

ITIL
SECURITY MANAGEMENT
Security as a managed service

Dr. Paul Overbeek
Director
KPMG Information Risk Management
Overbeek.Paul@KPMG.NL



kpmg

+31 70 338 2563

June 2004

ITIL SECURITY MANAGEMENT

- **Information Security**
- **Management of IT - ITIL**
- **Security Management**
 - **The ITIL Process**
 - **Relationships with other ITIL Processes**

Ambition: show you how you can integrate the security process in the normal processes, in this case: ITIL ICT management

What is information security?

WHAT IS INFORMATION SECURITY?

- **Business drivers**
 - needs for information security
- **Business depends on services provided by second and third parties, providing IT services**
- **Business view: What should or may be expected from our IT service providers?**
 - define services also for security
 - define controls
- **IT service providers view: What services should reasonably be offered**
 - which services and controls as a minimum
 - what can be done in addition
 - how do we organise that in our ITIL management framework
- **An introduction to information security ...**

Converging from accepted industry standards

ITIL Security Management

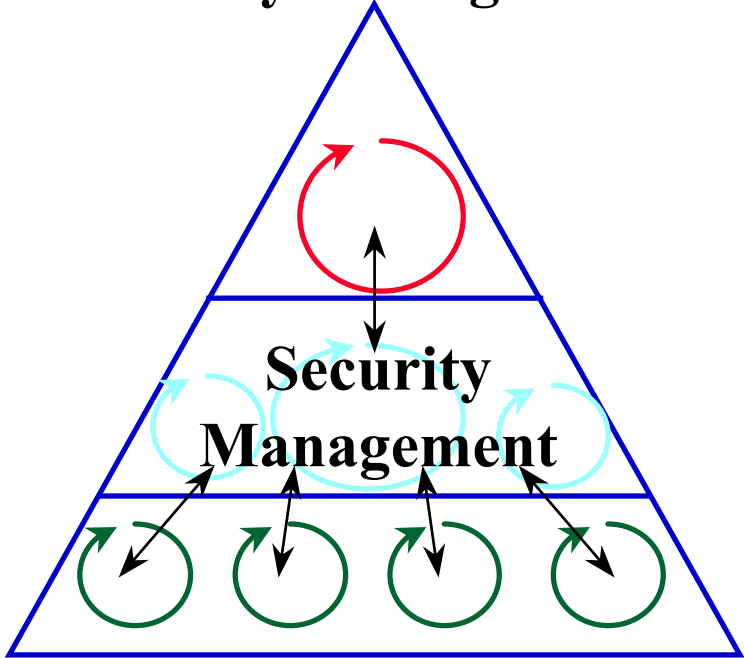
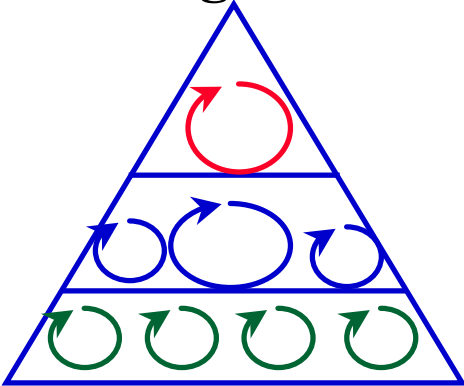
Converging from accepted industry standards

Take best Information Security Practices

- Code Of Practice (BS7799/ISO17799)
- Site Security Handbook
- GASP (NIST)

Develop Security Management

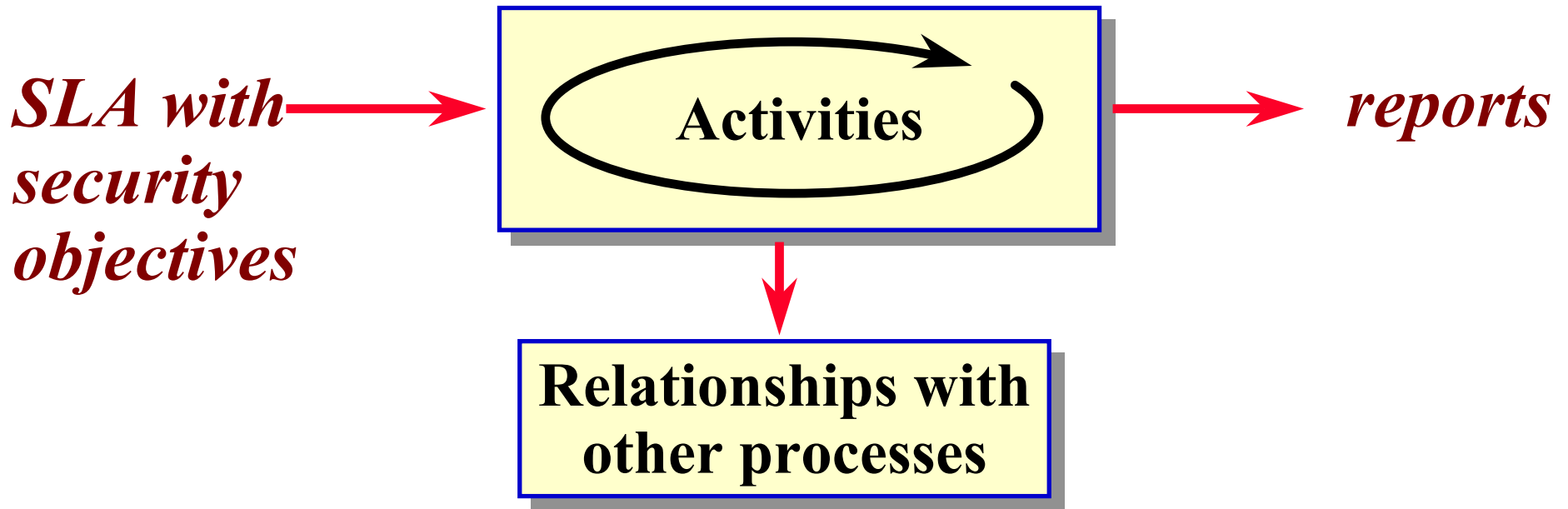
Take existing ITIL framework

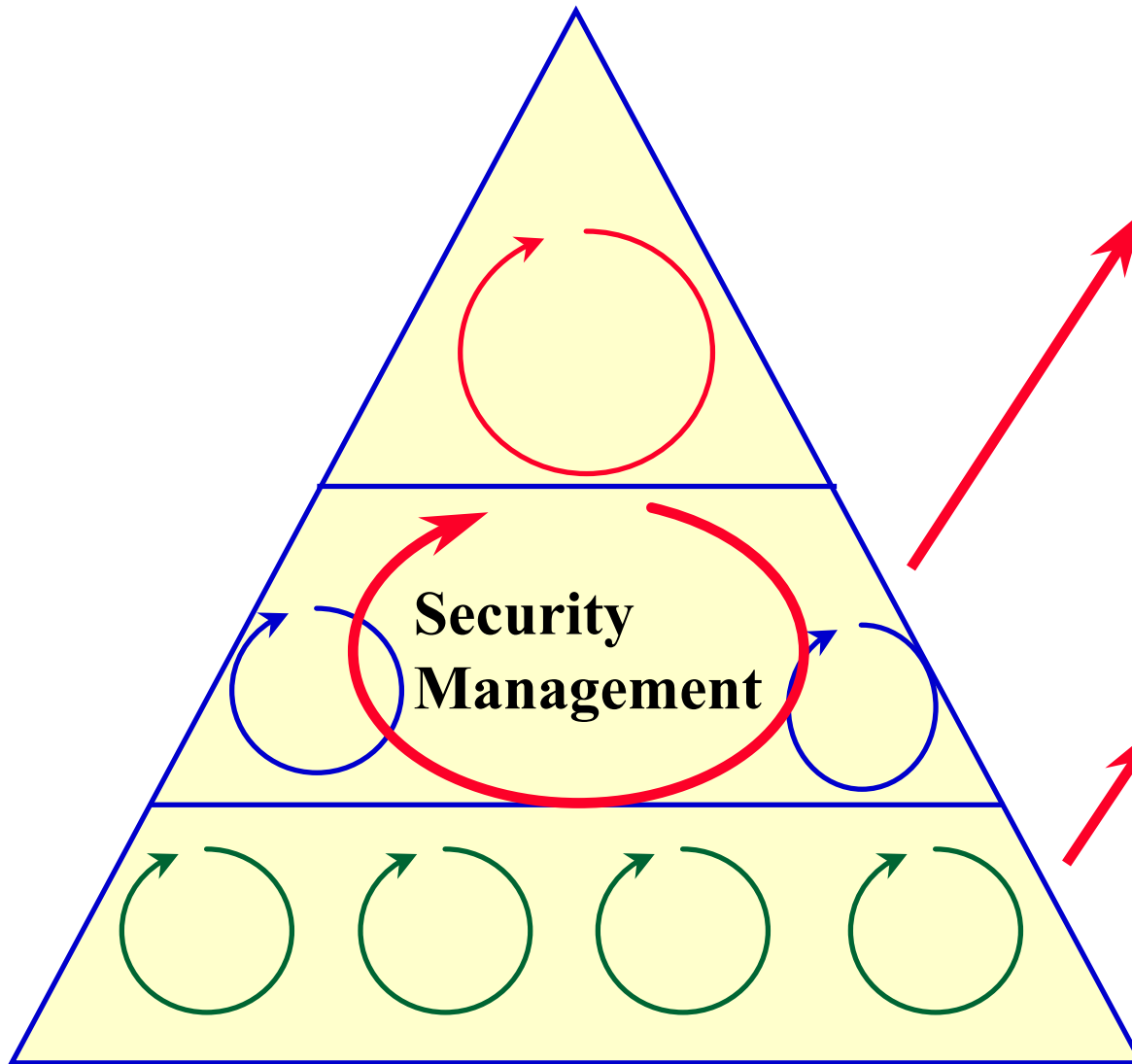


ITIL PROCESS SECURITY MANAGEMENT

Process

Purpose: comply with objectives + baseline security





Relations with:

- **Service Level Management**
- **Availability Management**
- **Performance & Capacity Management**
- **Business Continuity Planning**

Relations with:

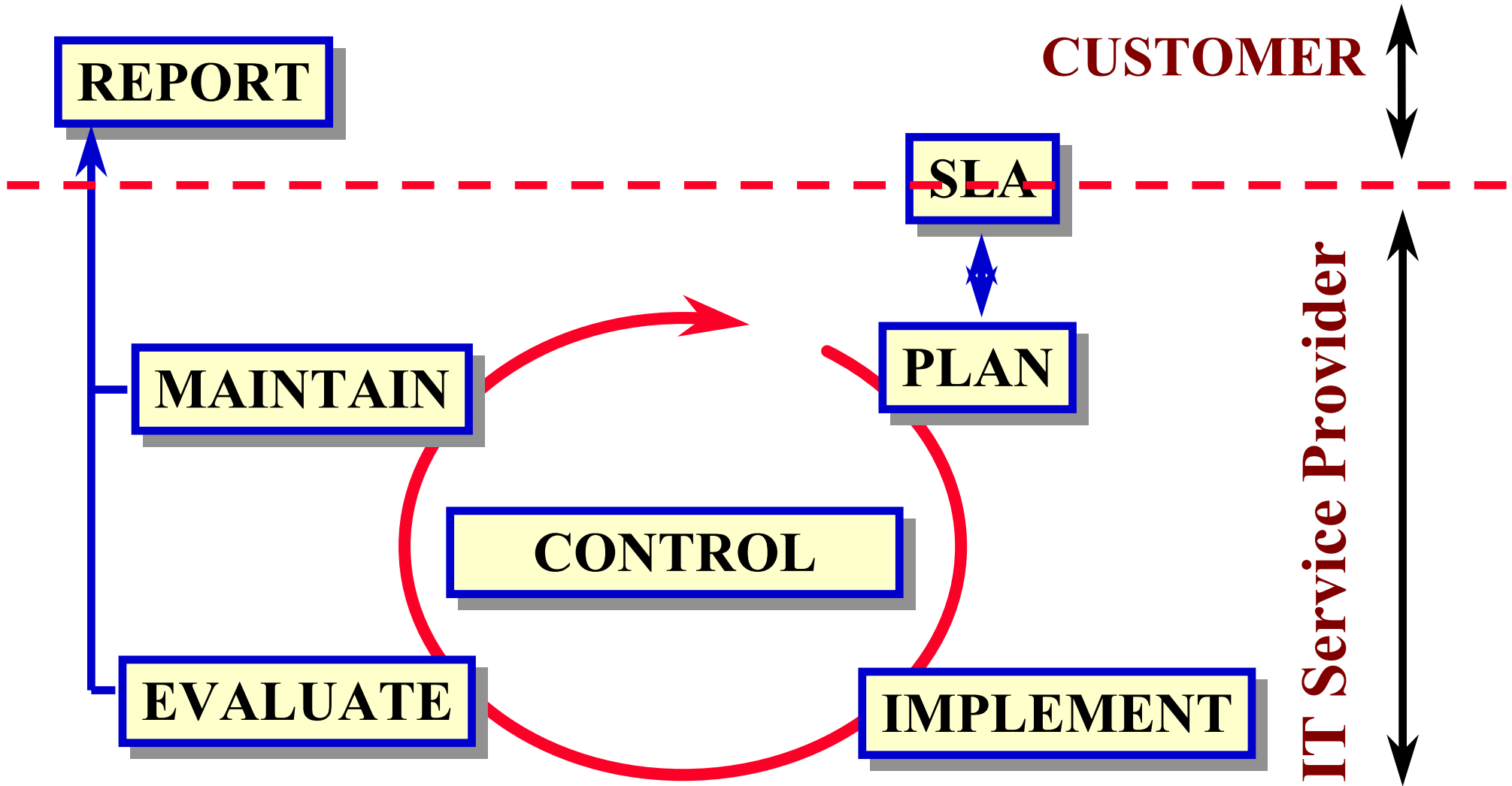
- **Configuration & Asset Management**
- **Incident Control / Helpdesk**
- **Problem Management**
- **Change Management**
- **Release Management (SW C & D)**

SECURITY MANAGEMENT

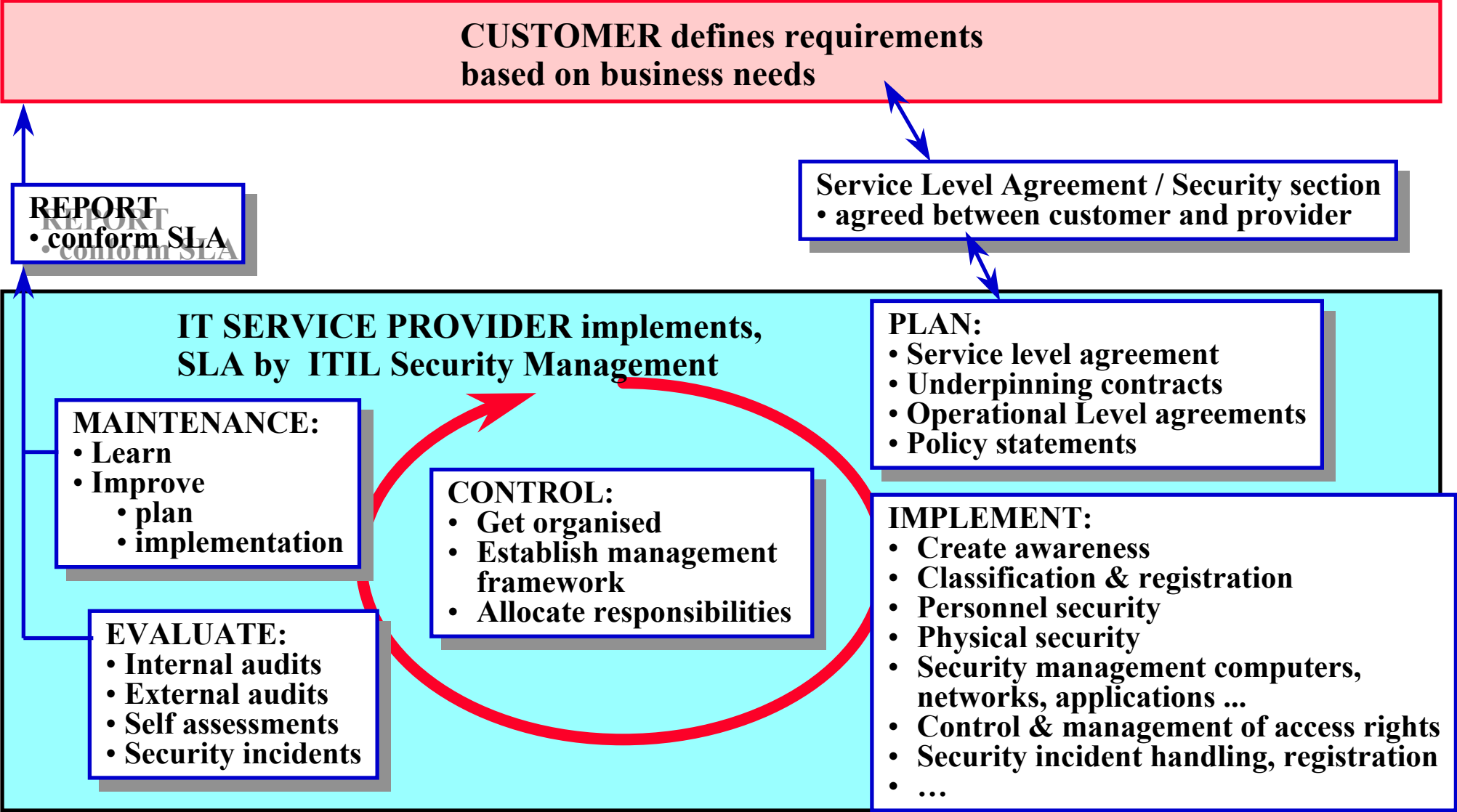
The Three Challenges

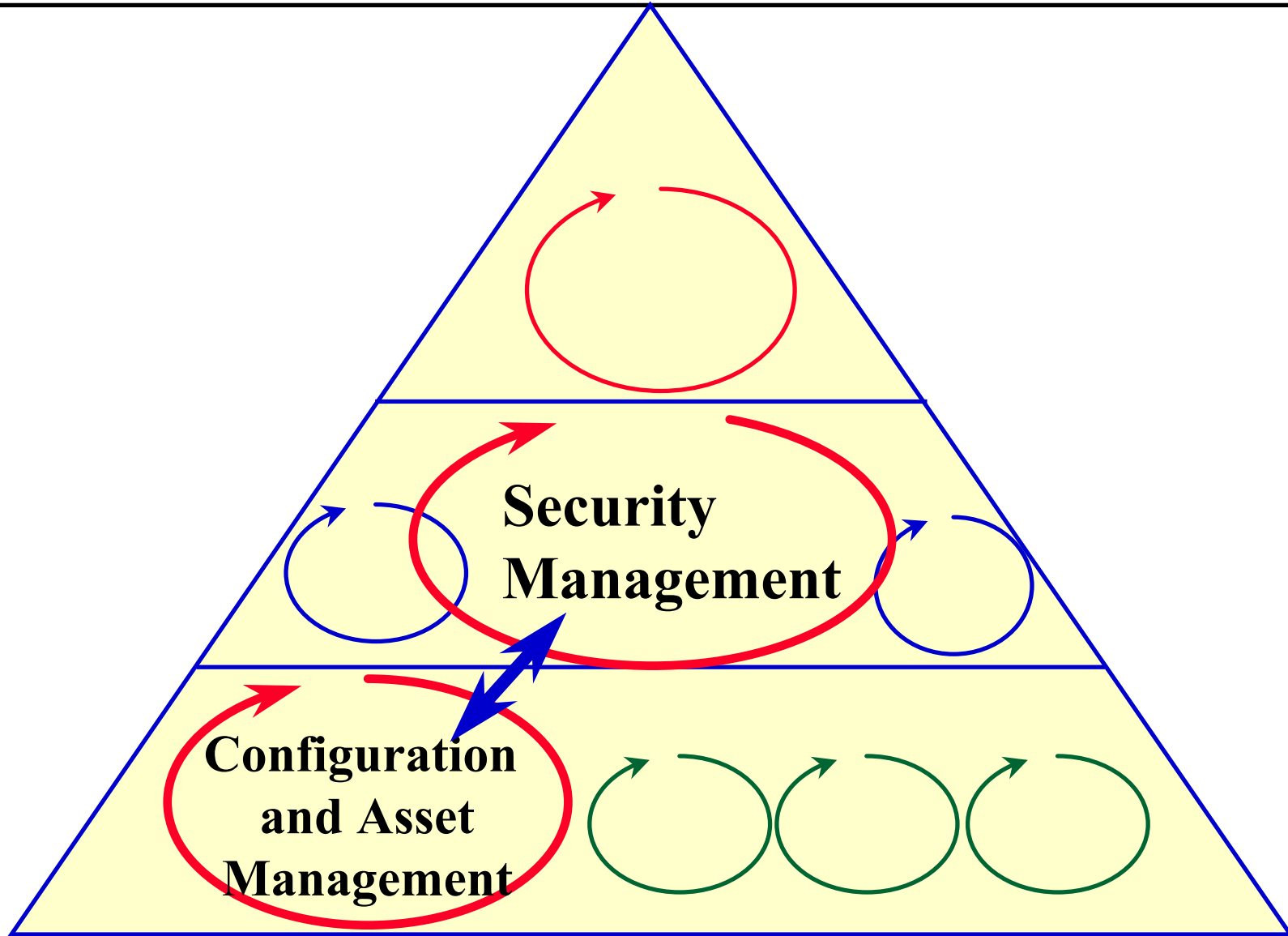
- **Process**
 - the Security Management Process itself
- **Relationships**
 - between Security Management and the other processes
- **External relationships**
 - managing the SLA requirements for security





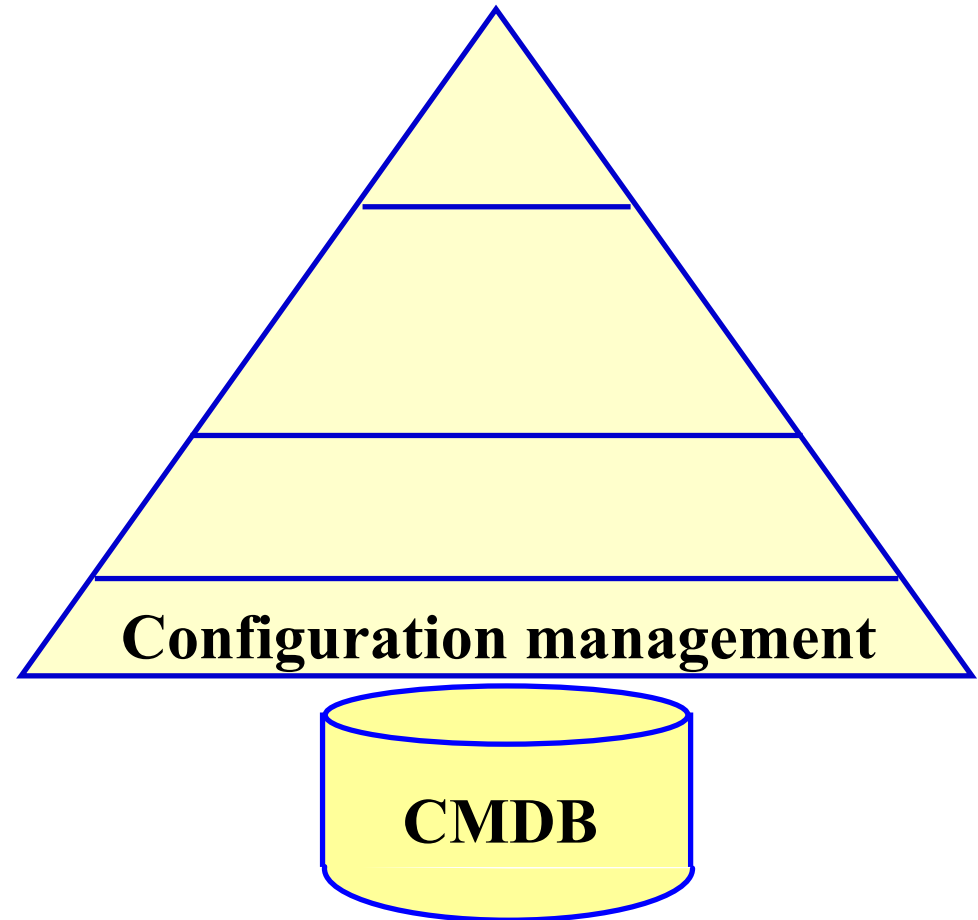
Security management ...





CONFIGURATION and ASSET MANAGEMENT SERVICE SUPPORT SET

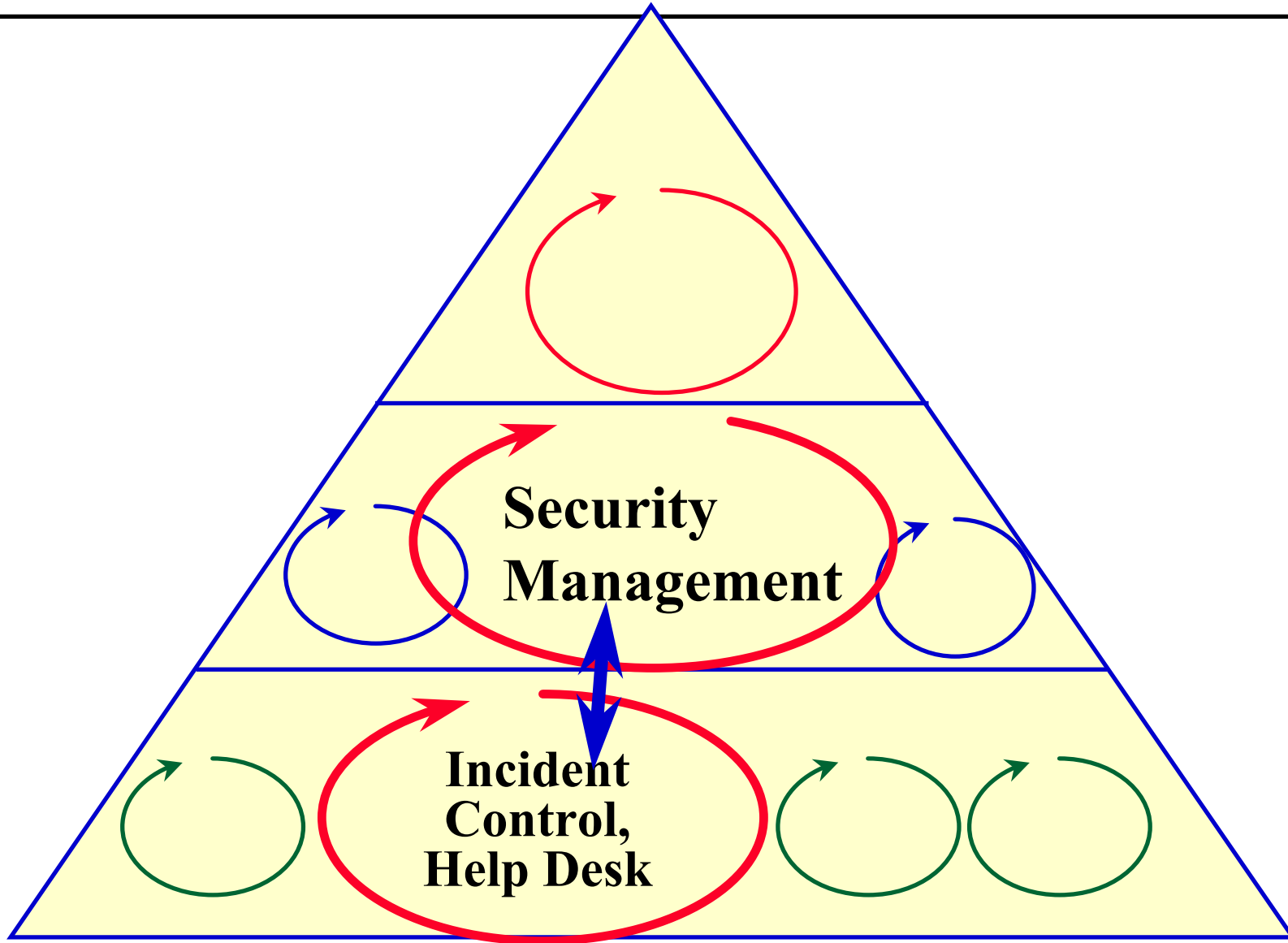
- **The foundation for control**
- **Know what you have**
 - **version management**
- **Use it to control the changes**
- **Terms**
 - **CI : Configuration Item**
 - **CMDB : Configuration Management Data Base**



CONFIGURATION and ASSET MANAGEMENT SUPPORT OF SECURITY MANAGEMENT

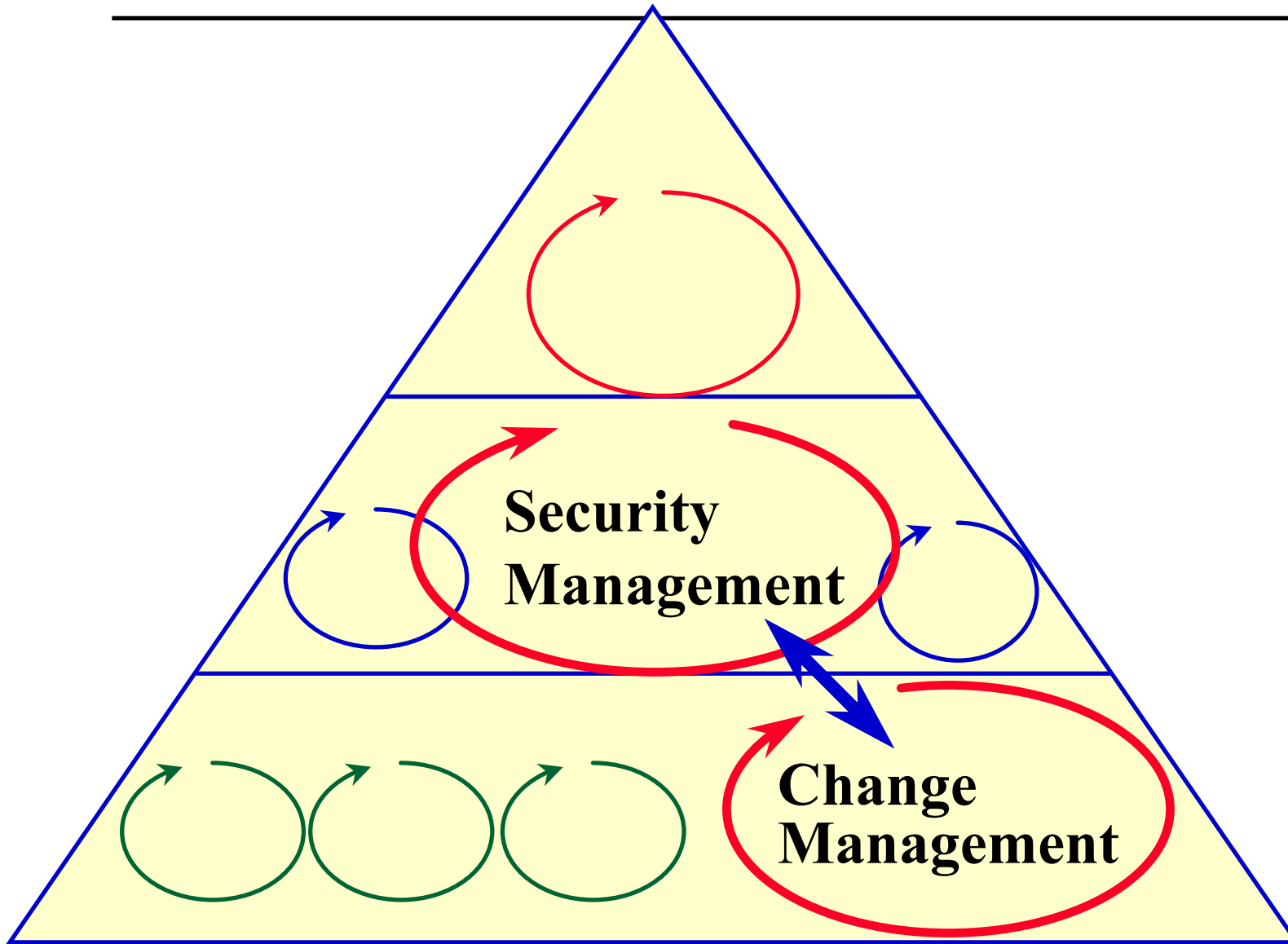
SECURITY ATTRIBUTES

- **Classification system**
 - **confidentiality**
 - **integrity / reliability**
 - **availability / continuity**
- **Classification connects CI to**
 - **activities, to be understood as**
 - » **instructions for how to handle, or**
 - » **procedures !**
 - » **documentation**
 - » **or Manuals / Implementation Guidelines**



INCIDENT MANAGEMENT SUPPORT OF SECURITY MANAGEMENT

- **When is an incident a security incident ?**
 - **CI classified**
 - **SLA-defined events**
 - **?**
- **Activities**
 - **handling security incidents is a ‘normal’ procedure**
 - **possible contact with / reporting to security officer / manager**
 - **implement some security measures**
 - » **e.g., security incident reporting and alarm**
 - » **rapporting**
- **Consider classification scheme for incidents**
 - **incidents making it impossible to comply with the security objectives mentioned in the SLA**



CHANGE MANAGEMENT SUPPORT OF SECURITY MANAGEMENT

In change management many issues are to be ensured

- **Perform risk analyses**
 - impact on business processes (customer's responsibility) - dependencies
 - impact on IT infrastructure as a whole - vulnerabilities
 - which level of security is needed - service level requirements for security
 - **Security plan (SOLL)**
 - selection of security controls / measures + audit + contingency + availability + BASELINE
 - **define Operational Level Agreements (OLAs), UPCs**
-

CHANGE MANAGEMENT SUPPORT OF SECURITY MANAGEMENT (cont.)

- **Implementation plan for security ('to be' minus 'as is'), plan for**
 - **implementation of selected controls / measures**
 - **implementation of security baseline**
 - **OLA's, UPC's**
- **Implementation plan for security is part of RFC**
- **Change Advisory Board (CAB) decides and authorizes**

A change

RFC = Request for Change, change proposal on CI(s)



Urgent / not



Impact on security



Reviewed / authorised by CAB



Implementation



Tests



Acceptance

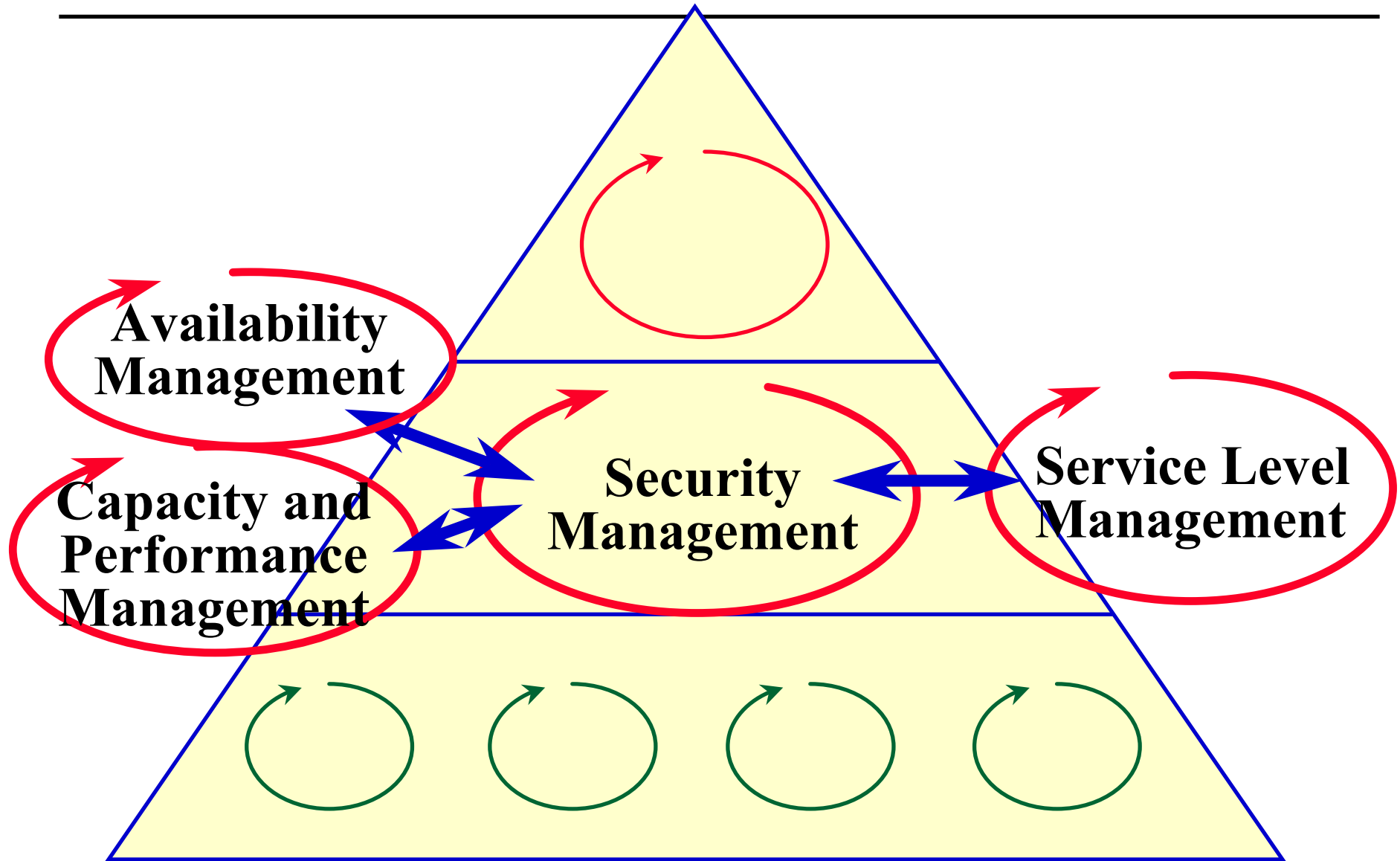


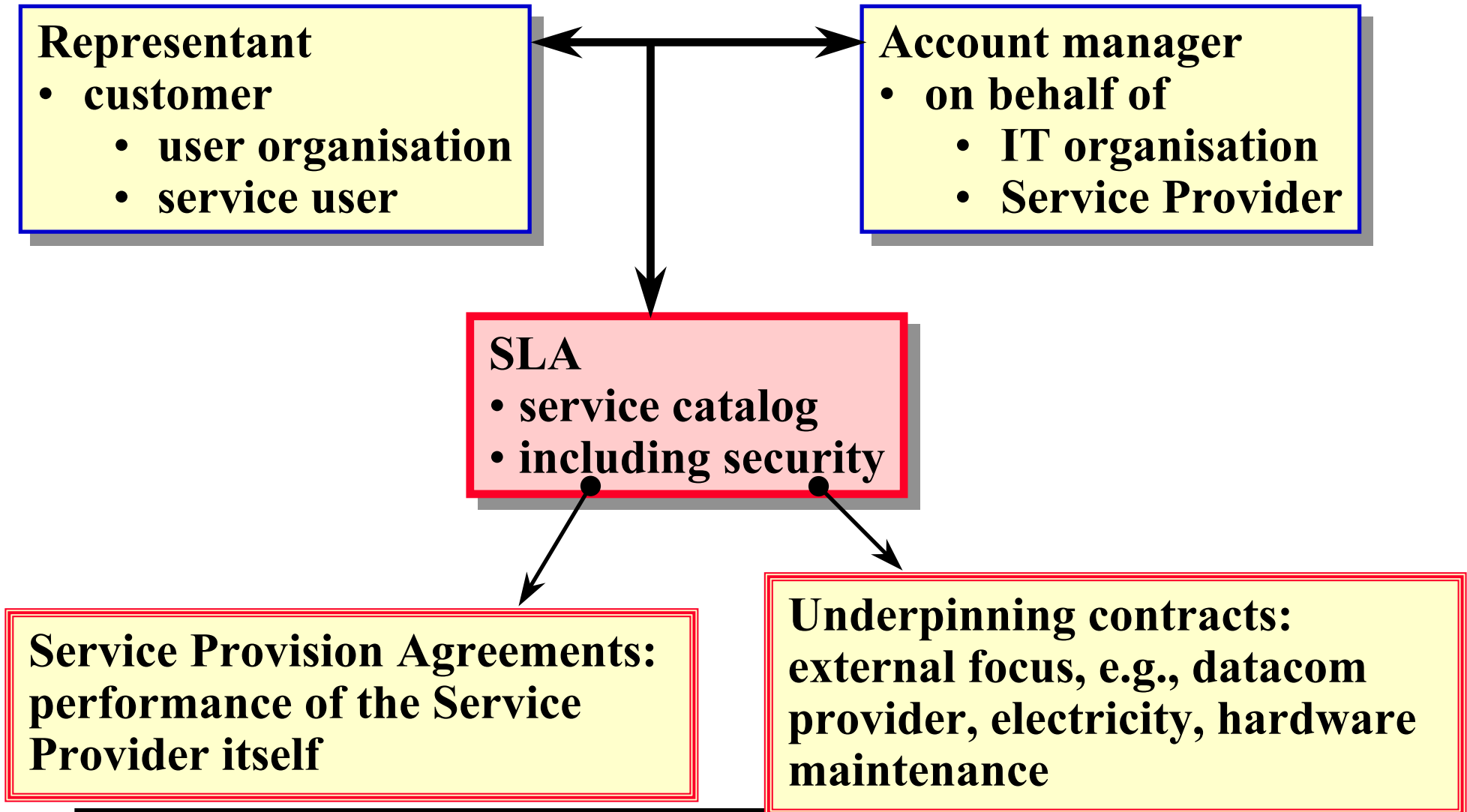
CHANGE ADVISORY BOARD (CAB)

Configuration Control Board, participation should vary

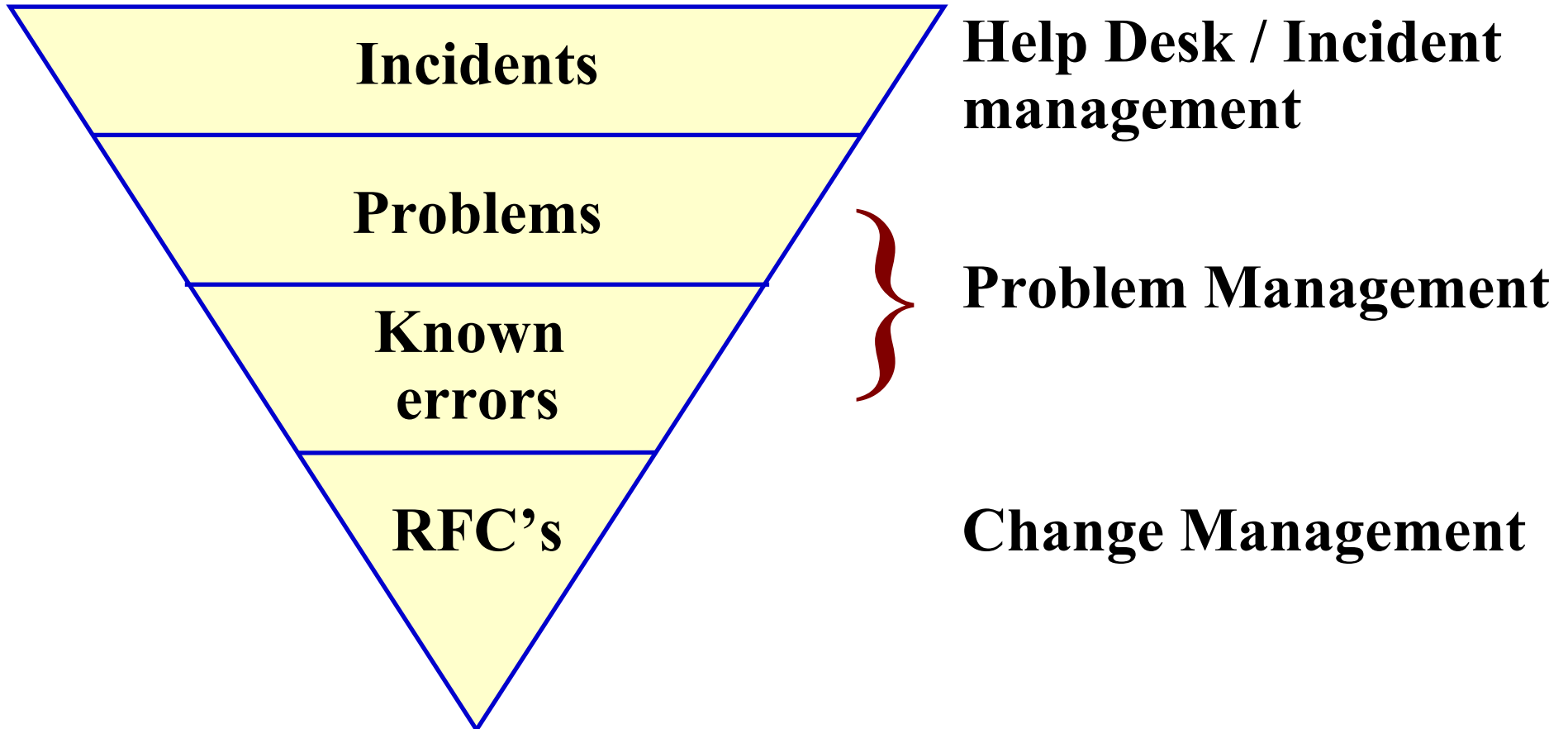
- Change Manager
- Service Level Manager
- Case specialists
 - architect
 - technical experts
 - design & development
- Operational management
- Customer ?
- ...
- Other process managers
- Security Manager for security relevant changes !







ITIL & security provides a controlled process and hence results in less errors in operation and security



ITIL SECURITY MANAGEMENT: IN SUMMARY

- ✓ **Background**
- ✓ **Information security**
- ✓ **Management of IT - ITIL**
- ✓ **Security Management**
 - ✓ **the ITIL process**
 - ✓ **relationships with other ITIL processes**
 - ✓ **external relationships: SLA + UC**
 - ✓ **organisation of ... : OLA**

Security Management: Transforming security into a managed service