Policy and Procedure (PnP)

KEBIJAKAN & PROSEDUR

Budi Rahardjo – 2025

Apa pentingnya?

- *Policy & Procedures* merupakan salah satu pilar dari security
- Dipersyaratkan oleh standar (ISO 27000 series)
- Komplemen dengan aspek teknis
- Paling sulit diterapkan (karena menyangkut orang dan organisasi)

- People
- Process
- Technology

ISO 27001 Domains (14)

Information security policies

Human resource security

Access control

Physical and environmental security

Operations security

Supplier relationships

Information security aspects of business continuity management

Organisation of information security

Asset management

Cryptography

Operations security

System acquisition, development and maintenance

Information security incident management

Compliance

The 14 domains of ISO 27001

1. A5 Information Security Policy
   2 CONTROLS
2. A6 Organizing information security
   7 CONTROLS
3. A7 Human resource security
   6 CONTROLS
4. A8 Asset management
   10 CONTROLS
5. A9 Access control
   14 CONTROLS
6. A10 Cryptography
   2 CONTROLS
7. A11 Physical and environmental security
   15 CONTROLS
8. A12 Operations security
   14 CONTROLS
9. A13 Communications security
   7 CONTROLS
10. A14 System acquisition, development, and maintenance | 13 CONTROLS
11. A15 Supplier relationships
    5 CONTROLS
12. A16 Information security incident management
    7 CONTROLS
13. A17 Information security aspects of business continuity management | 4 CONTROLS
14. A18 Compliance
    8 CONTROLS

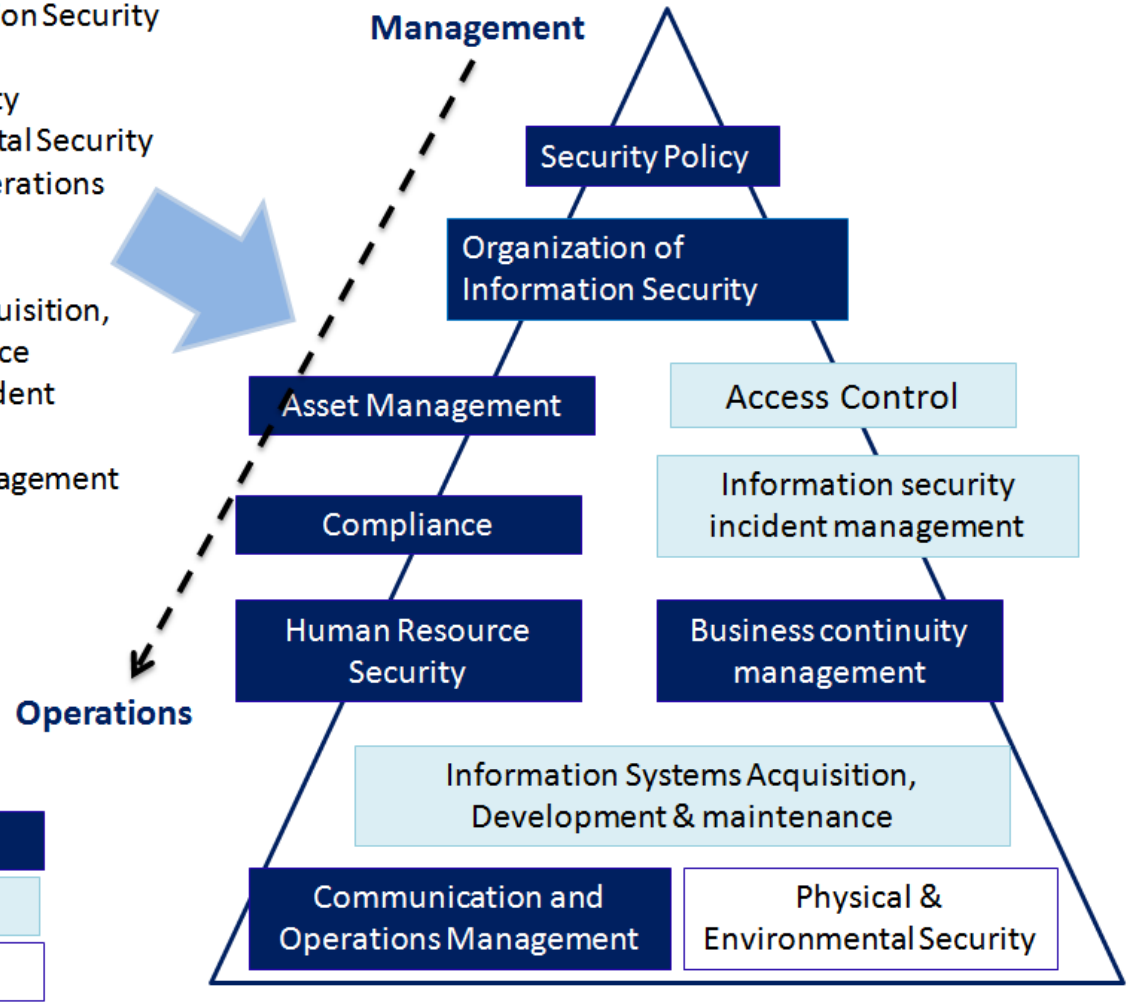
POSITIVE THINKING COMPANY

INDUCISC

The 11 ISO/IEC 27001 Domains

- ❑ Security Policy
- ❑Organization of Information Security
- ❑Asset Management
- ❑Human Resources Security
- ❑Physical and Environmental Security
- ❑Communications and operations management
- ❑Access control
- ❑Information Systems Acquisition, Development & maintenance
- ❑Information security incident management
- ❑Business Continuity Management
- ❑Compliance

Organizational Structure



Legend:

- Management Aspect
- Technical Aspect
- Physical Aspect

Apa Pentingnya PnP?

- Perangkat pengaman (seperti firewall) dipasang untuk menerapkan policy & procedures. Tanpa ada P&P, akan sulit untuk mengambil keputusan
  - Semua dilarang, kecuali yang diijinkan? (white list)
  - Semua boleh, kecuali yang dilarang? (black list)
  - Siapa yang boleh menjalankan aplikasi XYZ?
- Sering dianggap sebagai penghambat

Standar Kebijakan

- Standar yang lazim digunakan
  - **ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements.**
    Merupakan standar baku, namun agak kaku dan sulit untuk operasional
  - Terbaru: ?
  - ISO 27002 – code of practice
    Merupakan contoh kendali yang menjadi sorotan di ISO 27001

Standar Kebijakan (2)

- **Best practice**
  Lebih bersifat praktis dan operasional
  - Misal contoh-contoh dari SANS.org
    (**S**ysAdmin, **A**udit, **N**etworking, and **S**ecurity)
  - Dibutuhkan koleksi contoh/template untuk Indonesia

DEFINITIONS

Definisi

- *Policy*
  - Kebijakan yang singkat dan mengikat
  - Sangat spesifik kepada instansi
  - SANS:
    "A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities."

Definisi

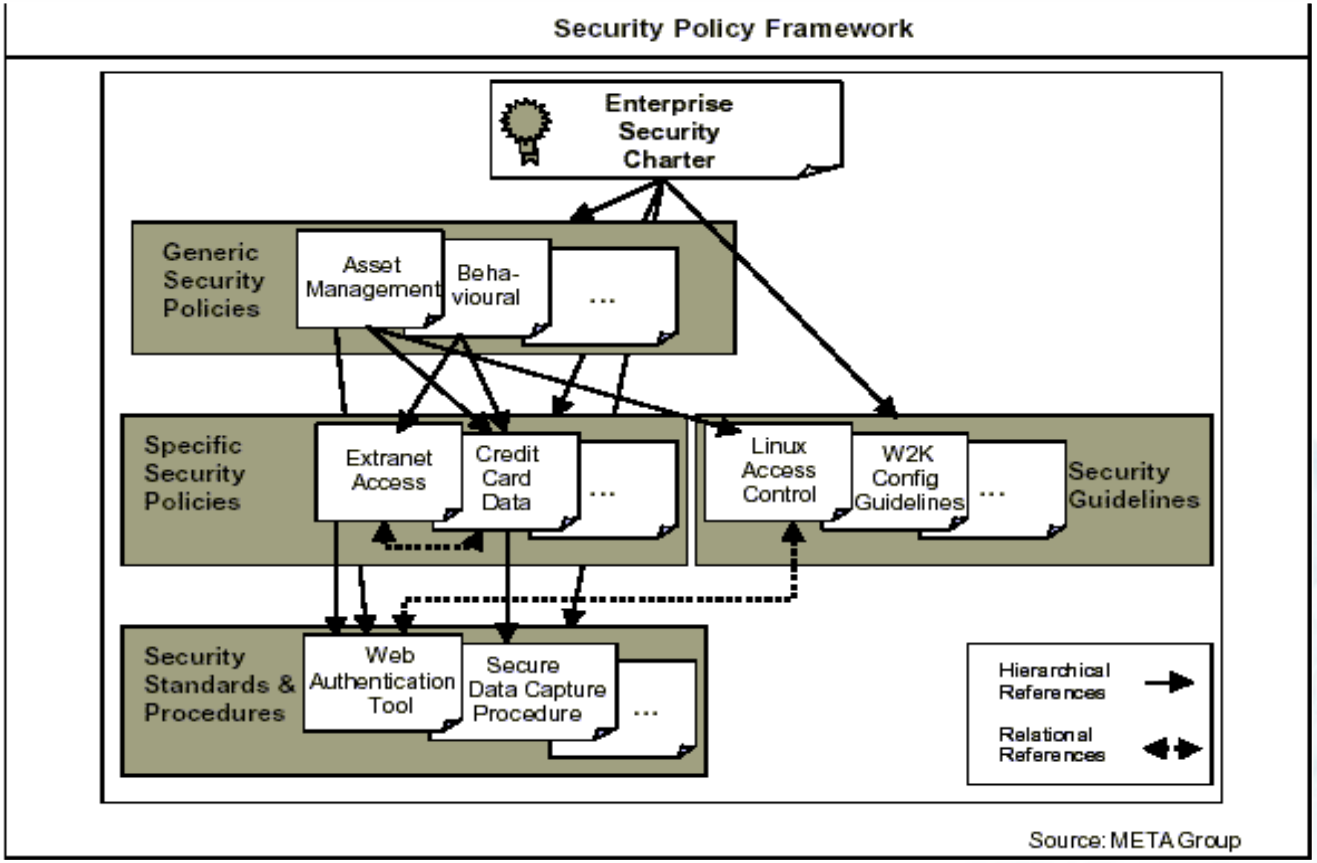
- *Standard*
  - Cara untuk menerapkan semua kebijakan untuk sistem tertentu
  - Dapat "meminjam" dari instansi lain
  - SANS:
    "A standard is typically collections of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to harden a Windows 7 workstation for placement on an external (DMZ) network. People must follow this standard exactly if they wish to install a Windows 7 workstation on an external network segment."

Definisi

- *Procedure*
  - Langkah-langkah rinci yang baku untuk melakukan suatu hal tertentu
- *Guidelines*
  - Panduan, jika belum memiliki standar
  - Dapat dilanggar
  - SANS:

    "A guideline is typically a collection of system specific or procedural specific 'suggestions' for best practice. They are not requirements to be met, but are strongly recommended."

Hirarki P&P


Security Policy Framework
Enterprise Security Charter
Generic Security Policies
Asset Management
Beha-vioural
...
Specific Security Policies
Extranet Access
Credit Card Data
...
Linux Access Control
W2K Config Guidelines
...
Security Guidelines
Security Standards & Procedures
Web Authentication Tool
Secure Data Capture Procedure
...
Hierarchical References
Relational References
Source: META Group

Pengecualian (Exception)

- Sebaiknya ada klausul pengecualian untuk mengakomodasi hal-hal yang tidak sesuai dengan P&P yang ada
  - Teknologi baru
  - Proses bisnis baru
- Default menggunakan P&P yang ada
- Pengecualian dilakukan dengan mengajukan kepada pimpinan alasannya dan mendapatkan pengecualian secara tertulis

P&P Selalu Ada

- Secara historis, kebijakan (P&P) selalu menjadi bagian dari standar
  - Mulai dari ISO 17799 sampai sekarang

POLICY DEVELOPMENT

Membuat *Policy*

- Membuat sebuah tim pembuat kebijakan
  - Melibatkan semua pihak (*stakeholders*) sehingga ada perasaan memiliki
  - Menyangkut berbagai aspek bisnis dan operasional yang mungkin tidak diketahui oleh satu dua orang saja
    - Kebijakan tertentu mungkin menghambat operasional sehingga di-potong-kompas oleh pengguna. (Misal pembatasan akses yang terlalu kompleks, password yang terlalu rumit dan banyak)

Setelah *policy* dibuat

- Perlu ada sosialisasi, diajarkan
  - Biasanya keberadaan policy tidak diketahui oleh pengguna
  - Tidak dimengerti alasan hal yang diatur sehingga dianggap sebagai penghambat
- Ada gap pemahaman yang perlu dicari
- Perlu dibuatkan "jembatan" untuk mengecilkan gap ini
- Pengajaran (sosialisasi) perlu dilakukan terus dan masukan dari proses ini digunakan untuk menyempurnakan policy

Masalah Pemahaman

- Bagaimana cara mengajarkan policy yang efektif?
  - Membuat dokumen mudah diakses, misalnya membuatnya online
  - Mengajarkan dan mengingatkan terus menerus
    - Membuat tema / slogan / poster
    - Membuat quiz, pertanyaan berkala
    - Membuat on-line learning
  - Mengkaitkan dengan penilaian kinerja pegawai. (Harus terkoordinasi dengan SDM)