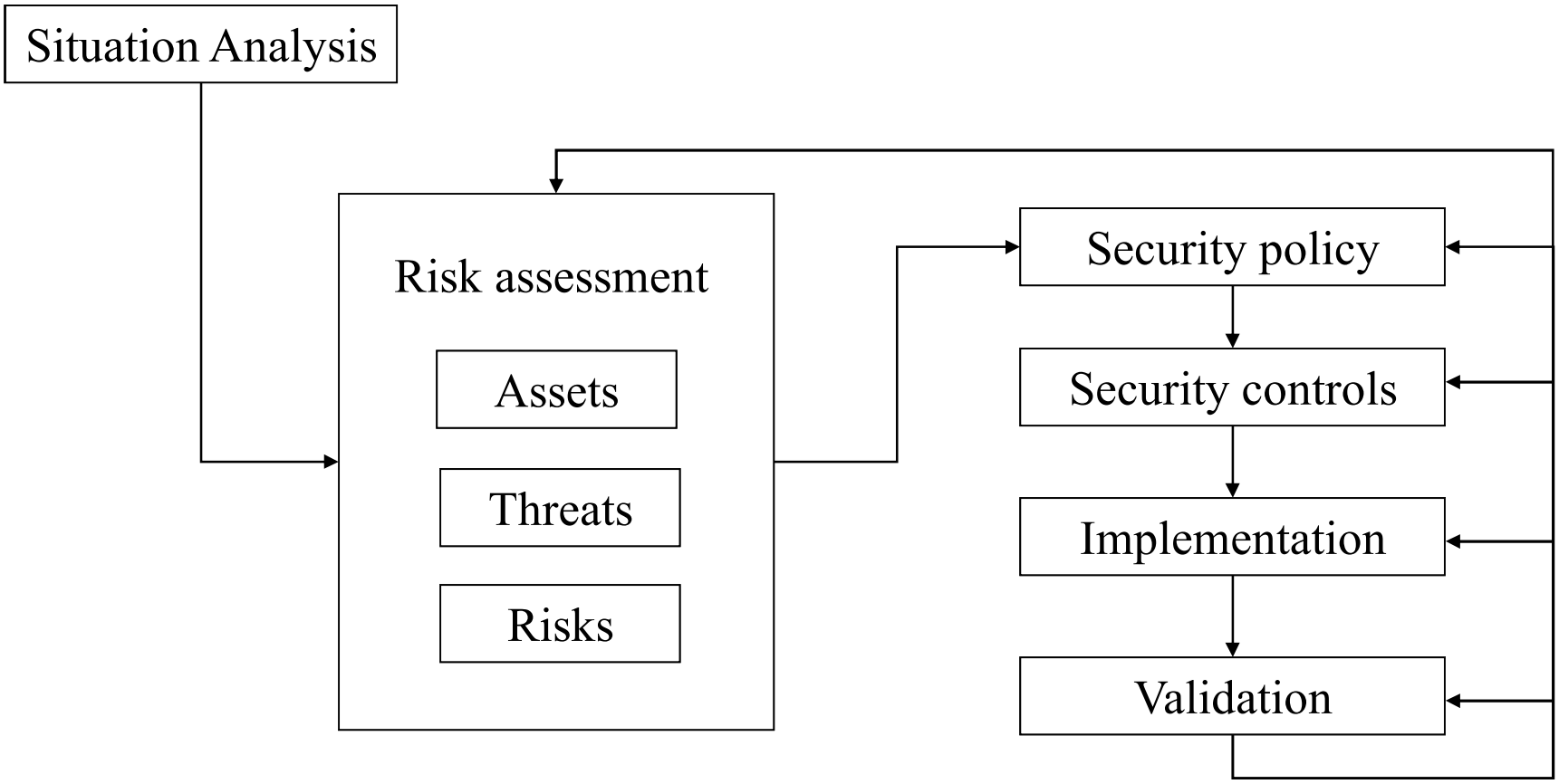
Management of IT Security

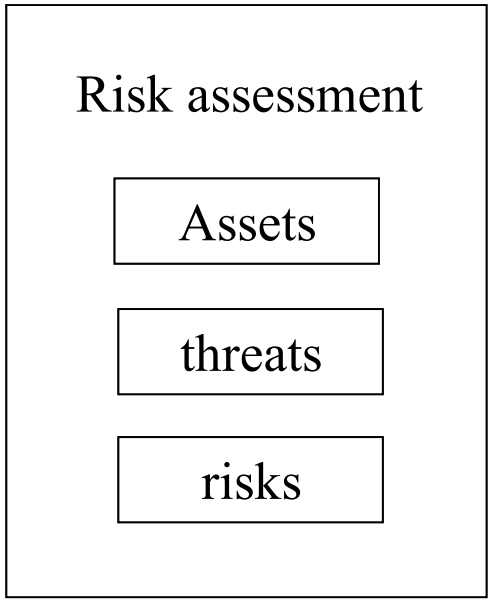
Managing security



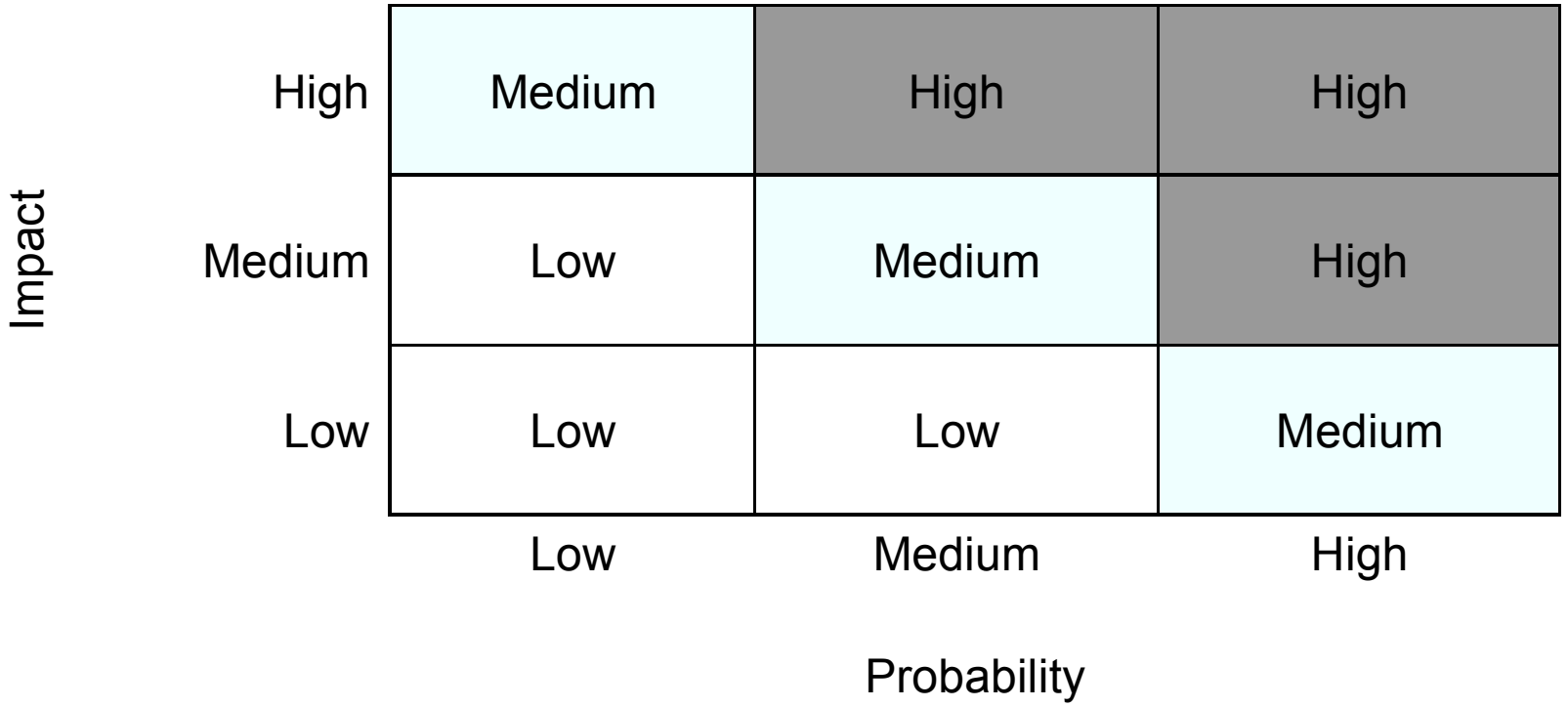
Risk assessment

- 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

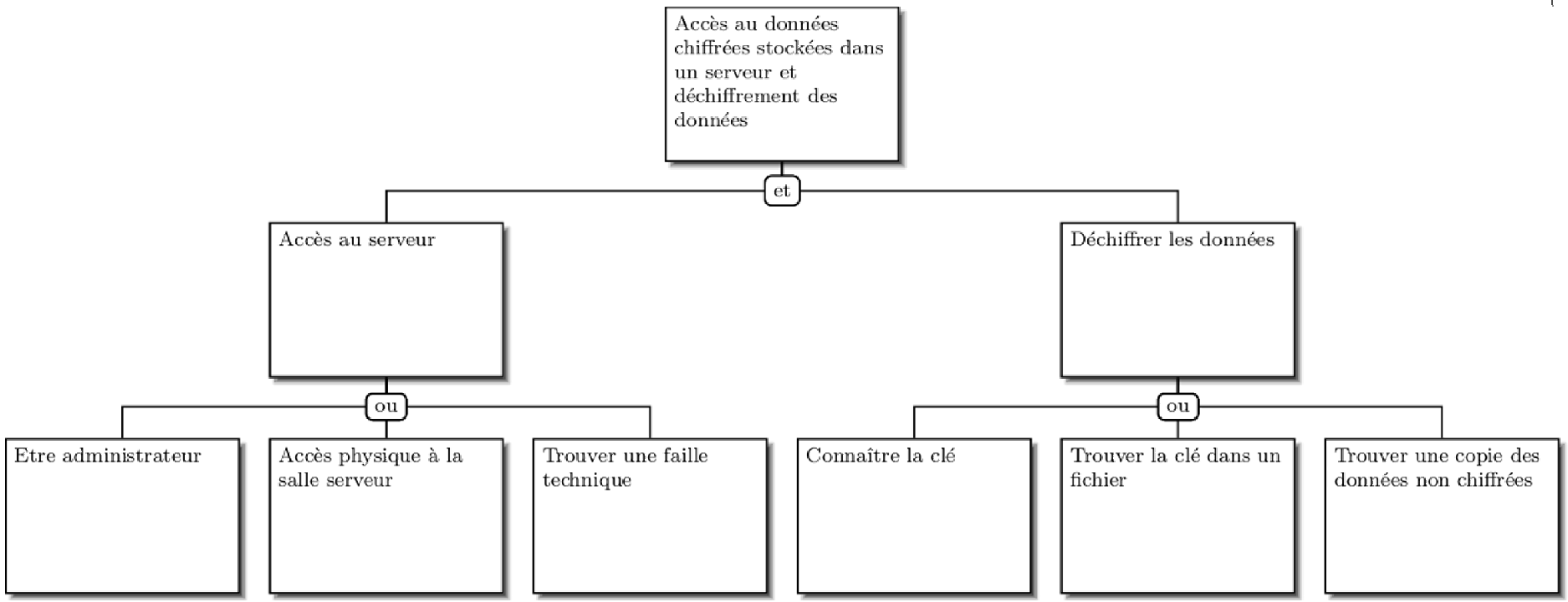


- The risk must be brought to an acceptable level
  - Reduce, transfer, refuse

Risk assessment alternatives

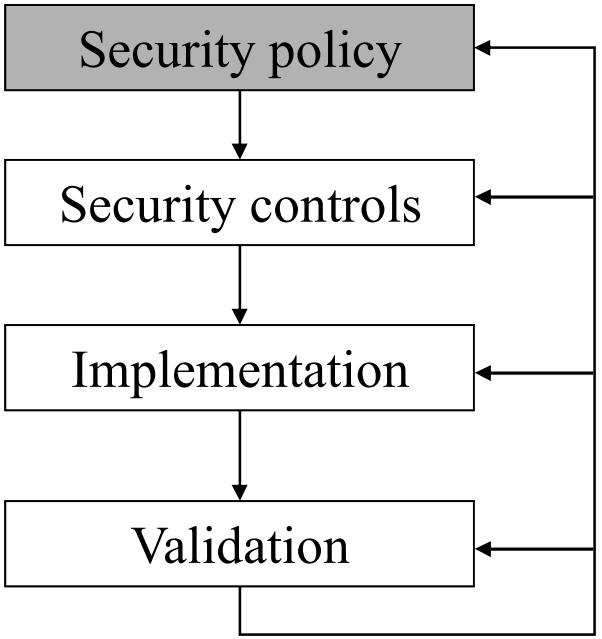
- Security baseline
  - Standards
    - ISO 27002
    - German BSI Grundschutz catalogs
    - Center for Internet Security (CSI) benchmarks
  - Gap analysis
  - Achieve a security baseline, indepent of your risk
- Attack trees
  - Identify all actions and scenarios that would lead to a loss
  - Assign probabilities to each path in the tree

Attack tree example



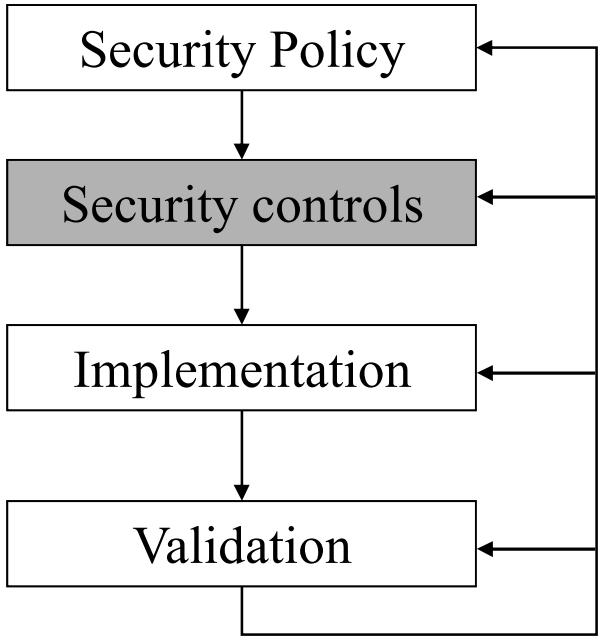
Security Policy

- 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



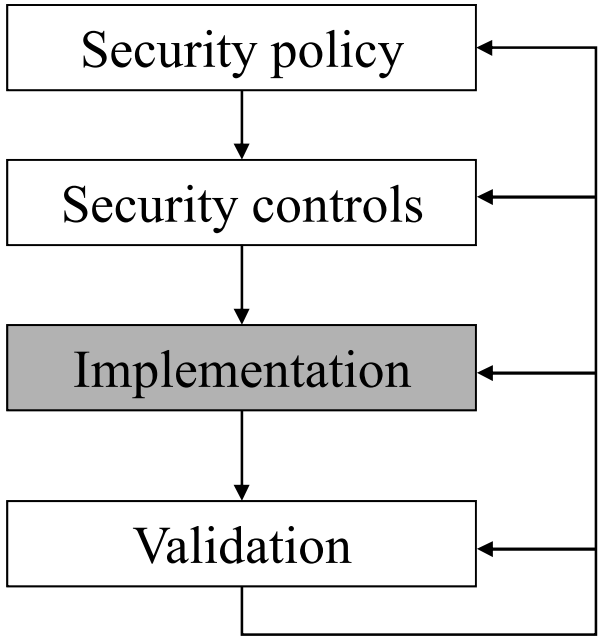
Security controls

- 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



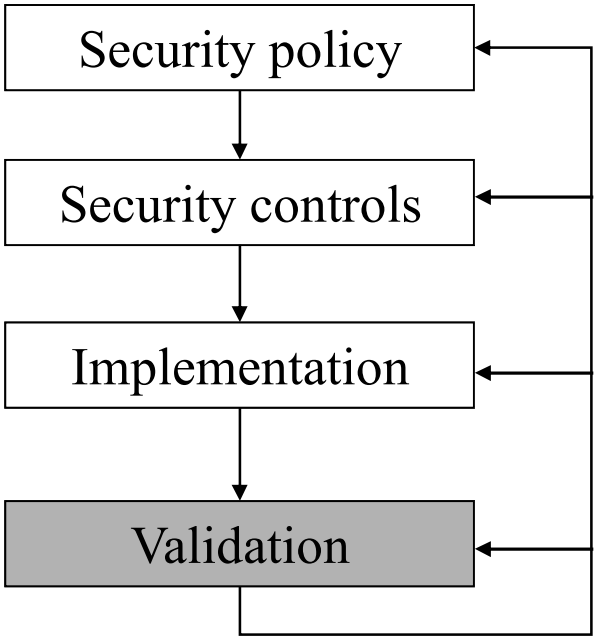
Implementation

- Nominate personnel
- Assign tasks
- Install equipment
- Configure



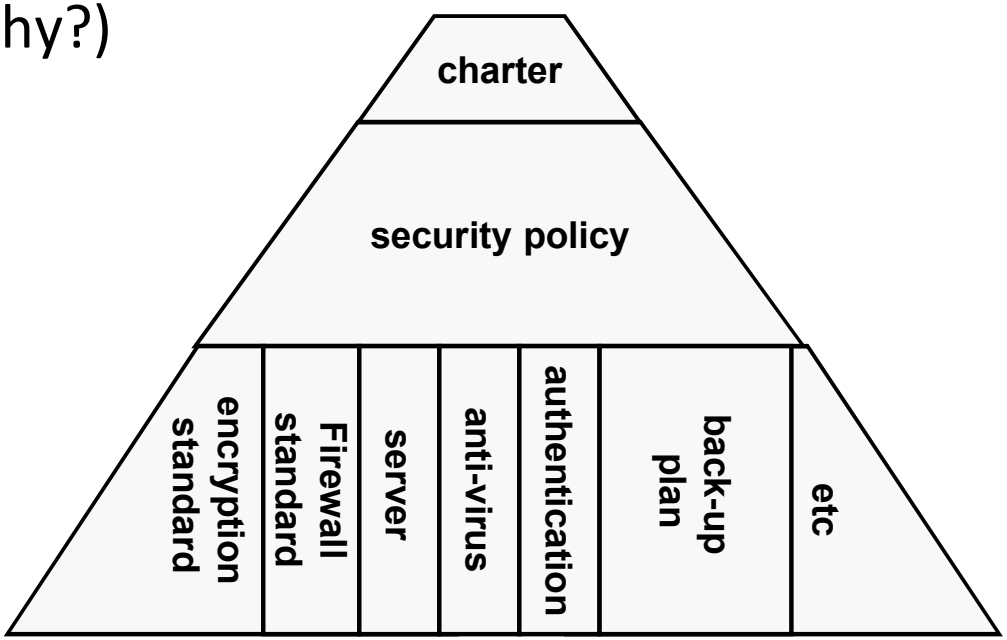
Validation

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



Key documents

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



ISO 270XX standards

ISO 27001

- ISO 27001: **Information technology – Security techniques – information security management systems – Requirements**
- Specifies the requirements for establishing, operating, imporving and documenting an ISMS
- ISMS: Information security management system
  - Context, spcope, risk assessment, security policy, monitoring
- Certifiable standard

Plan-Do-Check-Act

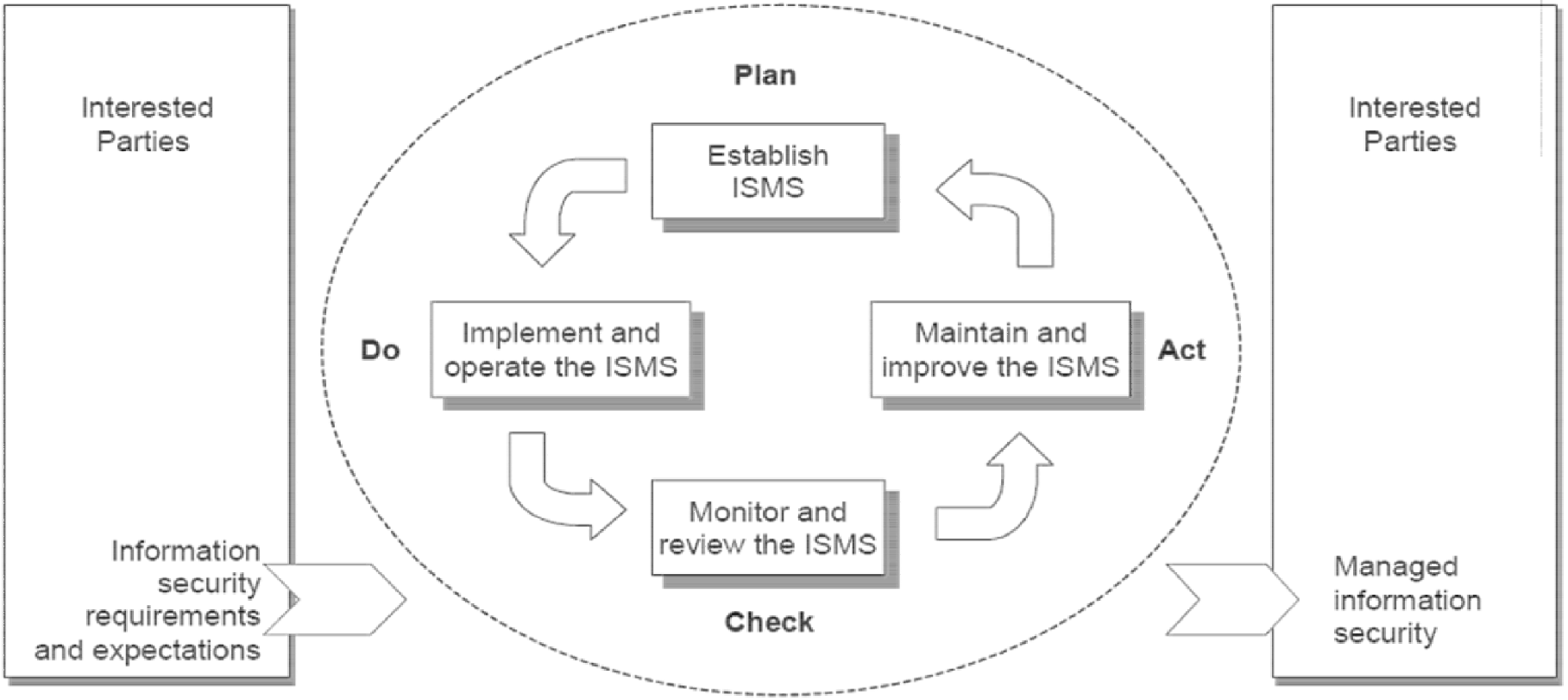


Figure 1 — PDCA model applied to ISMS processes

ISO 27002

- ISO 27002: **Information technology – Security techniques – Code of practice for information security controls**
- Reference document
- Contains complete set of security controls, based on best practices
- 14 sections with a total of 114 controls
- No certification:
  - Recommandations, 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, informationsecurity 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.