

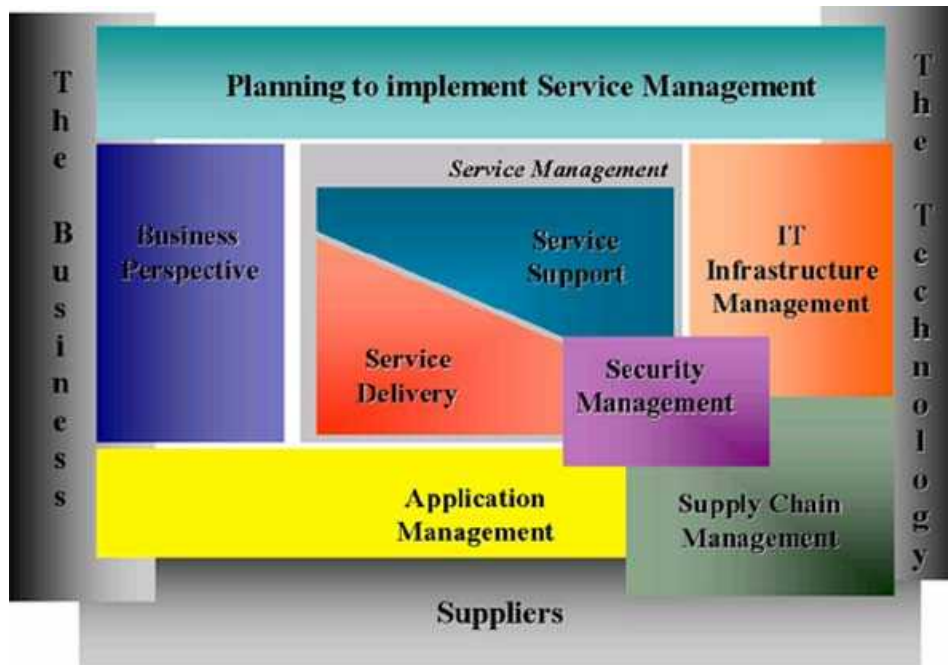
ITIL Security Management

May 2005

-

John Wallhoff
(CISA, CISM, CISSP)

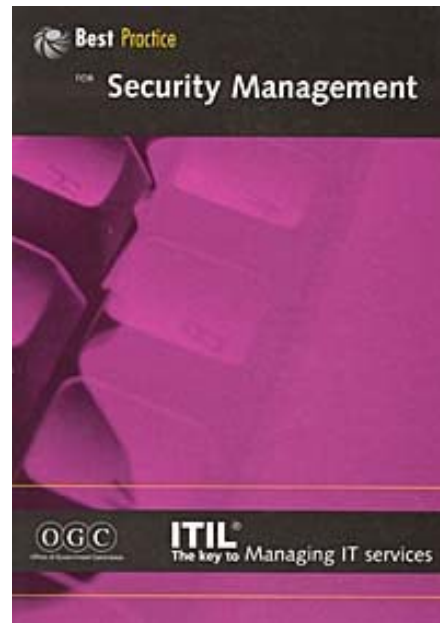
The ITIL Landscape



The ITIL Landscape



The ITIL Landscape



Scope

- Security Management within the boundaries of ITIL
 - Not the ISO17799:2000 scope
 - Management of physical security or personal safety are not covered
 - Technical details of devising and incorporating security measures is out of the scope
 - Risk analysis is out of the scope

ITIL processes meets Security

- ITIL processes
 - Availability Management
 - See Service Delivery publication
 - IT Service Continuity Management
 - See Service Delivery publication
- Security (ISO17799)
 - Availability as a characteristics for security
 - Business Continuity Management a separate section

Leads us to

ITIL is not used to implement security

... but ...

ITIL process may lead to enhanced security
through controlled processes

... and ...

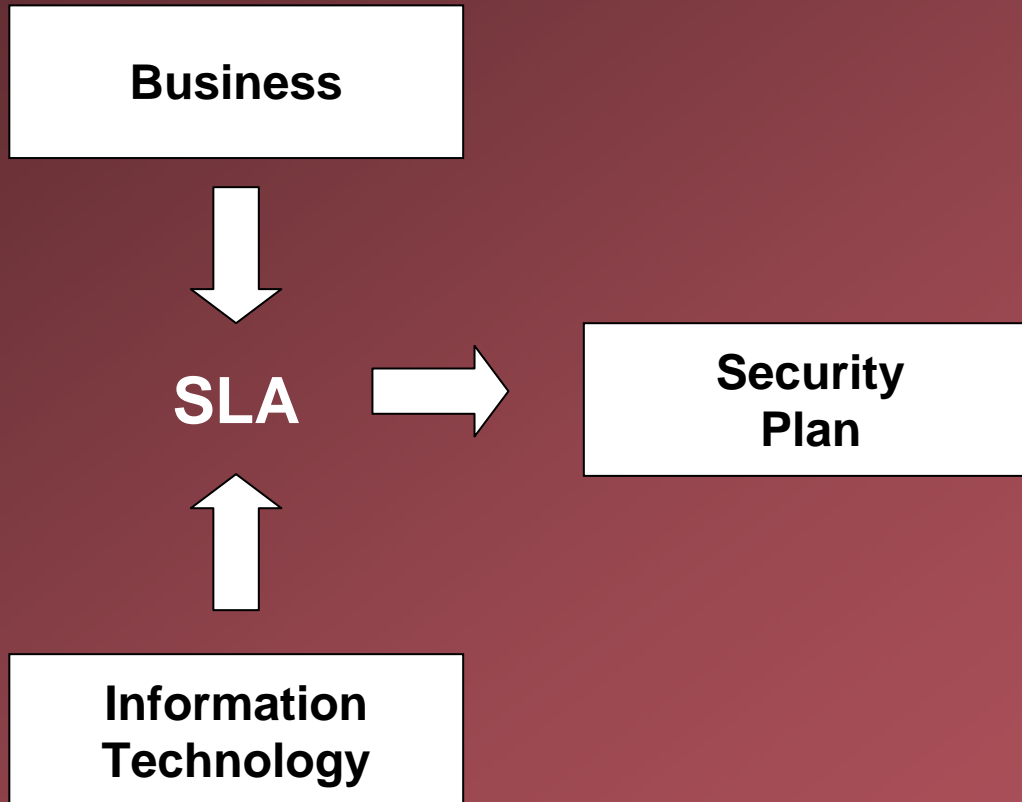
ITIL Security Management will support ITIL
process to take security into account

Definition

Security Management is the process of managing a defined level of security on information and IT services

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met. (ISO 17799:2000)

SLA in focus



Disposition of publication

Section 2
Fundamentals
of
information
security

Section 3
ITIL and
Security
Management

Section 4
Security
Management
Measures

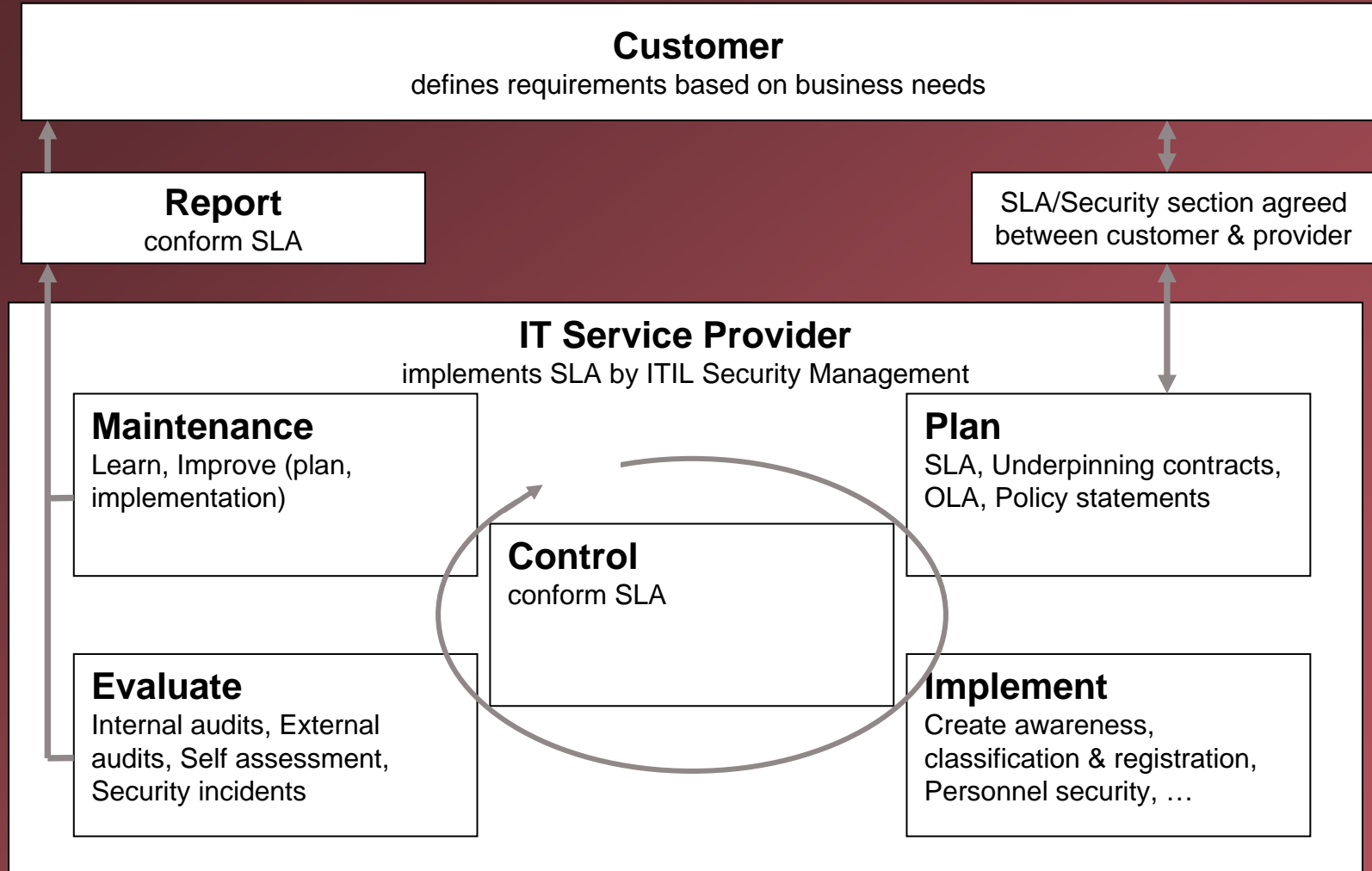
Section 5
Guidelines for
Implementing
Security
Management

Annex A
ITIL
-
BS7799

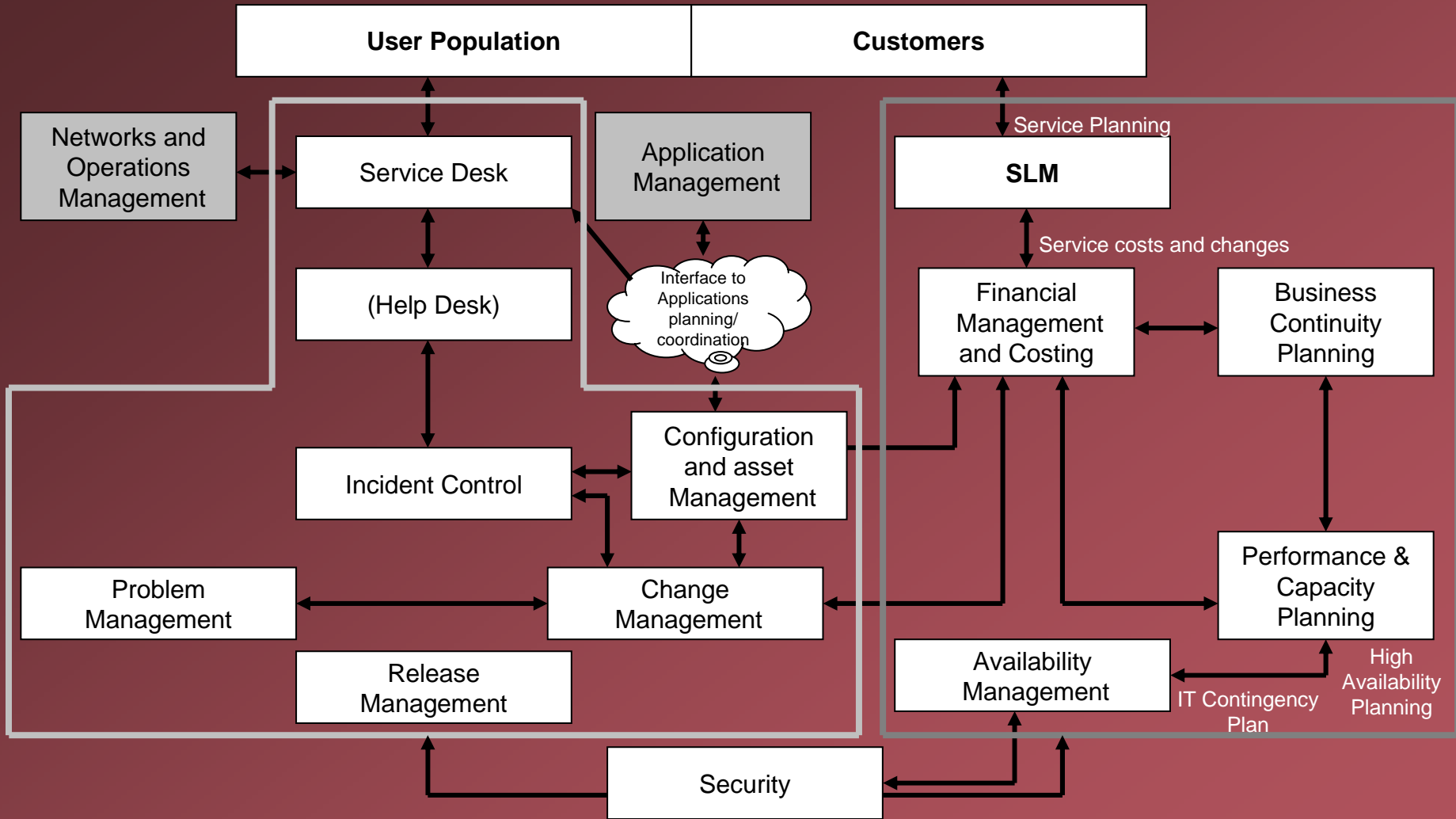
Annex B
Specimen
security
section
in the SLA

Annex C
Framework
for drawing up
security plan

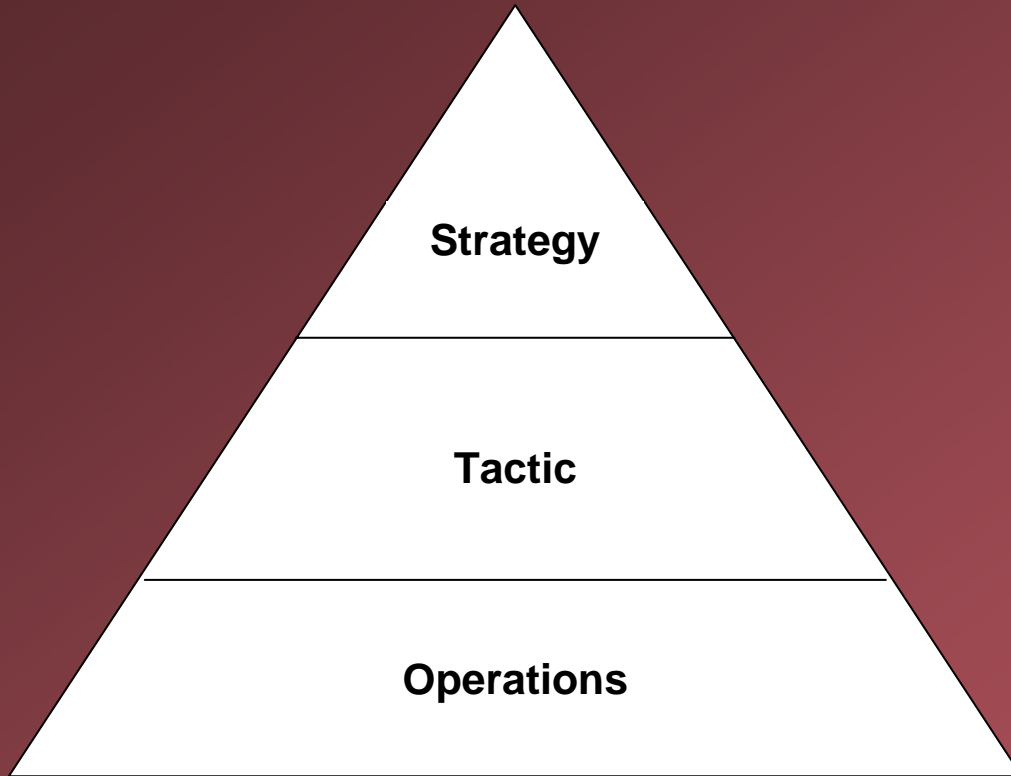
IT Security Management process



ITIL Process Model



Layers in ITIL

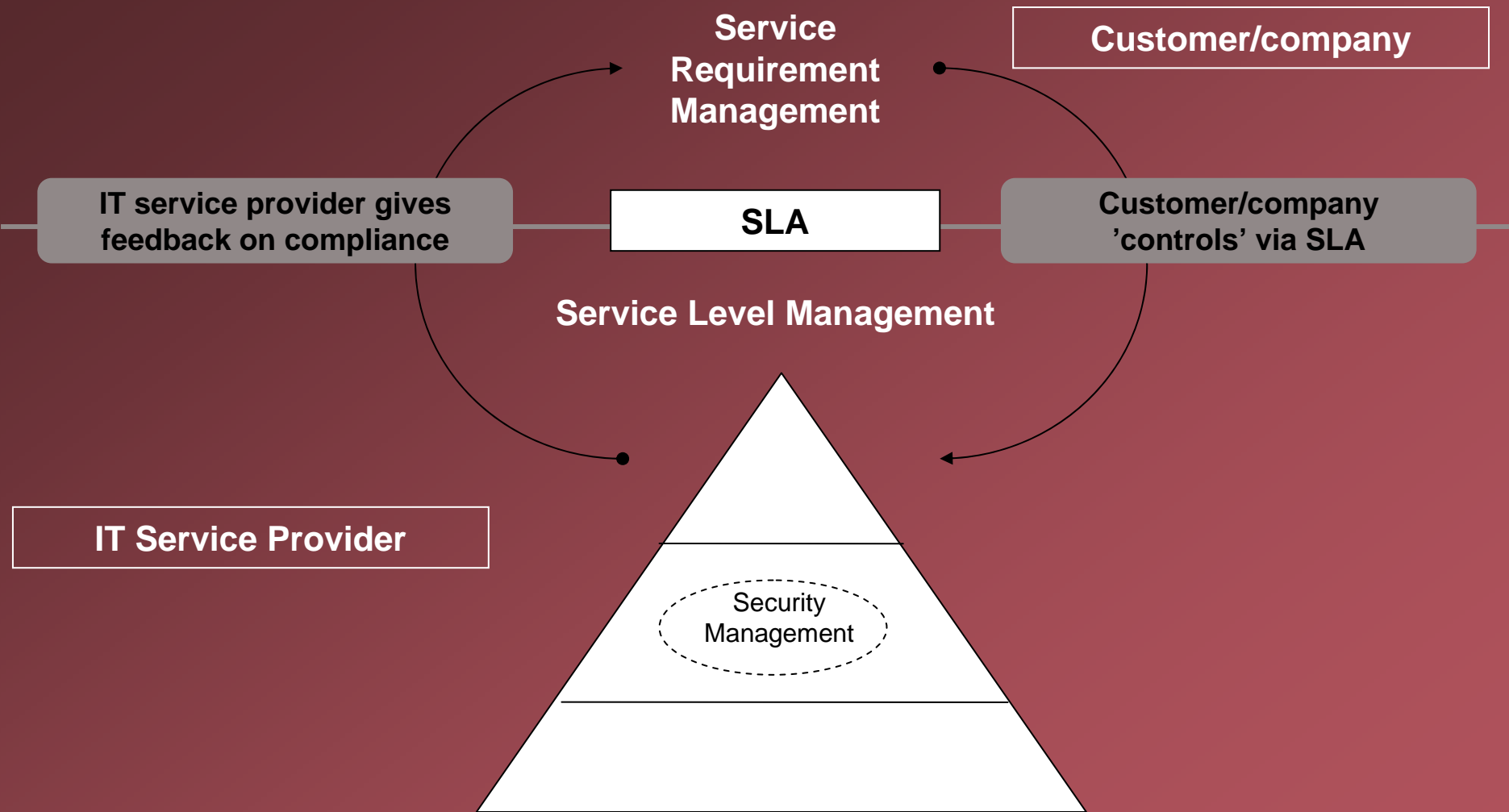


Manager's set

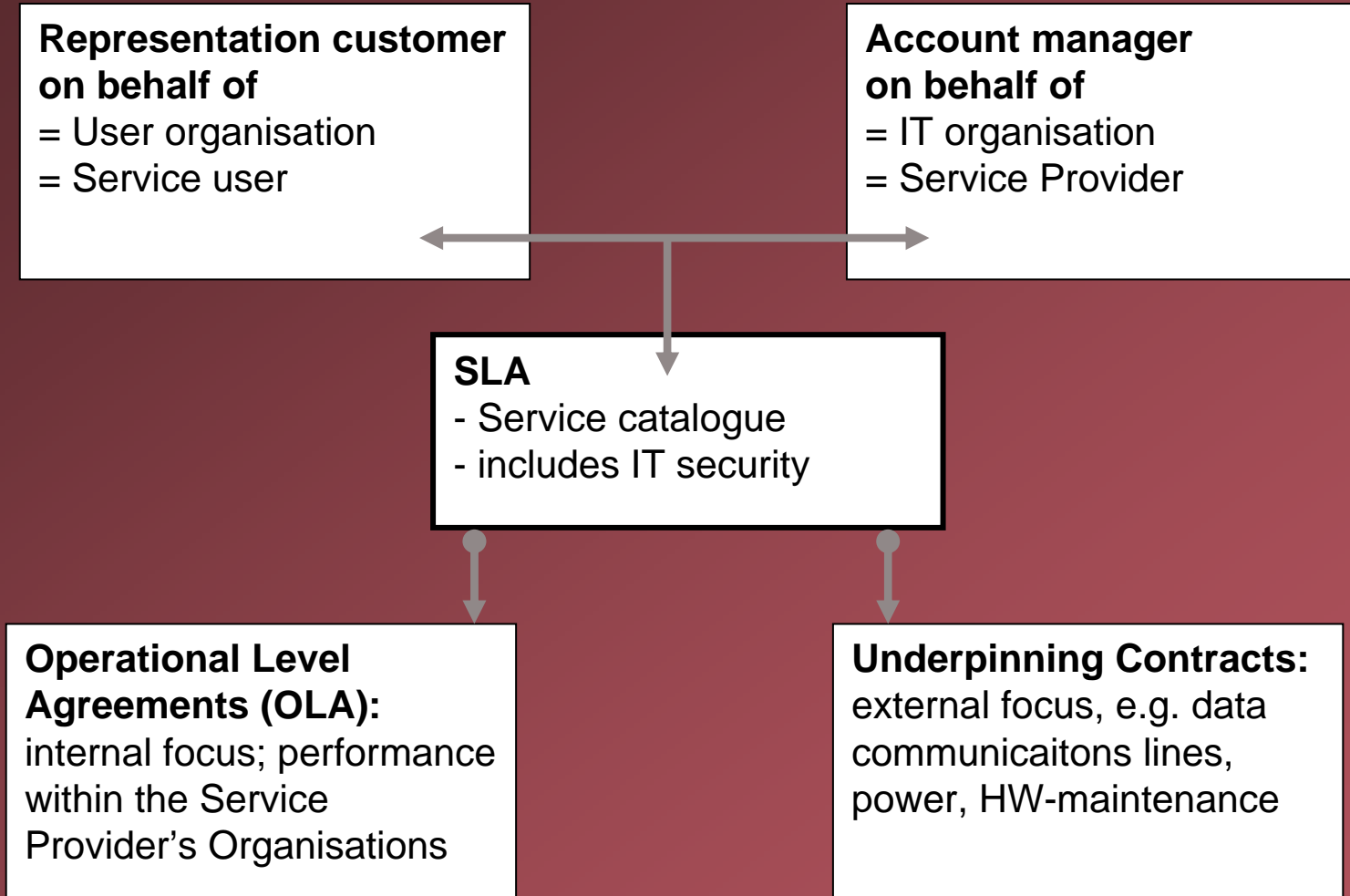
Service Delivery set

Service Support set

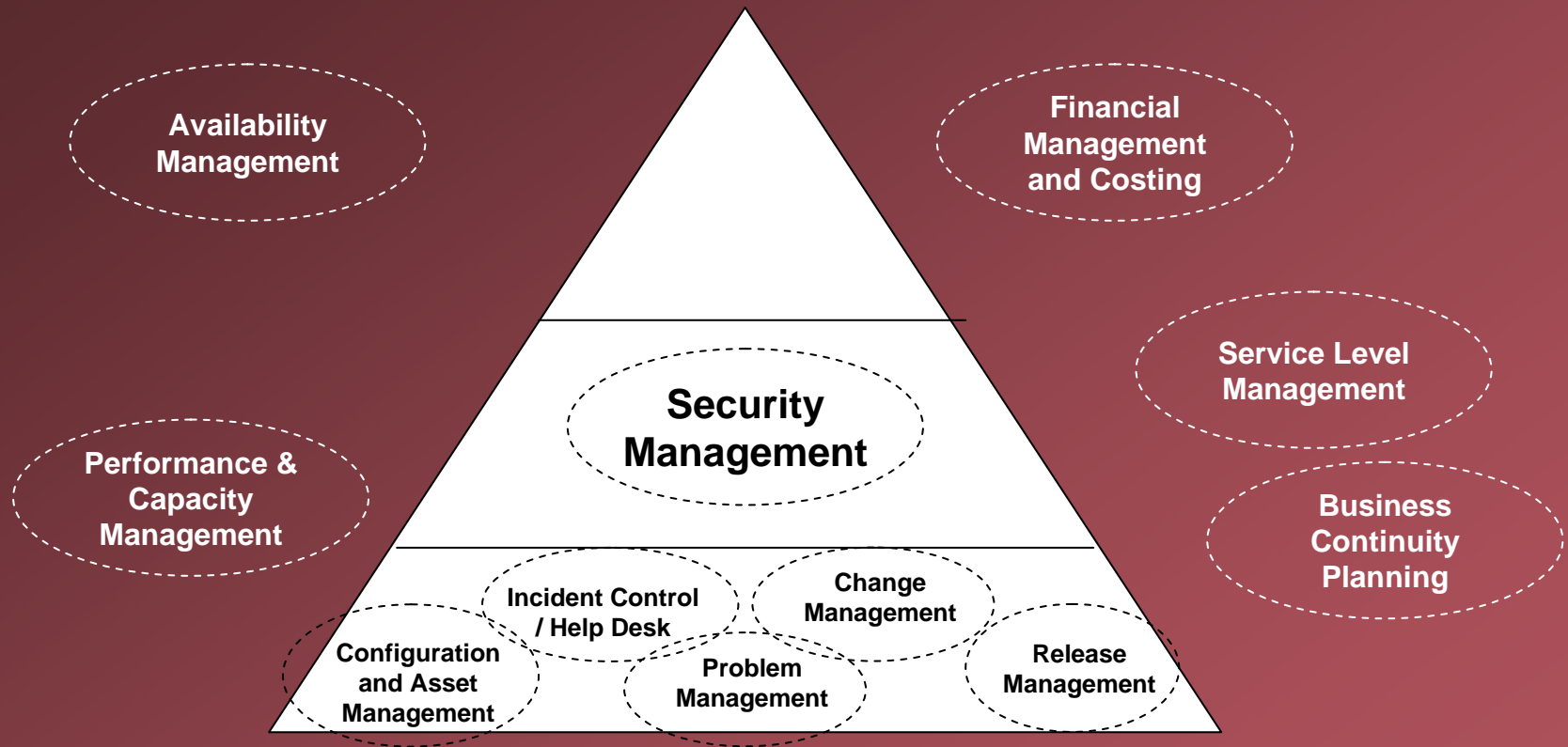
Related processes



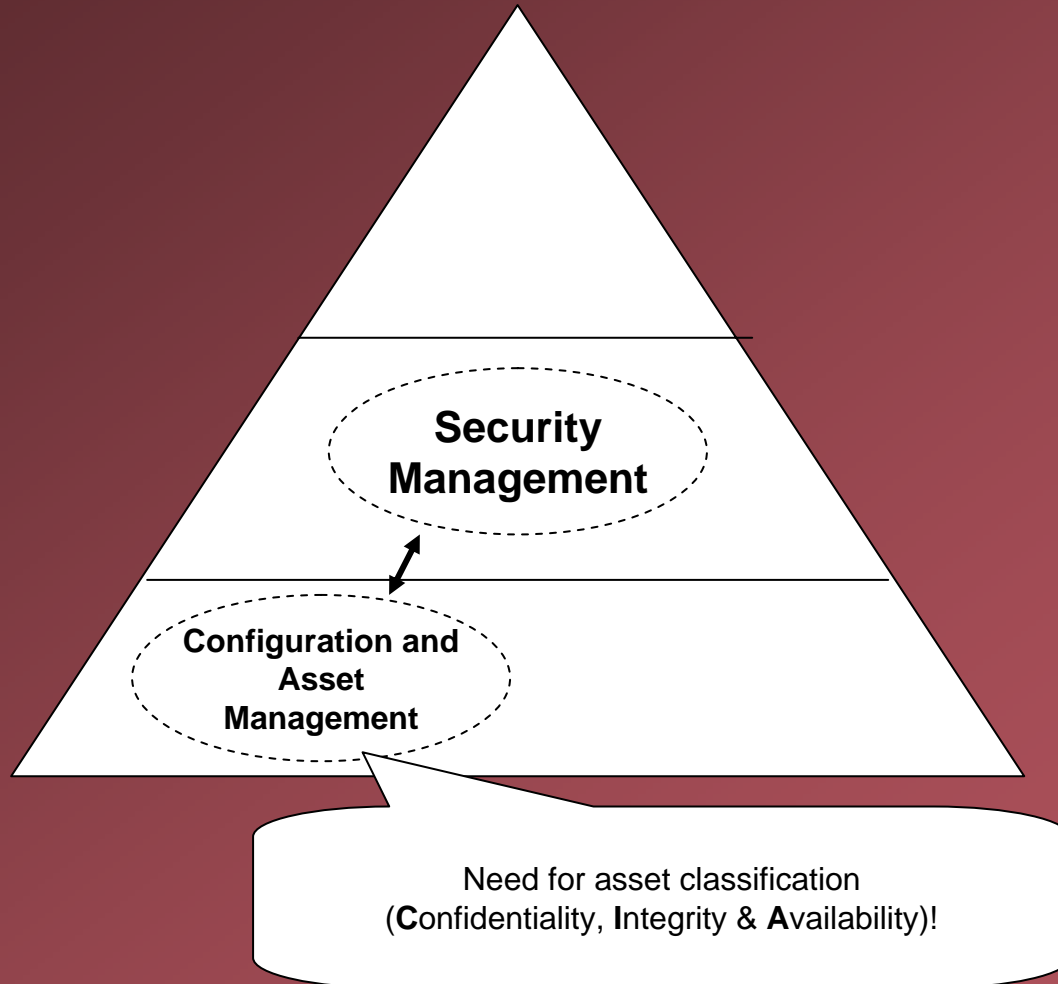
Security section in SLA



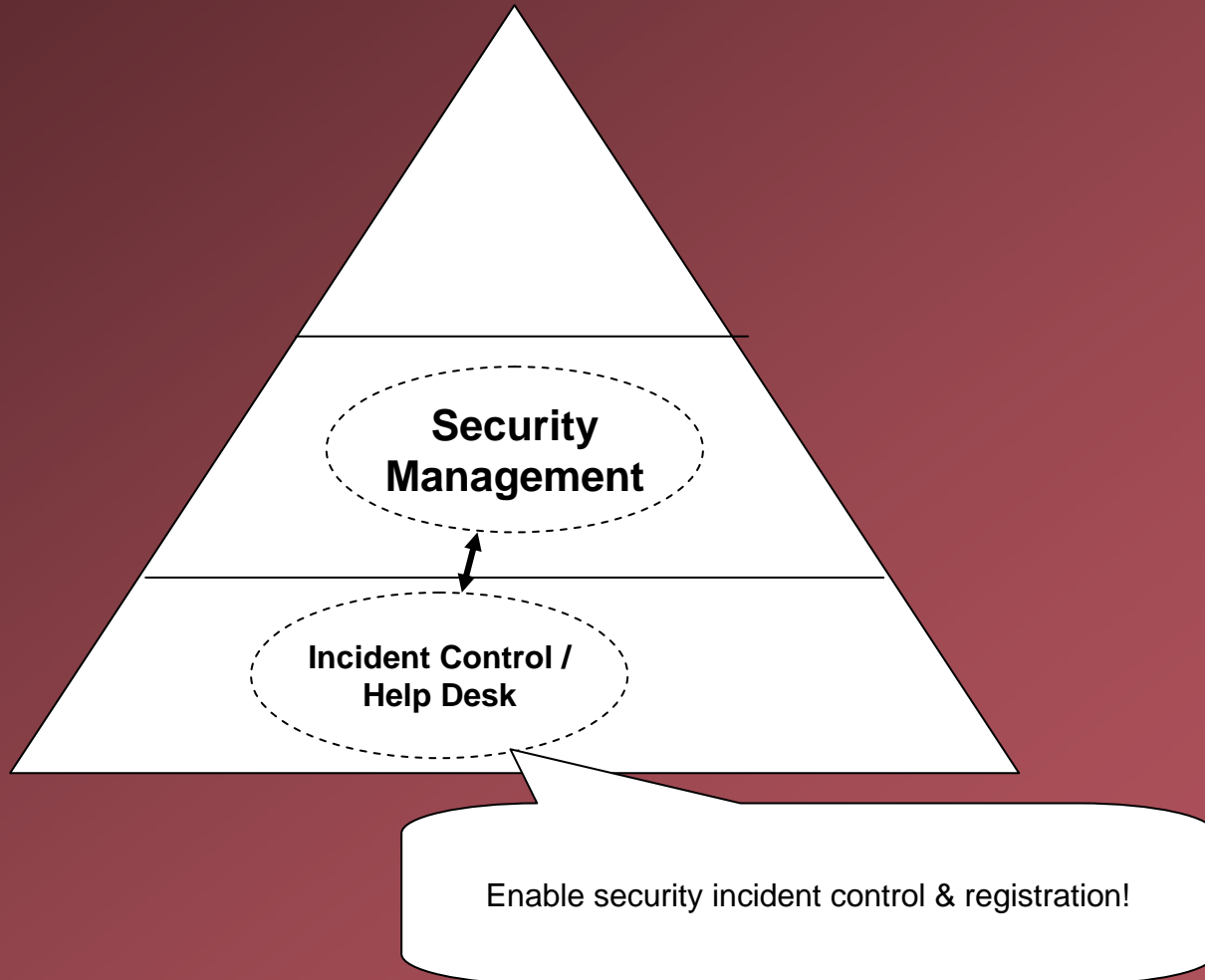
Relation with Service Support



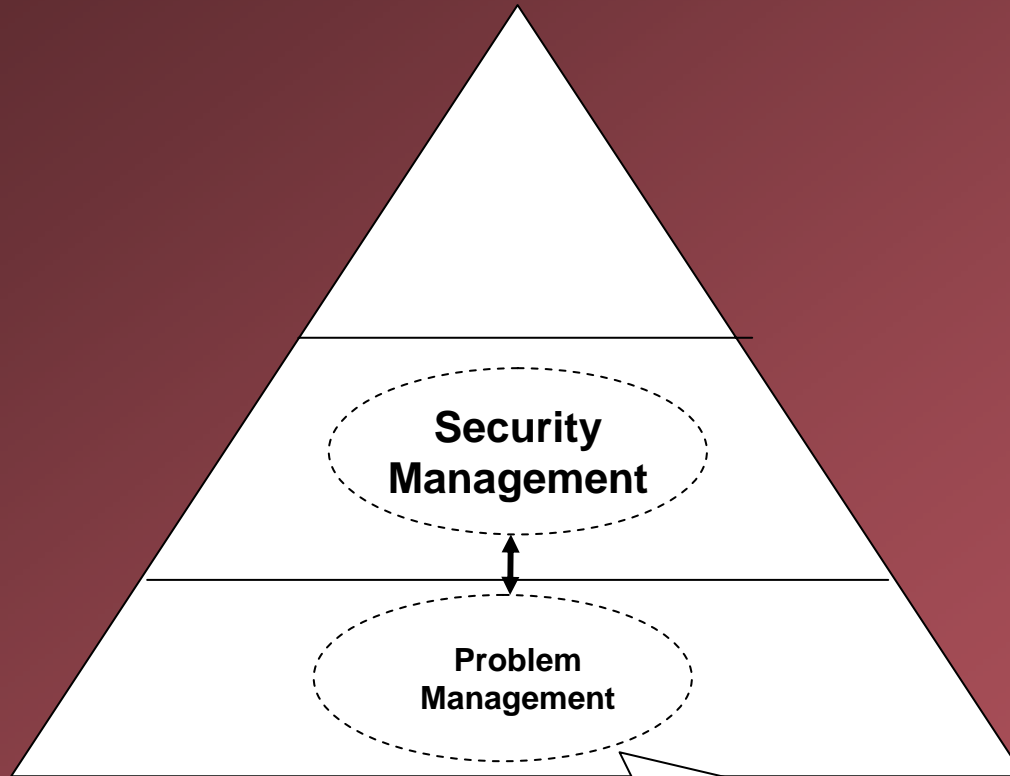
Relation with Service Support



Relation with Service Support

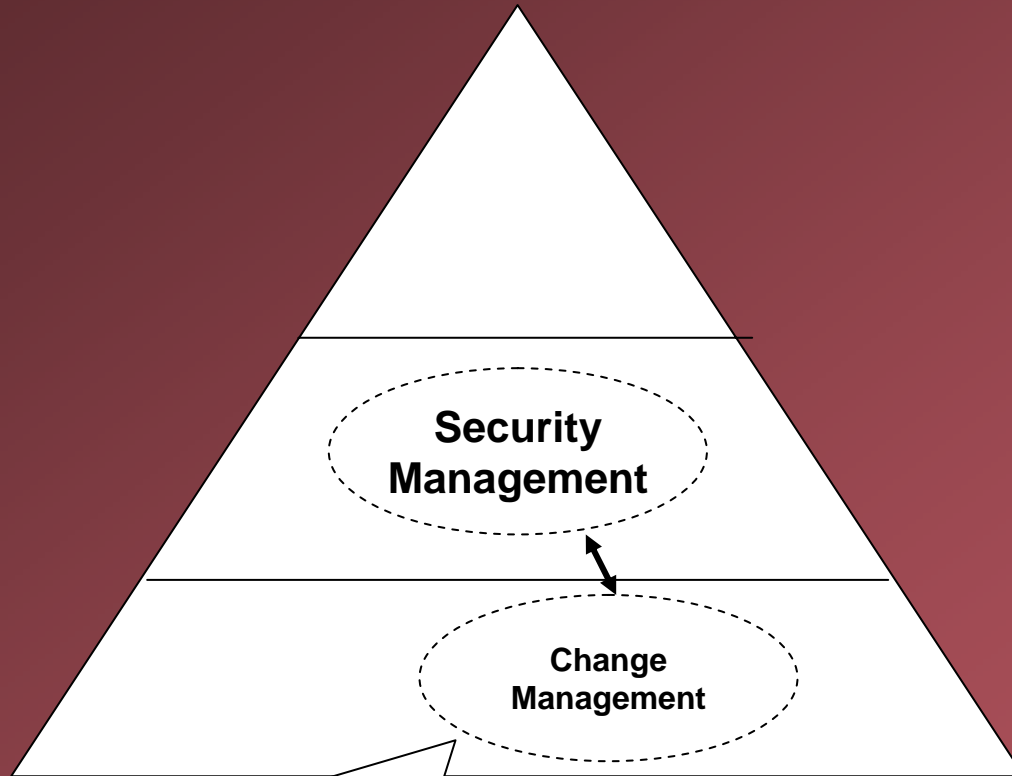


Relation with Service Support



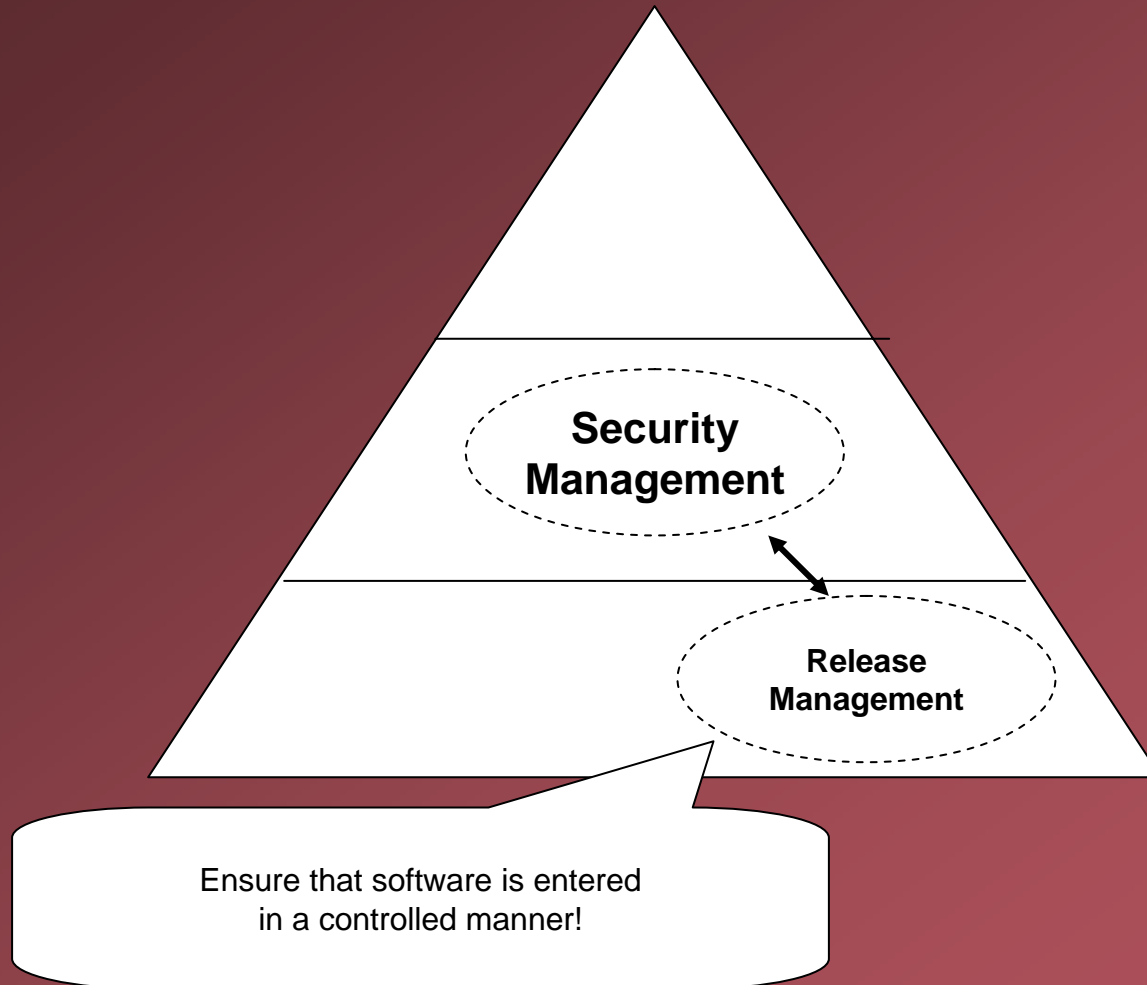
Security incidents require separate procedures!

Relation with Service Support

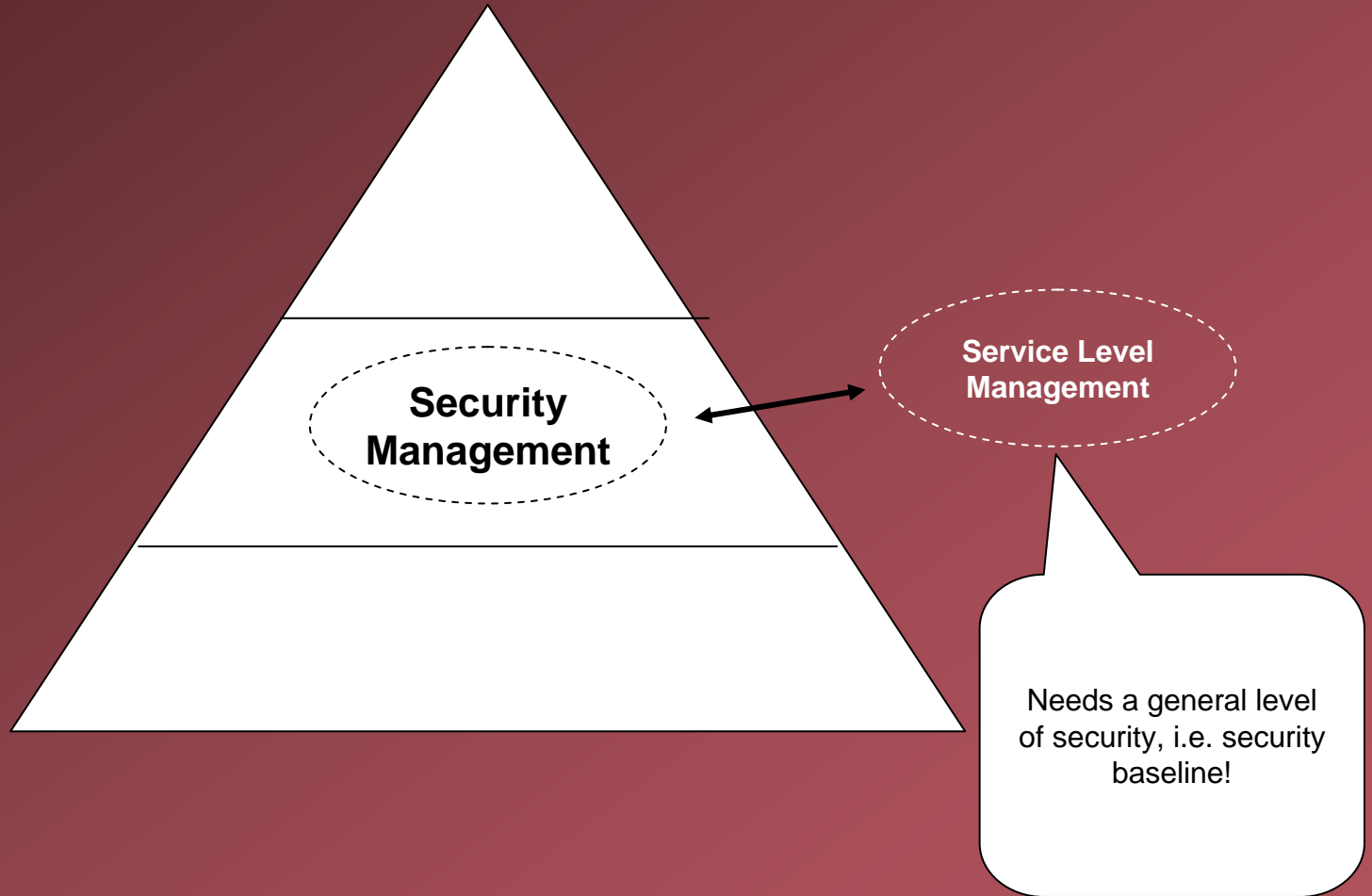


Ensure that security level is not reduced by a change!

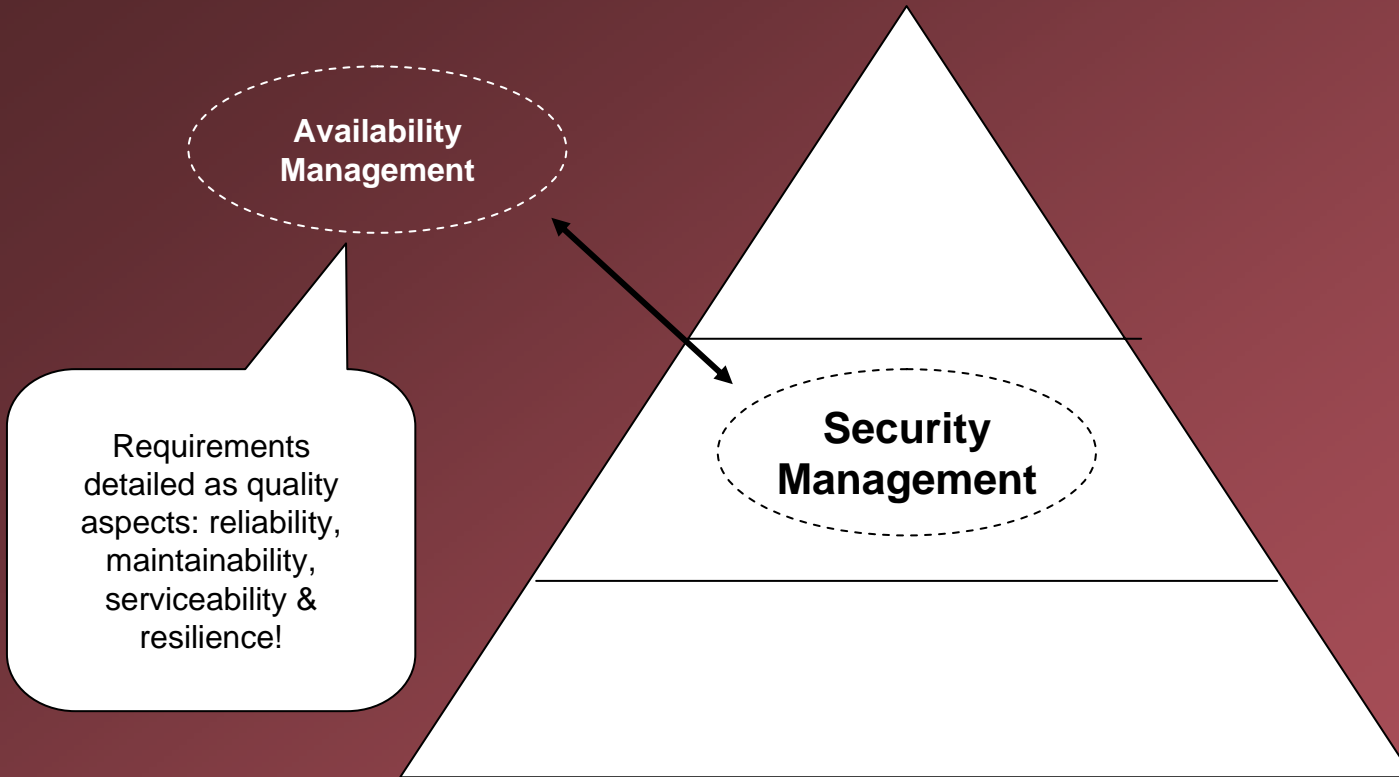
Relations with Service Support



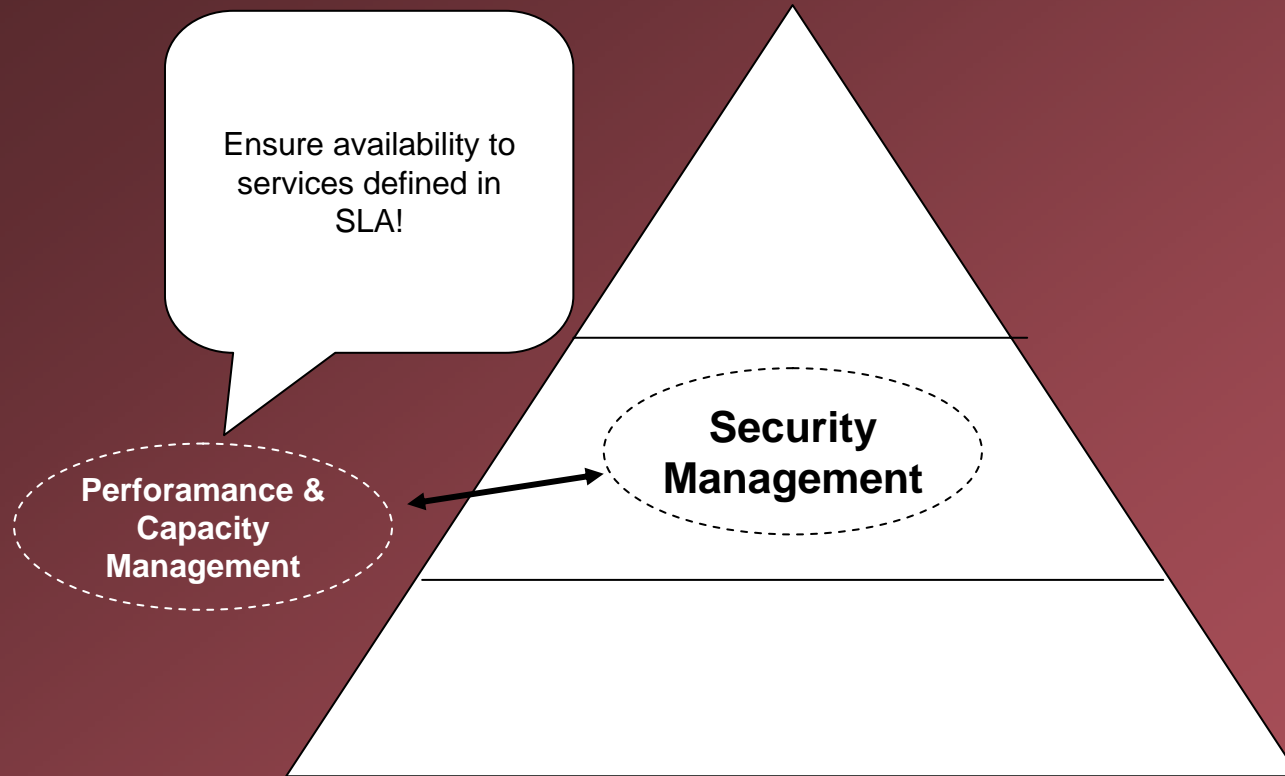
Relation with Service Delivery



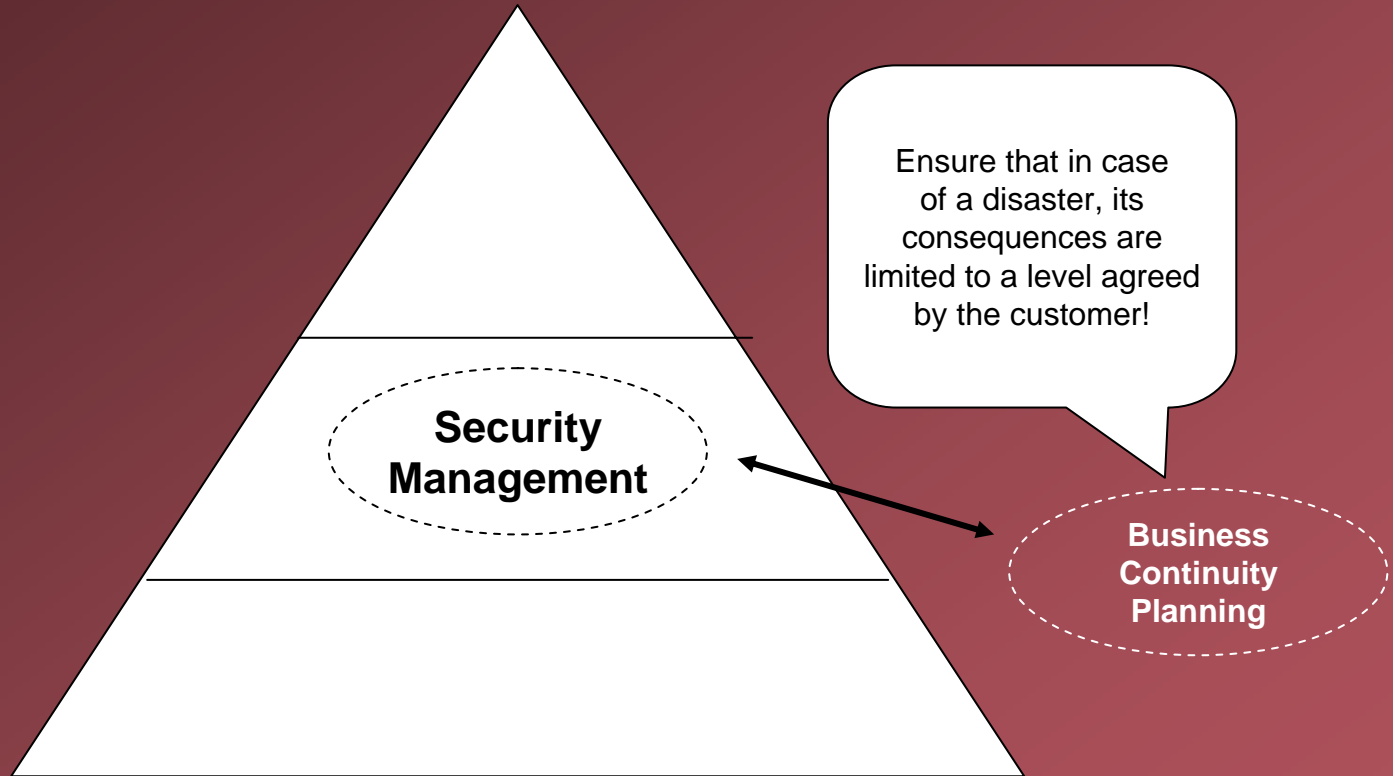
Relation with Service Delivery



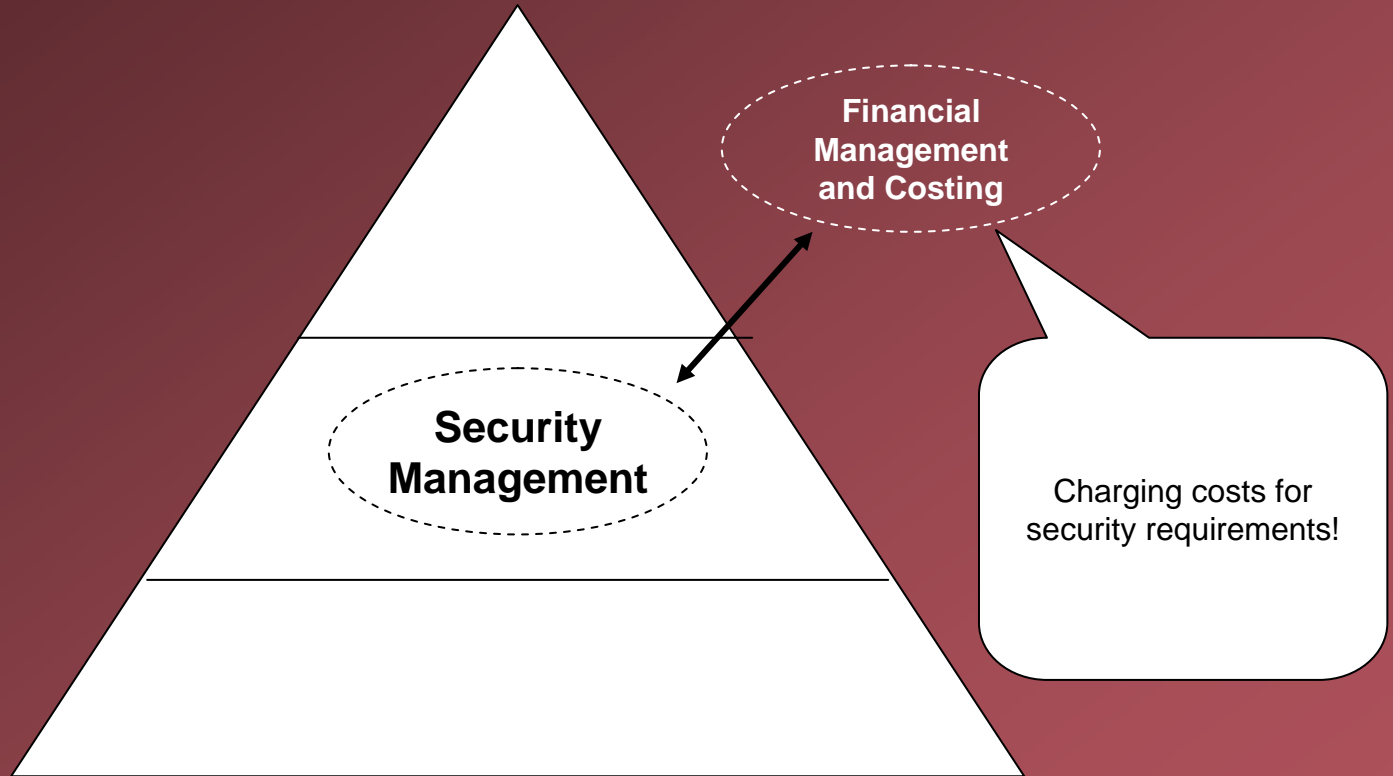
Relation with Service Delivery



Relation with Service Delivery



Relation with Service Delivery



Guidelines for organisation

Service Provider

Security Manager

Responsible for the Security Management Process at the service provider to fulfil security demands as specified in SLA



Customer

Security Officer

Responsible for security requirements in the customers organisation and co-ordinates assessing the business risks

Assurance issues

- Ensure that Security Service Level Agreement exists
 - Are security demands defined and agreed?
- Assess Effectiveness and Efficiency of the SLA
 - Does it cover the current business & IT environment?
 - Is it implemented and understood?
 - Evaluation (audits, reviews and self assessments)?
- Verify responsibility
 - Security manager role assigned?

Assurance issues

- Walk-through defined ITIL processes:
 - Are ITIL processes implemented with Security Management requirements?
 - Configuration and asset management / Incident control and Help Desk / Change Management / Release Management
 - Service Level Management / Availability Management / Performance and Capacity Management / Business Continuity Planning / Financial Management and Costing

Implementation issues

- Include security requirements in contracts
- Specify security requirements in SLA
- Draw up security plan
- Specify roles and responsibilities
 - Security Manager versus Security Officer
- Add security measures in ITIL processes
- Evaluation

- The need to know -

Scillani Information AB

Ekgatan 6

SE 230 40 BARA

Phone +46 (0)40 – 54 31 31

Fax +46 (0)40 – 54 31 30

Internet: www.scillani.com

E-mail: info@scillani.se