

# LECTURE NOTES

## SECURITY MANAGEMENT

Taslim Rochmadi, Ir., Dipl.Ing., Dr.

[taslim@binus.ac.id](mailto:taslim@binus.ac.id)



## LEARNING OUTCOMES

1. Peserta diharapkan mampu mengidentifikasi, mengkarakteristikkan, dan dapat menyebutkan apa itu security.
2. Peserta diharapkan mengerti fungsi, definisi Manajemen security bagi organisasi.
3. Peserta dapat mengerti cara /metode manajemen security sebagai hal yang harus ada dalam IT service.
4. Untuk melaksanakannya, peserta dapat mengetahui adanya standard manajemen security.

### OUTLINE MATERI :

1. Pengertian Management Security
2. Konsep Dasar Management Security
3. Tujuan Management Security
4. Standard yang digunakan untuk Management Security
5. Developing a Strategic Security Process

# ISI

## 1. Pengertian Majemen Keamanan

Manajemen Keamanan merupakan beberapa kegiatan yang menyangkut keamanan, didalamnya ada proses yang harus dilakukan untuk menangani agar terjadinya gangguan keamanan dapat diatasi. Kegiatan ini dilakukan sesuai kebutuhan. Manajer keamanan yang bertanggung jawab untuk melaksanakan proses kegiatan ini. Yaitu dengan suatu Manajemen Keamanan, manajemen ini akan memberikan indikasi dan membentuk proses yang tepat agar keamanan khusus yang diberikan dalam kegiatan itu terstruktur.

## 2. Basic Consept

Konsep dasar manajemen keamanan adalah keamanan informasi.

- Tujuan utama dari keamanan informasi adalah untuk menjamin keamanan informasi. Keamanan informasi berarti melindungi informasi, yang artinya melindungi nilai yang ada pada informasi itu.
- Nilai-nilai ini ditentukan atau ditetapkan berdasarkan: kerahasiaan, integritas dan ketersediaan. Didalamnya tersirat aspek privasi, anonimitas dan pemastian/verifiability

## 3. Tujuan Security Management

Tujuan dari Manajemen Keamanan terbagi dalam dua bagian:

- **Realisasi persyaratan keamanan**, didefinisikan dengan Perjanjian Tingkat Layanan (SLA), dan bentuk persyaratan eksternal lainnya, yang biasanya ditentukan dalam kontrak. Jadi persyaratan keamanan ini yang akan mendukung, menjadi legislasi dan menjadi kebijakan yang secara riil dapat dipaksakan baik secara internal atau eksternal.

- **Realisasi tingkat dasar keamanan.** Adalah suatu keamanan yang diperlukan untuk menjamin kelangsungan organisasi. Dimana manajemen keamanan ini juga penting untuk mendapatkan service-level manajemen yang diperlukan untuk mencapai keamanan informasi.

#### 4. Standard yang digunakan

Kesesuaian suatu manajemen sekuriti dalam manajemen layanan sebagai yang ada pada ITIL v 3 adalah berdasarkan standar ISO 27001. Dimana ISO 27001 ini pun dikembangkan dari ISO 17799 maka untuk penjelasannya dapat dilihat pada diagram berikut.

Pertama dasar standard adalah:

- *ITIL security management is based on the ISO 27001 standard.*
- ISO/IEC 27001:2005
- *"ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties."*

#### ISO/IEC 27001:2005

ISO / IEC 27001:2005 menetapkan persyaratan untuk: penetapan, penerapan, melaksanakan/operasional, memonitor, mengkaji, memelihara dan meningkatkan dari Sistem Informasi Manajemen Keamanan. Persyaratan itu didokumentasikan dalam konteks mengetahui risiko keseluruhan organisasi/bisnis yang ada didalamnya. Semua yang ada pada ISO 27001 itu menentukan persyaratan pelaksanaan kontrol keamanan, namun disesuaikan dengan kebutuhan organisasi, baik hingga individu atau bagiannya.

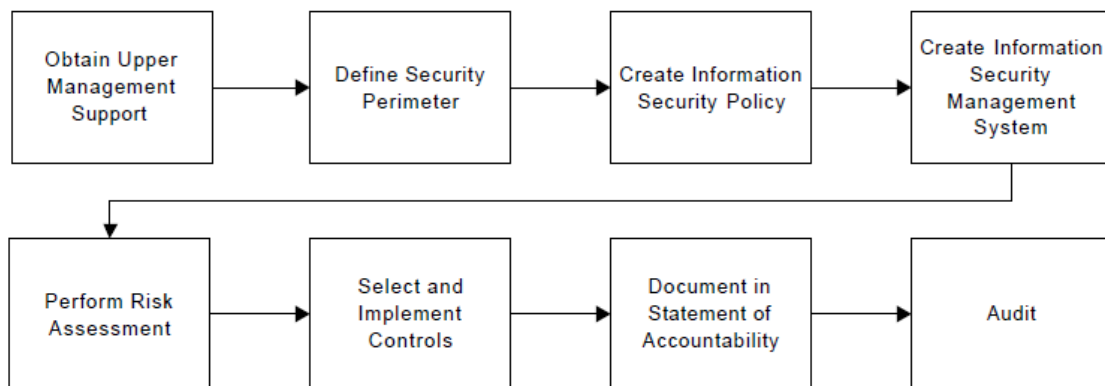
ISO 17799, information security is characterized as:

- **Confidentiality** – Memastikan informasi yang dapat diakses hanya untuk mereka yang berwenang untuk mendapatkan akses.
- **Integrity** – Menjaga ketepatan dan kelengkapan informasi dan metode pengolahan/pemrosesan
- **Availability** – Memastikan bahwa pengguna resmi memiliki akses ke informasi dan aset terkait bila diperlukan )

## 5. Process ISO 17799

The process for implementing information security management using ISO 17799 proceeds as shown in Figure 1.

**Figure 1: ISO 17799 Process**



ISO 17799 consists of 10 security controls:

- *Security Policy*
- *Organizational Security*
- *Asset Classification and Control*

- *Personnel Security*
- *Physical and Environmental Security*
- *Communications and Operations Management*
- *Access Control*
- *System Development and Maintenance*
- *Business Continuity Management*
- *Compliance*

## **6. Developing a Strategic Security Process**

- Pengertian:

Keamanan strategis dirancang untuk menjaga ketersediaan, integritas, dan kerahasiaan data dan program terhadap bentuk bentuk akses yang tidak sah, modifikasi, atau perusakan.

Dalam membentuk Keamanan Strategis ini ada beberapa langkah yang harus dilakukan, diantaranya disini di terapkan 12 Langkah yaitu:

12 step (Developing a Strategic Security)

- Identify an executive sponsor
- Select a process owner,
- Define goals of strategic security,
- Establish review board,
- Identify, categorize, and prioritize requirement,
- Inventory current state of security,

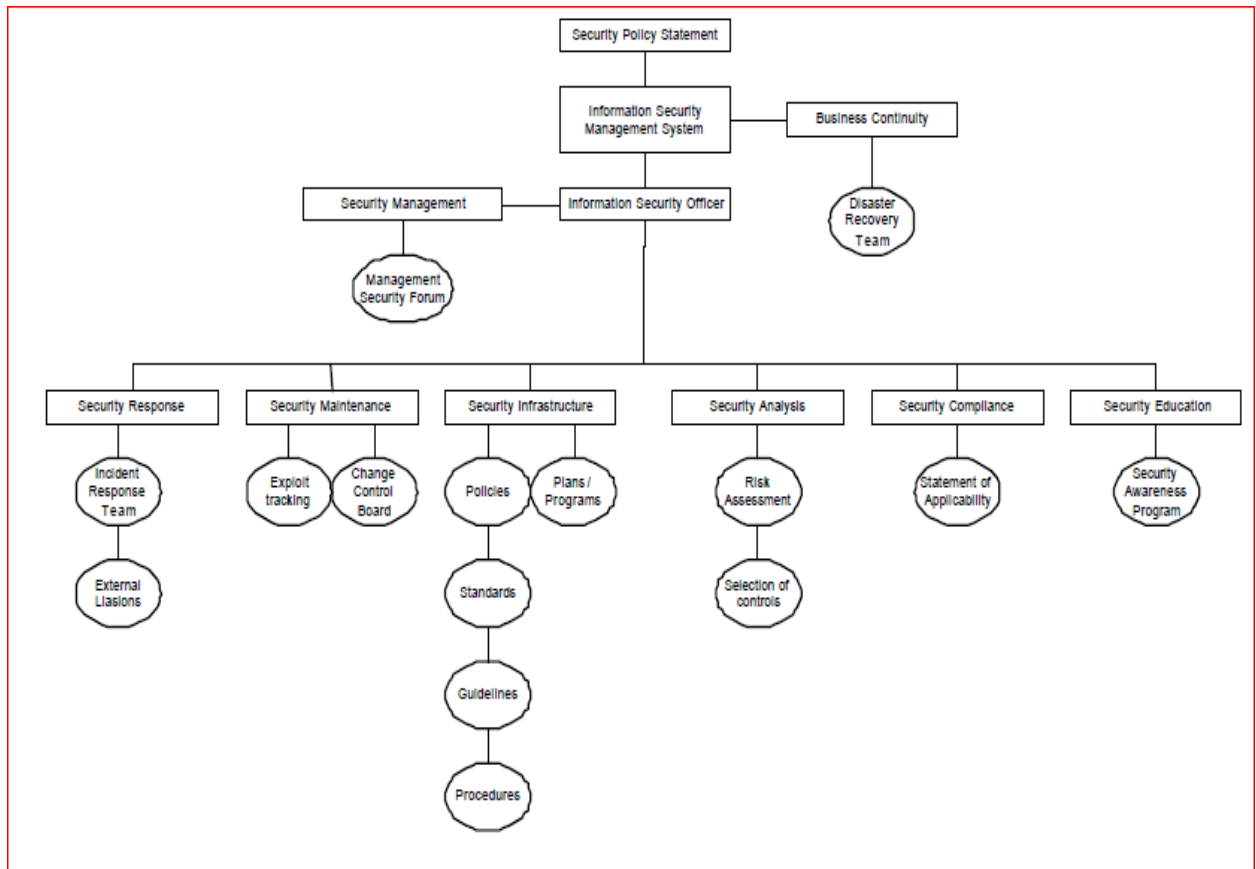
- Establish security organization,
- Develop security policies,
- Assemble planning teams,
- Review and approve plans
- Evaluate technical feasibility of plans
- Assign and schedule the implementation of plans.

Untuk menggambarkan lebih jelas lagi tentang proses yang ada dalam manajemen keamanan, disini dapat dijelaskan secara diagram dibawah yang intinya sebagai berikut:

Proses data model dibawah menjelaskan secara structural atas komponen-komponen yang menyusun system keamanan sehingga menjadi suatu statemen kebijakan keamanan.

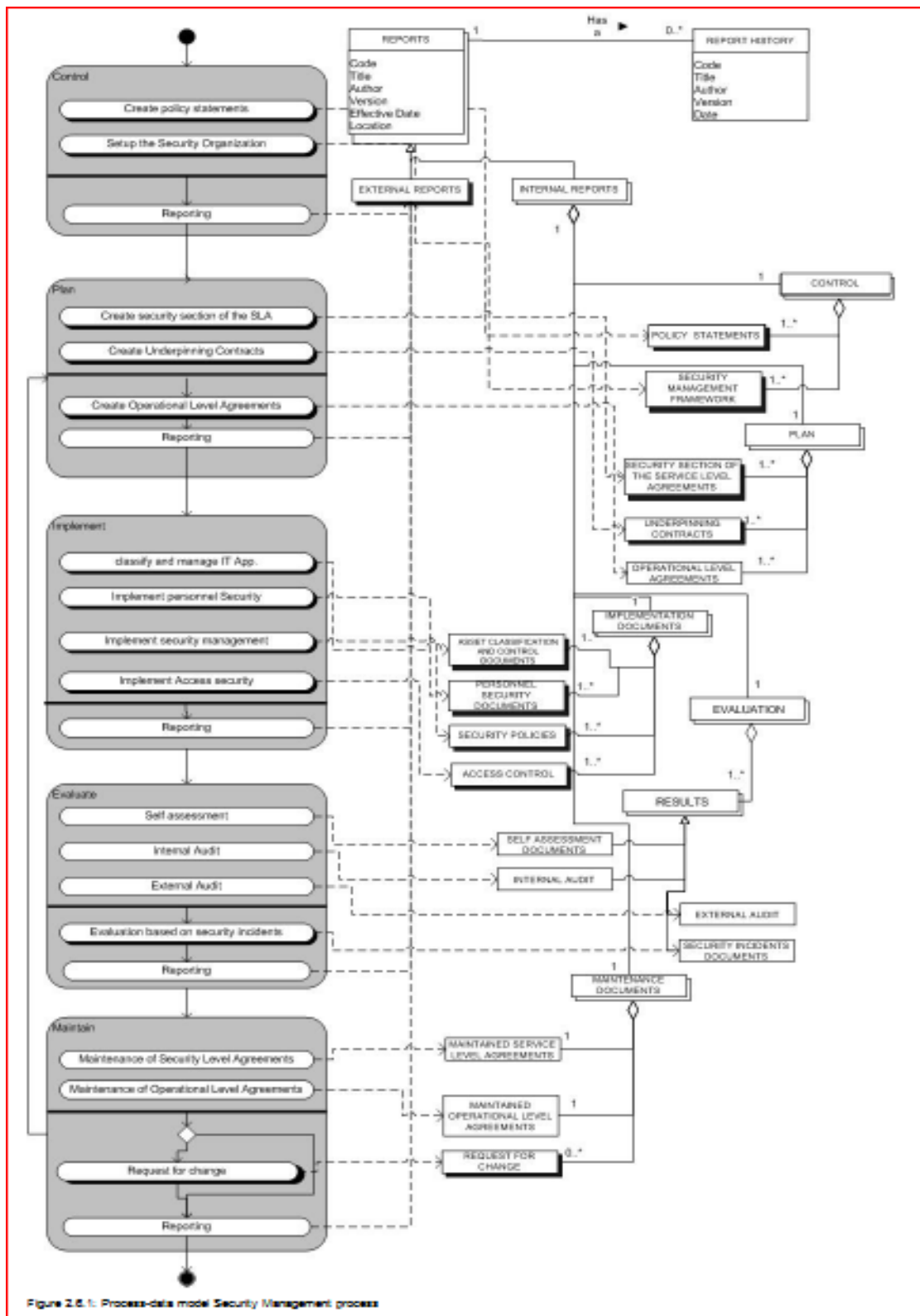
Information security officer yang bertanggung jawab pada seluruh keamanan informasi sebetulnya tergantung pada pelaksanaan dari: security education, security compliance, security analysis, security infrastructure, security maintenance, dan security response. Pengelolaannya ada dalam lingkup tata kelola security management. Sedangkan tujuan utamanya adalah bisnis continuity.

# The complete process-data model of the Security Management process





Adapun prosesnya secara diagramatik dapat ditelusur sebagai diagram berikut.



## SIMPULAN

Pengertian Management security sepenting dengan manajemen lainnya karena Security Management ini akan memberikan indikasi terhadap process manajemen, sehingga spesifik security yang khusus harus di strukturisasi dengan cara tertentu.

Basic concept atau konsep dasar security management berasal dari information security, dimana tujuan utama atau primary goal dari information security adalah menjamin keamanan atau safety dari informasi, dimana yang diproteksi dari informasi tersebut adalah Nilai atau 'the value'.

'values' akan ditunjukkan pada keadaan data didalamnya yang disifatkan dengan confidentiality, integrity dan availability. Didalamnya ada aspek aspek privacy, anonymity dan verifiability

Standard yang digunakan untuk Manajemen Security sesuai dengan ITIL security management adalah berdasar ISO 27001, yaitu standard ISO/IEC 27001:2005.

Dalam rangka pengembangan proses Strategic Security ada 12 step (Developing a Strategic Security)

## DAFTAR PUSTAKA

1. Rich Schiesser, IT Systems Management.2010. 2<sup>nd</sup> Edition.Chapter 16
2. ISO/IEC 27001:2005