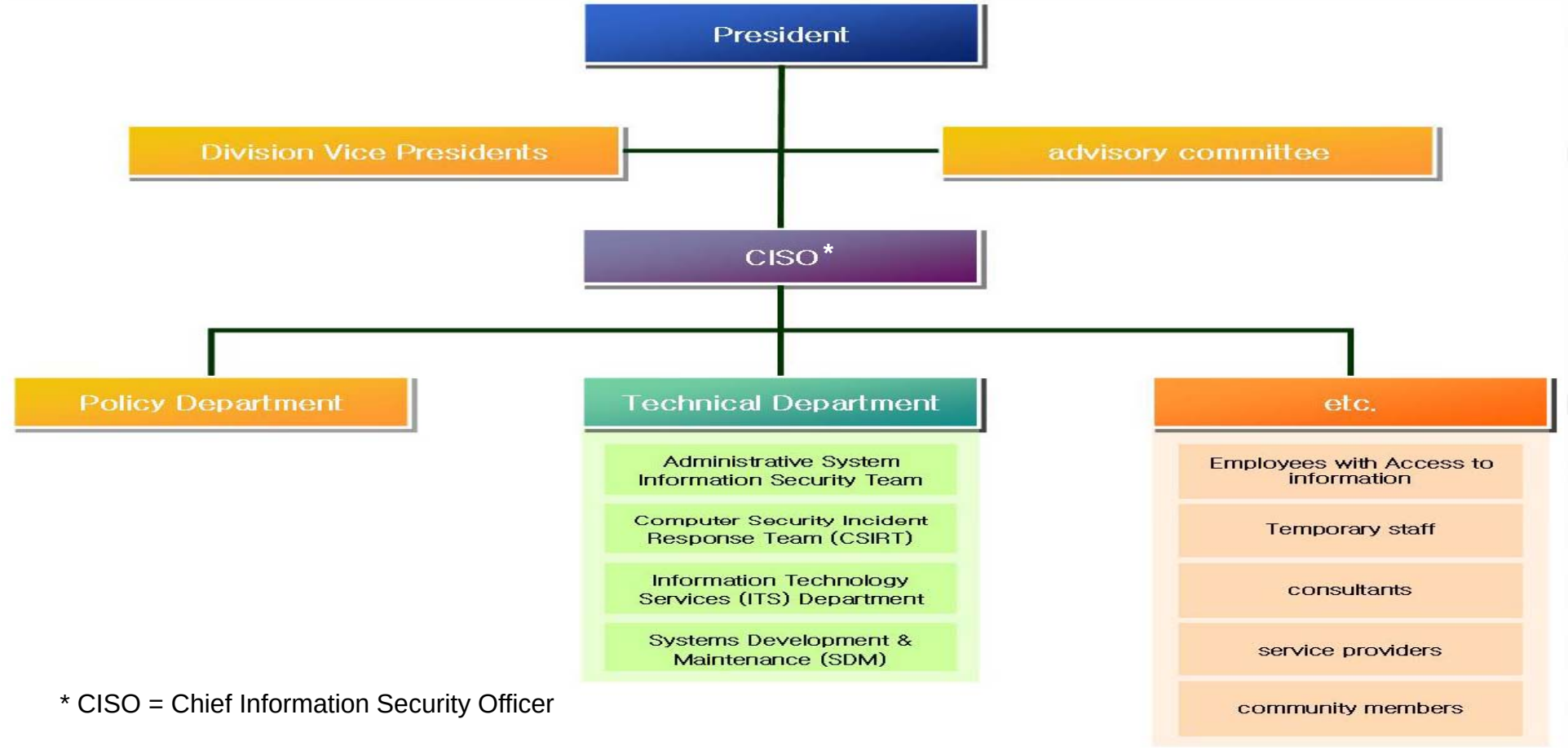
- Merumuskan kebijakan keamanan informasi nasional mencakup:
  1. Menentukan arah kebijakan
  2. Membentuk organisasi keamanan informasi beserta peran dan tanggung jawabnya
  3. Menyatakan kerangka kerja kebijakan keamanan informasi
  4. Menyusun dan/atau merevisi hukum supaya konsisten dengan kebijakan; dan
  5. Mengalokasikan anggaran implementasi kebijakan informasi.

Merumuskan Kebijakan Keamanan Informasi - Menentukan arah kebijakan

- Penyusunan kebijakan keamanan informasi harus dipelopori oleh pemerintah ketimbang menyerahkannya ke sektor swasta
- Peran pemerintah: menetapkan kebijakan, berperanan penting dalam menyediakan infrastruktur yang diperlukan, dan memberikan dukungan jangka panjang
- Peran swasta: bergabung ke proyek ini kemudian, terutama untuk mengambil bagian dalam penelitian dan pengembangan, serta konstruksi sistem

Merumuskan Kebijakan Keamanan Informasi - Konstitusi organisasi keamanan informasi

- Struktur organisasi keamanan informasi nasional yang umum



* CISO = Chief Information Security Officer

Merumuskan Kebijakan Keamanan Informasi - Konstitusi organisasi keamanan informasi

- Division Vice-Presidents
  - Memiliki tanggung jawab utama terhadap informasi yang dikumpulkan, dipelihara dan/atau diidentifikasi serta dimanfaatkan atau ‘dimiliki’ oleh divisinya masing-masing
  - Dapat menunjuk seorang *information security officer* (ISO) dan individu lainnya untuk membantu ISO dalam melaksanakan kebijakan keamanan informasi
  - Harus memastikan bahwa aset informasi yang berada dalam kendali mereka telah ditunjuk pemiliknya, bahwa penilaian risiko telah dilaksanakan, dan proses mitigasi berdasarkan pada risiko-risiko tersebut telah diimplementasikan
- Pengawas (Direktur, Ketua, Manajer, dan lain-lain)
  - Mengatur pegawai yang memiliki akses ke informasi dan sistem informasi dan menentukan, melaksanakan dan menegakkan kontrol keamanan informasi yang digunakan di bidangnya masing-masing
  - Mereka harus memastikan bahwa semua pegawai mengerti tanggung jawab masing-masing terkait dengan keamanan informasi, dan bahwa pegawai memiliki akses yang diperlukan untuk melakukan pekerjaannya
  - Meninjau secara rutin semua tingkatan akses pengguna

Merumuskan Kebijakan Keamanan Informasi - Konstitusi organisasi keamanan informasi

- *Chief Information Security Officer* (CISO)
  - Bertanggung jawab untuk koordinasi dan pengawasan kebijakan keamanan informasi
  - Juga membantu pemilik informasi dengan praktik terbaik keamanan informasi dalam:
    - ✓ Menetapkan dan menyebarkan peraturan yang dapat dilaksanakan terkait akses dan penggunaan sumber daya informasi yang dapat diterima;
    - ✓ Melaksanakan/Koordinasi penilaian dan analisis risiko keamanan informasi;
    - ✓ Membuat pedoman dan langkah keamanan yang layak untuk melindungi data dan sistem;
    - ✓ Membantu pemantaian dan pengelolaan kerentanan keamanan sistem;
    - ✓ Melaksanakan/Koordinasi audit keamanan informasi; dan
    - ✓ Membantu investigasi/penyelesaian masalah dan/atau dugaan pelanggaran kebijakan keamanan informasi nasional

Merumuskan Kebijakan Keamanan Informasi - Konstitusi organisasi keamanan informasi

- *Computer Security Incident Response Team* (CSIRT)
  - Memberikan informasi dan membantu *stakeholder* dalam pelaksanaan langkah proaktif untuk mengurangi risiko insiden keamanan komputer, dan dalam investigasi, penanganan dan meminimalkan kerusakan akibat dari insiden
  - Dua lapisan dalam CSIRT terdiri dari:
    - ✓ Tim operasional yang bertugas untuk identifikasi awal, penanganan, *triage* dan penentuan kebutuhan eskalasi, dan
    - ✓ Tim manajemen yang bertugas untuk memelopori penanganan nasional terhadap insiden penting.
  - Operasional CSIRT terdiri atas: CISO dan staf TI
  - Tim manajemen CSIRT terdiri dari *Chief Information Officer*, *Chief of Police*, *Director of Public Information*, *Director of Information Technology Services*, *Director of Systems Development and Maintenance*, CISO, manajer sistem dan jaringan, penasihat hukum, penasihat sumber daya manusia, dan delegasi dengan keahlian teknis tertentu yang ditunjuk oleh *Vice President*

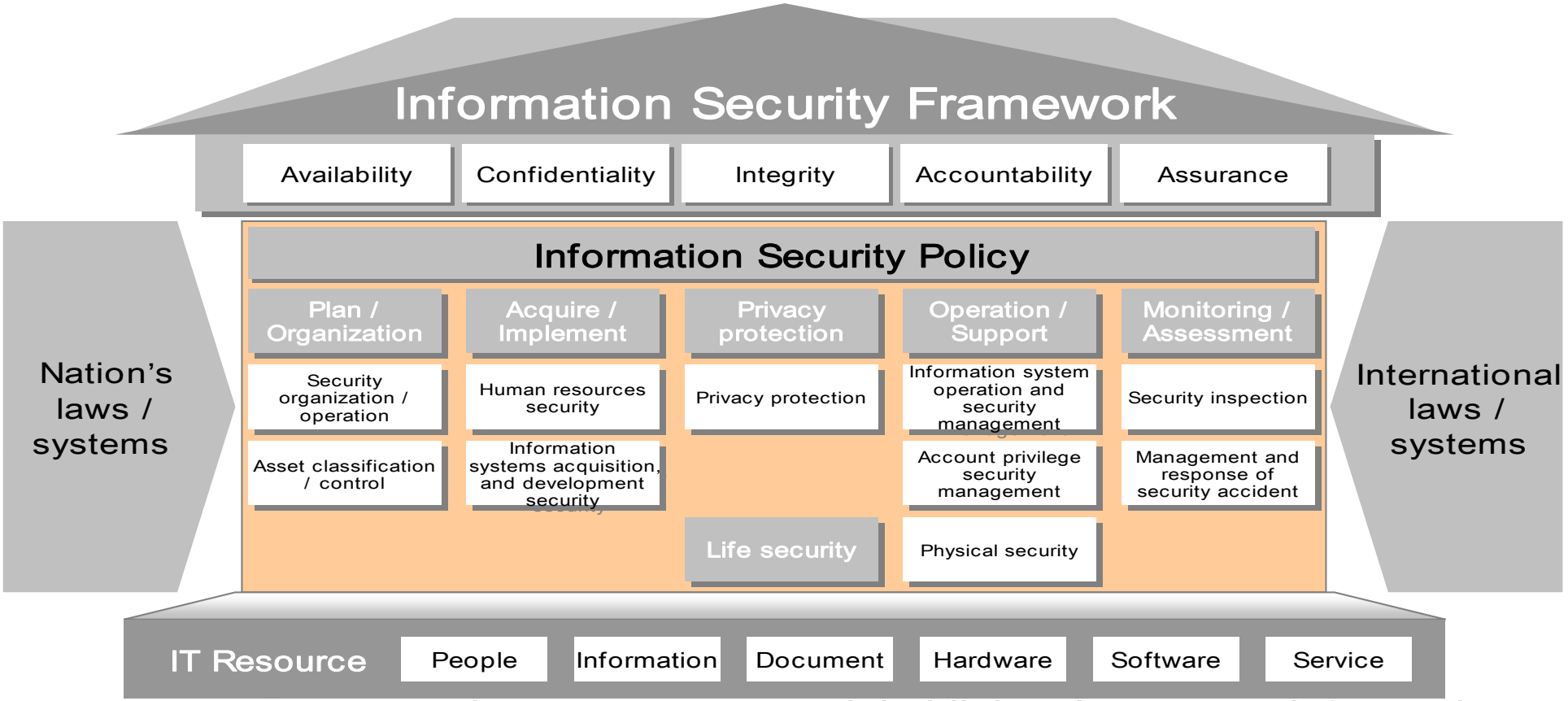
Merumuskan Kebijakan Keamanan Informasi - Konstitusi organisasi keamanan informasi

- Departemen Layanan Teknologi Informasi
  - Anggota staf mencakup: administrator sistem dan jaringan beserta penyedia layanan teknis.
  - Bertanggung jawab untuk: integrasi perangkat, kontrol, dan praktik keamanan informasi teknis dalam lingkungan jaringan.
  - Menerima laporan kegagalan keamanan informasi atau insiden yang dicurigai dari pengguna.
- Pengembangan dan Pemeliharaan Sistem
  - Anggota staf mencakup : pengembang dan administrator basisdata
  - Mengembangkan, mempraktikkan, mengintegra-sikan dan melaksanakan praktik terbaik keamanan untuk aplikasi nasional, dan melatih pengembang aplikasi *web* dalam penggunaan prinsip keamanan aplikasi.

Merumuskan Kebijakan Keamanan Informasi - Konstitusi organisasi keamanan informasi

- Pegawai dengan akses ke informasi
  - Harus patuh pada kebijakan dan prosedur nasional yang ada, serta praktik atau prosedur tambahan yang ditetapkan oleh atasan atau direktur mereka
  - Termasuk melindungi akun *password* mereka dan melaporkan penyalahgunaan informasi atau insiden keamanan informasi
- Pegawai tidak tetap
  - Dianggap sebagai pegawai dan memiliki tanggung jawab yang sama.
- Konsultan, penyedia layanan dan pihak ketiga yang dikontrak lainnya
  - Diberikan akses ke informasi pada basis ‘perlu mengetahui’ (*need to know*)
  - Akun jaringan yang dibutuhkan oleh pihak ketiga harus dimintakan oleh ‘sponsor’

Merumuskan Kebijakan Keamanan Informasi
- Penetapan kerangka kerja kebijakan



- Menentukan parameter untuk kebijakan keamanan informasi
- Memastikan kebijakan tersebut —
  - ✓ Mempertimbangkan sumber daya TI
  - ✓ Mencerminkan hukum dan peraturan internasional
  - ✓ Memenuhi prinsip ketersediaan, kerahasiaan, integritas, akuntabilitas dan jaminan informasi

Merumuskan Kebijakan Keamanan Informasi
- Penetapan kerangka kerja kebijakan

- Rencana dan Organisasi

Organisasi dan operasi keamanan

- Organisasi dan sistem dari organisasi keamanan informasi nasional
- Prosedur masing-masing organisasi keamanan informasi
- Konstitusi dan manajemen keamanan informasi nasional
- Kerjasama dengan lembaga internasional terkait
- Kerjasama dengan kelompok ahli

Klasifikasi dan kontrol aset

- Pemberian kepemilikan dan standar klasifikasi untuk aset informasi penting
- Instruksi pendaftaran dan penilaian risiko aset informasi penting
- Manajemen hak akses terhadap aset informasi penting
- Publikasi dan pengeluaran aset informasi penting
- Penilaian ulang dan pengakhiran aset informasi penting
- Manajemen keamanan dokumen

Merumuskan Kebijakan Keamanan Informasi - Penetapan kerangka kerja kebijakan

- Pengadaan dan Implementasi

Keamanan sumber daya manusia

- Langkah keamanan sumber daya manusia dan pelatihan keamanan
- Pemrosesan pelanggaran hukum dan peraturan keamanan
- Manajemen keamanan akses pihak ketiga
- Manajemen keamanan akses personel alih daya
- Manajemen pekerjaan pihak ketiga dan *outsourcing* pegawai
- Manajemen keamanan ruangan dan perlengkapan komputer
- Akses ke fasilitas dan bangunan utama.
- Pemrosesan insiden keamanan

Keamanan pengadaan dan pengembangan sistem informasi

- Pemeriksaan keamanan ketika sistem informasi diadakan
- Manajemen keamanan program aplikasi *in-house* maupun alih daya
- Sistem enkripsi nasional (program dan kunci enkripsi, dan sebagainya)
- Pengujian setelah pengembangan program
- Persyaratan keamanan yang disarankan ketika pengembangan di-alih daya-kan
- Verifikasi keamanan dalam pengadaan dan pengembangan

Merumuskan Kebijakan Keamanan Informasi - Penetapan kerangka kerja kebijakan

- Perlindungan Privasi
  - Dimasukkannya perlindungan privasi dalam kebijakan keamanan informasi bersifat tidak wajib.
  - Namun, akan lebih baik untuk menyertakannya mengingat perlindungan privasi adalah isu internasional

Ketentuan perlindungan privasi harus mencakup **:**

- Pengumpulan dan penggunaan informasi pribadi
- Permintaan izin sebelumnya ketika memanfaatkan privasi seseorang
- PIA

Merumuskan Kebijakan Keamanan Informasi - Penetapan kerangka kerja kebijakan

➢ Operasi dan Dukungan

Manajemen keamanan dan operasi sistem informasi

- Manajemen keamanan dan operasi *server*, jaringan, aplikasi dan basis data
- Pengembangan sistem keamanan informasi
- Catatan dan *back-up* dari aksi-aksi yang sah
- Manajemen penyimpanan informasi
- Komputasi *mobile*
- Standar untuk penjagaan dan pengamanan data komputer
- Layanan *e-commerce*

Manajemen keamanan hak akun

- Pendaftaran, penghapusan, manajemen hak pengguna sistem informasi nasional
- Manajemen akun dan hak dalam jaringan ter-enkripsi

Keamanan fisik

- Konfigurasi dan pengelolaan metode area keamanan
- Kontrol akses dan pengiriman untuk pusat komputer
- Pencegahan kerusakan dari bencana alam dan lainnya

Merumuskan Kebijakan Keamanan Informasi
- Penetapan kerangka kerja kebijakan

➢ Pemantauan dan Penilaian

Inspeksi keamanan

- Pembentukan rencana inspeksi keamanan
- Pelaksanaan inspeksi keamanan secara rutin
- Pengorganisasian/penyusunan bentuk laporan
- Pengidentifikasian subyek dari target inspeksi dan laporan keamanan

Manajemen dan penanganan insiden keamanan

- Tugas dan peran tiap organisasi dalam pemrosesan insiden keamanan
- Prosedur untuk memantau dan mengenali gejala insiden keamanan
- Prosedur pemrosesan insiden keamanan dan metode penanganan
- Langkah yang perlu dilakukan sesudah pemrosesan insiden keamanan

Merumuskan Kebijakan Keamanan Informasi - Penyusunan dan Pengubahan Hukum

- Hukum harus konsisten dengan kebijakan keamanan informasi. Perlu ada hukum yang mengatur organisasi pemerintah dan perusahaan swasta.

Hukum Terkait Keamanan Informasi di Jepang

Undang-undang	Target Industri	Target Peraturan	Hukuman
Unauthorized Computer Access Law	Semua industri	Tindakan yang membantu akses tidak sah dan memberikan informasi ID orang lain tanpa pemberitahuan	
Act on the Protection of Personal Information	Usaha swasta yang menggunakan informasi pribadi untuk tujuan bisnis	Manajemen informasi privasi (alamat, nomor telepon, *e-mail*, dll)	Hukum pidana, denda
Act on Electronic Signatures and Certification	-	Fasilitasi *e-commerce* yang mengambil manfaat dari Internet dan aktivitas ekonomi melalui jaringan	

Merumuskan Kebijakan Keamanan Informasi - Penyusunan dan Pengubahan Hukum

Hukum Terkait Keamanan Informasi di UE

Undang-undang	Rincian
A Common Regulatory Framework (Directive 2002/21/EC)	• Memberikan kerangka kerja pengaturan jaringan dan layanan telekomunikasi • Bertujuan untuk melindungi privasi melalui jaringan komunikasi yang aman
EU Directive on Data Protection (Directive 1995/46/EC)	• Pedoman pemrosesan dan penghapusan informasi pribadi • Hukum dasar yang menetapkan tanggung jawab negara anggota dan pengakuan kewenangan penuh individu atas informasi pribadi • Lebih ketat daripada standar AS
EU Directive on Electronic Signatures (Directive 1999/93/EC) *EU Directive on Electronic Commerce (Directive 2000/31/EC)*	• Mengatur penggunaan tanda tangan elektronik • Mengatur pelaksanaan *e-commerce*
Cybercrime Treaty	• Perjanjian internasional paling komprehensif mengenai *cybercrime*; mendefinisikan secara rinci semua aksi kriminal menggunakan Internet beserta dendanya
Data Preservation Guideline on Communication and Networks	• Mensyaratkan penyedia layanan komunikasi untuk mempertahankan data panggilan dari enam bulan sampai 24 bulan (diumumkan sesudah serangan teroris di tahun 2004 dan tahun 2005))

Merumuskan Kebijakan Keamanan Informasi - Penyusunan dan Pengubahan Hukum

Hukum Terkait Keamanan Informasi di AS

Undang-undang	Target Industri	Target Peraturan	Hukuman
Federal Information Security Management Act of 2002	Lembaga administratif federal	Informasi lembaga administratif, sistem TI, program keamanan informasi	-
Health Insurance Privacy and Accountability Act of 1996	Lembaga kesehatan dan penyedia layanan kesehatan	Data elektronik berisi informasi kesehatan seseorang	Hukum pidana, denda
Gramm-Leach-Bliley Act of 1999	Lembaga keuangan	Privasi informasi konsumen	Hukum pidana, denda
Sarbanes-Oxley Act of 2002	Perusahaan terdaftar pada *Stock Exchange of USA*	Kontrol internal dan catatan keuangan publik	Hukum pidana, denda
Database Security Breach Information Act of 2003	Lembaga administratif dan perusahaan swasta di California	Informasi privasi terenkripsi	Denda dan pemberitahuan pada korban

Merumuskan Kebijakan Keamanan Informasi - Pengalokasian anggaran

- *Anggaran perlindungan informasi di Jepang dan AS*

Jepang	2004	2005
Total anggaran tahunan	JPY 848.967.000.000.000	JPY 855.195.000.000.000
Anggaran keamanan informasi	JPY 267.000.000.000	JPY 288.000.000.000
Persentase dari total anggaran	0,03%	0,03%
AS	2006	2007
Total anggaran tahunan	USD 2.709.000.000.000	USD 2.770.000.000.000
Anggaran keamanan informasi	USD 5.512.000.000	USD 5.759.000.000
Persentase dari total anggaran	0,203%	0,208%

Latihan

- Jika negara Anda memiliki kebijakan keamanan informasi, lacak perkembangan-nya dari sisi lima aspek formulasi kebijakan keamanan informasi yang dijelaskan di atas. Artinya, jelaskan:
  1. Arah kebijakan
  2. Organisasi keamanan informasi
  3. Kerangka kerja kebijakan
  4. Hukum yang mendukung kebijakan keamanan informasi
  5. Alokasi biaya untuk keamanan informasi

Latihan

- Jika negara Anda belum memiliki kebijakan keamanan informasi, uraikan kemungkinan dari masing-masing lima aspek di atas dalam menyusun kebijakan. Gunakan pertanyaan-pertanyaan berikut sebagai panduan:
  1. Apa yang seharusnya menjadi arah kebijakan keamanan informasi di negara Anda?
  2. Bagaimana pengaturan organisasi yang harus ditempatkan? Organisasi mana yang perlu dilibatkan dalam pengembangan kebijakan keamanan informasi dan implementasinya di negara Anda?
  3. Apa permasalahan khusus yang harus diatasi oleh kerangka kerja kebijakan?
  4. Hukum apa yang harus ditetapkan dan/atau dicabut untuk mendukung kebijakan informasi?
  5. Apa pertimbangan anggaran yang harus diperhatikan? Dari mana sebaiknya dana didapatkan?

Implementasi/Pelaksanaan Kebijakan

- Pengembangan kebijakan keamanan informasi

Sektor	Kontribusi pada Pengembangan Kebijakan
Pemerintah	• Organisasi perencanaan dan strategi nasional: memastikan kecocokan kebijakan informasi dengan rencana nasional • Organisasi teknologi informasi dan komunikasi: memastikan kerjasama pembentukan standar teknologi keamanan informasi nasional • Organisasi analisis tren keamanan informasi: menggambarkan analisis dan tren keamanan domestik dan internasional dalam kebijakan • Organisasi analisis hukum: memeriksa kecocokan antara kebijakan keamanan informasi dan hukum yang ada • Organisasi informasi nasional: kerjasama dalam penentuan arah dan penetapan strategi • Lembaga investigasi: kerjasama dalam pemrosesan insiden keamanan
Sektor swasta	• Perusahaan konsultasi keamanan informasi: menggunakan agen profesional dalam penyusunan kebijakan keamanan informasi • Laboratorium teknologi keamanan informasi swasta: membentuk standar teknologi yang terkait dengan keamanan informasi • Departemen keamanan informasi di perguruan tinggi: memberikan keahlian dalam formulasi kebijakan
Organisasi internasional	• Memastikan pemenuhan standar kebijakan nasional • Kerjasama penanganan ancaman dan insiden internasional

Implementasi/Pelaksanaan Kebijakan

- Manajemen dan perlindungan infrastruktur informasi dan komunikasi

Sektor	Kontribusi pada Administrasi dan Perlindungan Infrastruktur Informasi dan Komunikasi
Sektor pemerintah	• Organisasi yang terkait dengan jaringan informasi dan komunikasi: menentukan komposisi dan tingkat keamanan jaringan informasi dan komunikasi nasional • Laboratorium teknologi informasi dan komunikasi: menyebarkan standar publik dan mengadopsi teknologi yang berguna
Sektor swasta	• Penyedia ISP: kerjasama dalam komposisi jaringan informasi dan komunikasi nasional • Laboratorium TIK: memberikan layanan pengembangan teknis dan bekerjasama dalam operasi teknologi keamanan dan infrastruktur informasi dan komunikasi yang stabil
Organisasi internasional	• Kerjasama dengan organisasi standar teknologi internasional untuk informasi dan komunikasi internasional, dan pengamanan teknologi informasi baru

Implementasi/Pelaksanaan Kebijakan

- Pencegahan dan penanganan terhadap ancaman dan insiden

Sektor	Kontribusi
Organisasi pemerintah	• Organisasi penanganan insiden keamanan: memberikan analisis situasi, menangani insiden *hacking*, dan teknologi untuk menangani pelanggaran dan insiden • Organisasi informasi nasional: menganalisis dan menginspeksi keamanan informasi yang terkait dengan pelanggaran dan insiden • Lembaga investigasi: bekerjasama dengan organisasi yang terlibat dalam penahanan dan penuntutan pelanggar • Organisasi yang memberikan evaluasi keamanan: menguji keamanan dan kehandalan produksi jaringan informasi dan keamanan informasi • Organisasi pendidikan keamanan informasi: menganalisis penyebab insiden keamanan informasi dan mendidik masyarakat untuk mencegah terulangnya insiden
Kelompok swasta	• Organisasi penanganan insiden swasta: memberikan dukungan penanganan dan teknis • Lembaga investigasi swasta: bekerjasama dengan lembaga investigasi pemerintah
Organisasi internasional	• Dalam kasus insiden dan ancaman internasional, melapor dan bekerja sama dengan Interpol, CERT/CC

Implementasi/Pelaksanaan Kebijakan

➢ Pencegahan insiden keamanan informasi

Sektor	Koordinasi
Organisasi pemerintah	• Agen pengawasan: pengawasan jaringan berkelanjutan dan deteksi ancaman keamanan yang lebih canggih • Agen pengumpulan: berbagi informasi dengan organisasi internasional dan situs-situs keamanan • Institusi pelatihan: pelatihan simulasi secara rutin untuk mengembangkan kemampuan untuk menangani pelanggaran dan kecelakaan keamanan informasi dengan cepat
Organisasi swasta	• Penyedia ISP, kontrol keamanan dan perusahaan anti-virus: menyediakan statistik lalu lintas, informasi jenis serangan dan profil *worm*/virus
Organisasi internasional	• Memberikan informasi jenis serangan, profil *worm*/virus, dan lain-lain

Implementasi/Pelaksanaan Kebijakan

➢ Keamanan privasi

Sektor	Koordinasi
Lembaga pemerintah	• Organisasi analisis sistem: melakukan bisnis berkaitan dengan informasi lokasi pribadi, dan analisis tren dalam perlindungan informasi pribadi internal dan eksternal • Organisasi perencanaan: meningkatkan hukum/sistem, langkah teknis/ administratif dan manajemen standar • Dukungan teknis: koordinasi sertifikasi pengguna *cyber* untuk bisnis • Organisasi pelayanan: kerjasama dukungan untuk penanganan pelanggaran privasi dan *spam*
Organisasi swasta	• Organisasi keamanan informasi pribadi: pendaftaran persyaratan dan mengatur asosiasi kerjasama untuk keamanan informasi personal • Konsultasi keamanan informasi pribadi
Organisasi Internasional	• Bekerja sama untuk menerapkan standar keamanan informasi pribadi internasional

Implementasi/Pelaksanaan Kebijakan

- Kerjasama internasional
  - Keamanan informasi tidak dapat dicapai melalui usaha satu negara saja karena pelanggaran keamanan informasi cenderung berlingkup internasional.
  - Jadi, kerjasama internasional dalam perlindungan keamanan informasi, baik di sektor pemerintahan maupun swasta, harus dilakukan.
    - ✓Untuk sektor swasta : CERT/CC
    - ✓Untuk pemerintah : ENISA (EU) dan ITU

Peninjauan dan Evaluasi Kebijakan Keamanan Informasi

- Aspek metode evaluasi kebijakan domestik:
  - Penggunaan organisasi audit
  - Revisi kebijakan keamanan informasi
  - Perubahan dalam lingkungan

Rangkuman

- Pengumpulan Informasi
- Analisis kesenjangan
- Merumuskan Kebijakan Keamanan Informasi
  - Menentukan arah kebijakan dan mendorongnya
  - Konstitusi organisasi keamanan informasi
  - Penetapan kerangka kerja kebijakan
  - Penyusunan dan/atau pengubahan hukum
  - Pengalokasian anggaran
- Implementasi/Pelaksanaan Kebijakan
- Peninjauan dan Evaluasi Kebijakan Keamanan Informasi

Tugas

- Identifikasi lembaga pemerintah dan organisasi swasta di negara Anda yang perlu bekerjasama dalam implementasi kebijakan keamanan informasi nasional. Identifikasi juga organisasi internasional yang perlu diajak bekerjasama.

- Untuk setiap bidang kerjasama dalam implementasi kebijakan informasi seperti terlihat pada Gambar 23, tentukan aksi atau aktivitas spesifik yang lembaga dan organisasi ini dapat lakukan.