Management of IT Security
Managing security

- Situation Analysis
- Risk assessment
  - Assets
  - Threats
  - Risks
- Security policy
- Security controls
- Implementation
- Validation
Risk assessment

- Inventory of all assets (V)
- Inventory of all threats (M)
- Probability estimation for each threat (P)

\[ R = \sum P_{M_i} V_i \]
## Risk assessment

<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Low</td>
</tr>
</tbody>
</table>

- The risk must be brought to an acceptable level
  - Reduce, transfer, refuse
Risk assessment alternatives

◆ Security baseline
  ■ Standards
    ◦ ISO 27002
    ◦ German BSI Grundschutz catalogs
    ◦ Center for Internet Security (CSI) benchmarks
  ■ Gap analysis
  ■ Achieve a security baseline, independent of your risk

◆ Attack trees
  ■ Identify all actions and scenarios that would lead to a loss
  ■ Assign probabilities to each path in the tree
Attack tree example

Accès au données chiffrées stockées dans un serveur et déchiffrement des données

Accès au serveur

être administrateur

Accès physique à la salle serveur

Trouver une faille technique

Connaitre la clé

Trouver la clé dans un fichier

Trouver une copie des données non chiffrées
Security Policy

◆ Security «Bible»:
  - Inventory of data system
  - Classification of data
  - Identification of security domains
  - Physical and organisational aspects
  - Rules of the game

◆ Existing standards:
  - ISO 27002
Security controls

- Security service with defined mission and competencies

- Technological choices
  - firewalls, filters, anti-virus
  - encryption, electronic signatures
  - authentication & access control

- Contingency plan
  - Technical controls
  - Legal actions
  - Public relations
Implementation

- Nominate personnel
- Assign tasks
- Install equipment
- Configure
Validation

- Automatic validation with the help of vulnerability scanners
- Manual audit
- Intrusion tests (« ethical » hackers)
Key documents

- Charter (motivation, why?)
- Policies (what?)
- Standards (how?)

Diagram:
- Charter
- Security policy
- Encryption standard
- Firewall standard
- Server
- Anti-virus
- Authentication
- Back-up plan
- etc
ISO 270XX standards

ISO 27001 SMSI
ISO 27005 risk management
ISO 27004 monitoring evaluation
ISO 27003 ISMS implementation
ISO 27002 security controls
ISO 27000 vocabulary
ISO 27008 audit of controls
ISO 27007 ISMS auditing
ISO 27006 ISMS certification
ISO 27001

- Specifies the requirements for establishing, operating, improving and documenting an ISMS
- ISMS: Information security management system
  - Context, scope, risk assessment, security policy, monitoring
- Certifiable standard
Plan-Do-Check-Act

Figure 1 — PDCA model applied to ISMS processes
ISO 27002

- Reference document
- Contains complete set of security controls, based on best practices
- 14 sections with a total of 114 controls
- No certification:
  - Recommendations, not mandatory
ISO 27002

5. Information security policies
6. Organization of information security
7. Human resource security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
ISO 27002

13. Communications security
14. System acquisition, development and maintenance
15. Supplier relationships
16. Information security incident management
17. Information security aspects of business continuity management
18. Compliance
ISO 27002

- Typical use of this standard
  - Reference catalogue of security controls:
    - Make sure you did not forget anything
  - Gap analysis
    - Measure how far you are
  - Dashboard
    - Present performance according to chapters of the standard
  - Audits:
    - Present results according to chapters of the standard
ISO 27002: Example

12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

Control: Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Implementation guidance: Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls.

The following guidance should be considered:

a) establishing a formal policy prohibiting the use of unauthorized software (see 12.6.2 and 14.2.);...
Conclusions

- IT security management is only possible
  - With support from upper management
    - It costs money and effort
    - People must comply
  - With a documented policy
    - We need to know what we want to achieve
  - With proper awareness training.