IT security management

- IT security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability
  ISO 13335:1
IT security management functions

- Determining organizational IT security objectives, strategies and policies
- Determining organizational IT security requirements
- Specifying appropriate safeguards
- Monitoring the implementation and operation of safeguards
- Developing and implementing security awareness
- Detecting and reacting to incidents

Code of practice for information security management

ISO 17799
(SS 627799)
Scope of ISO 17799

- List of best practices for information security management
  - It lacks a process and does not describe the activities involved in information security management (the to be published ISO 27003 should fix this problem)
- It is based on risk management
- ISO 27001 allows certification according to ISO 17799 (which will be renamed ISO 27002)

Key Controls I

- Security Policy
  - Defines the purpose of a policy and what it should contain
- Security Organization
  - Propose an organizational structure and how to deal with third parties
- Asset classification
  - How to define assets and analyze risks for them
- Personnel security
  - Requires the definition of job descriptions (for security), how to train users and how to handle security incidents by the personnel
Key Controls II

- Physical & environmental
  - Defines the need for security areas, equipment security and general controls for workplaces

- Communications and operations management
  - Describes operational procedures, logging and back-up strategies, network management, information and software exchange and media handling

- Access Control
  - Suggests AC for various systems and the corresponding administrative procedures

Key Controls III

- Systems development & maintenance
  - Defines how to develop and maintain software systems

- Business continuity management
  - Propose the establishment of a business continuity management

- Compliance to legal provisions
  - Defines which legal requirements have to be followed and what system audit is necessary
Guidelines for the management of IT Security

ISO 13335

Scope of GMITS Series I

  - outlines a sequential security management process

- [ISO 13335-2, 1997] **Managing and planning IT Security**
  - the activities of the process are outlined
  - covers a policy hierarchy
  - covers proposal for an organizational wide security structure
Scope GMITS Series II

  - Discuss four different risk analysis approaches are proposed
  - Discuss Implementation of the IT Security Plan
  - Discuss the follow up

- [ISO 13335-4, 2000] Selection of safeguards
  - describes a number of safeguards for physical protection and IT systems protection
  - propose a method to select the appropriate safeguards
Scope GMITS Series III

  - covers network security safeguards

- GMITS aims for closed systems - system's that are aimed for internal use
- Sequential nature of the process
- Excellent checklist for security management techniques

Basic Protection Manual

Bundesamt für Sicherheit in der Informationstechnologie

Scope of BPM

- BPM provides a detailed set of standard security measurements for “normal” computer systems – a baseline approach
  - Fantastic as a checklist!
- To support a large variety of system BPM has a modular approach
- Although remarkably well written with 2500+ pages “heavy literature”

<table>
<thead>
<tr>
<th>Generic Components</th>
<th>Infrastructure</th>
<th>Non-Networked Systems</th>
<th>Networked Systems</th>
<th>Data Transmission Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security Management</td>
<td>Buildings</td>
<td>DOS PC (Single User)</td>
<td>Servers-Supported</td>
<td>Exchange of Data Media</td>
</tr>
<tr>
<td>Organisation</td>
<td>Cabling</td>
<td>UNIX System</td>
<td>UNIX Servers</td>
<td>Modem</td>
</tr>
<tr>
<td>Personnel</td>
<td>Rooms - Office</td>
<td>Laptop PC</td>
<td>Peer-to-Peer Services</td>
<td>Firewall</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>Rooms - Server Room</td>
<td>PCs with a Non-Constant User</td>
<td>Windows NT Network</td>
<td>E-mail</td>
</tr>
<tr>
<td>Data Backup Policy</td>
<td>Rooms - Data Media Archives</td>
<td>PC under Windows NT</td>
<td>Novell Netware 3.x</td>
<td>Web Servers</td>
</tr>
<tr>
<td>Data Protection</td>
<td>Rooms - Technical</td>
<td>PC with Windows 95</td>
<td>Novell Netware 4.x</td>
<td>Remote Access</td>
</tr>
<tr>
<td>Computer Virus Protection</td>
<td>Protective Cabinets</td>
<td>Windows 2000 Client</td>
<td>Heterogeneous Networks</td>
<td>Lotus Notes</td>
</tr>
<tr>
<td>Hardware and Software</td>
<td>Working Files at Home</td>
<td>Internet PC</td>
<td>Network and System Information</td>
<td>Information</td>
</tr>
<tr>
<td>Cryptosconcept</td>
<td></td>
<td></td>
<td></td>
<td>Exchange/Outlook2000</td>
</tr>
<tr>
<td>Outsourcing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Holistic Security Management

For e-commerce

Business drivers for security

- Competitive advantage ⇒ business enabler
- Protecting ⇒ insurance

Security requirements  Top down

System security

Risk management  Bottom up
Environment

- Society
  - Legislation
  - Standards
  - Ethics
- Business
  - Business model
  - Business process
  - Business structure
  - Planning Model
Components

- Business Modeling
- Project Planning
- Security Planning
- Security Implementation
- Maintenance
- Privacy
- Humans and Organization
- Business Foundation

Workflow – Phases and iterations

- Inception
  - Starting
- Elaboration
  - Defining
- Construction
  - Building
- Transition
  - Deploying
- Operation
  - Running
Business Modeling

Security-enhanced business modeling

- The security enhanced business model identifies where
  - sensitive information is processed
  - the sphere of influence is left
  - interaction is required
- Business, security-enhanced business and security activities form the business model
Project Planning

Security analysis and design

- Security analysis aims to understand the requirements
- Component analysis identifies existing security measures that can be used
- Security design prepares for the implementation of security
Implementation

Security-enhanced Software Design

Validation

Organizational Implementation

Security Architecture - AD

Documentation

Technical Implementation

Deployment

System test

Design Model

Infrastructure development

Validation and Testing

Code

Documentation

Validation Report

Maintenence

Technical Maintenance

System Monitoring

External Audit

Internal Audit

Business Foundation

Humans and Organizations Activities

Incident - Response

Consequence Analysis and Planning

Implement Fix

[Technical Problem]

[Incident]

[Problem]

[Minor Problem]

Acceptable or Insurable

New Project

[Fix not available]

[Fix available Fix]

Risk acceptance or Insurance

Minor Adjustment

The un guarded feedback loops represent the continuous character.
Support activities

- Humans and organization
  - Conduct security training and education
  - Improve security awareness
  - Provide motivation
  - Enable communication
  - Organizational activities

- Business Foundation
  - Monitoring and Auditing
  - Controlling and Measuring
  - Project Management
  - Conducting Risk Analysis
  - Investigating Feasibility

Business Continuity Planning
Business Continuity Planning

- IT Disaster Recovery planning
  - Addresses the continuity planning needs of the IT infrastructure
- Business operations planning
  - Continuity of the organizations business operations

Business Continuity Planning

- Crisis management planning
  - Forming and training of management teams handling the emergency situation
- Continuous availability planning
  - Focus on high up-time (>99%) due to criticality
BCP Process

- Current state assessment
  - Is situation analysis
- Process risk and impact base-lining
  - Investigate problem areas
- Develop Strategy
  - Mitigation strategy for problems
- Establish Infrastructure & Implementation
  - Realize the preconditions and to initial tests
- Operate environment
  - Keep the system running and test its readiness

Characteristics BCP

- Recovery Organization
  - Disaster recovery staff
  - Incident monitoring
  - Crisis Management
- Resources
  - Plans
  - Facilities
  - Non-IT related resources
- Maintenance
  - Change Management (Capacity planning)
  - Disaster recovery drills
Questions ?