11 Security Management

Download printable version

IT Security Management is the process of managing a defined level of security for information, IT services and infrastructure. IT Security Management enables and ensures that:

- Security controls are implemented and maintained to address changing circumstances such as changed business and IT service requirements, IT architecture elements, threats, etc
- Security Incidents are managed
- Audit results show the adequacy of security controls and measures taken
- Reports are produced to show the status of information security.

IT Security Management needs to be part of every IT manager's job description. Management is responsible for taking appropriate steps to reduce the chances of a security Incident occurring to acceptable levels. This is the process of risk assessment and management.

Corporate executive management is accountable to stakeholders and shareholders for security, and is responsible for defining the corporate security policy. IT Security Management is governed by that policy. The existence of the policy registers and reinforces the corporate decision to invest in the security of information and information processing. It provides management with guidelines and direction regarding the relative importance of various aspects of the organisation, and of what is allowable and what is not, in the use of ICT systems and data.

Figure 11 illustrates the information security process as seen by the business. It covers all stages, from policy setting and initial risk assessment, through planning, implementation and operation, to evaluation and audit.

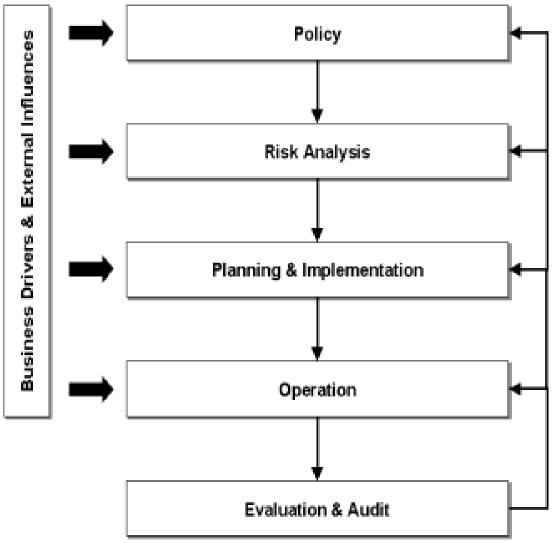
Business Drivers & External Influences
Policy
Risk Analysis
Planning & Implementation
Operation
Evaluation & Audit

Figure 11: The Information Security Model (ISM)

Every organisation must have an information security policy that is widely circulated, committed to by everyone within the organisation and actively enforced and reviewed.

Figure 12 provides an overview of the ITIL IT Security Management Process. The process shows the complete route from the collection of a Customer's requirements, through planning, implementation, evaluation and maintenance – under a framework of control - with regular status reporting to the Customer closing the loop.

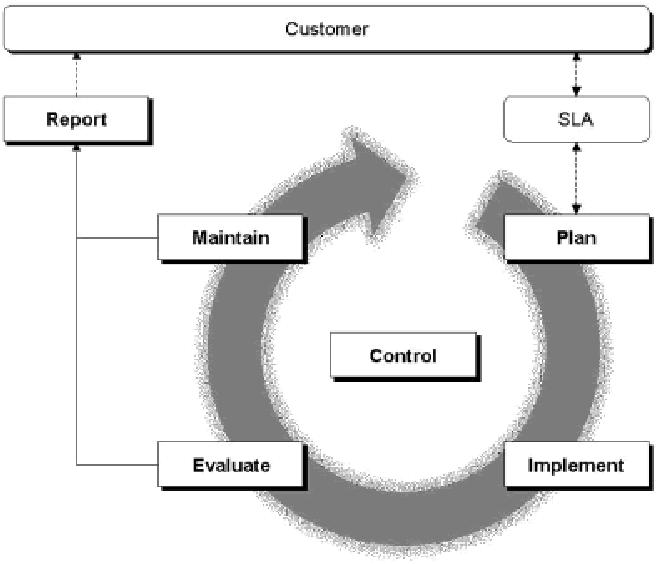

Figure 12: The IT Security Management Process

Intrinsic elements of all activities within the IT Security Management process are risk and vulnerability assessment, and management and the implementation of cost justifiable countermeasures to reduce vulnerability and risk to an acceptable business level. These activities must be closely co-odinated with all other areas of Service Management, especially the Availability and IT Service Continuity Management processes.

Table of contents | **Previous** | **Next**

Back to top

OGC Successful Delivery Toolkit™ 2005 // Version 5.00