

ISMS

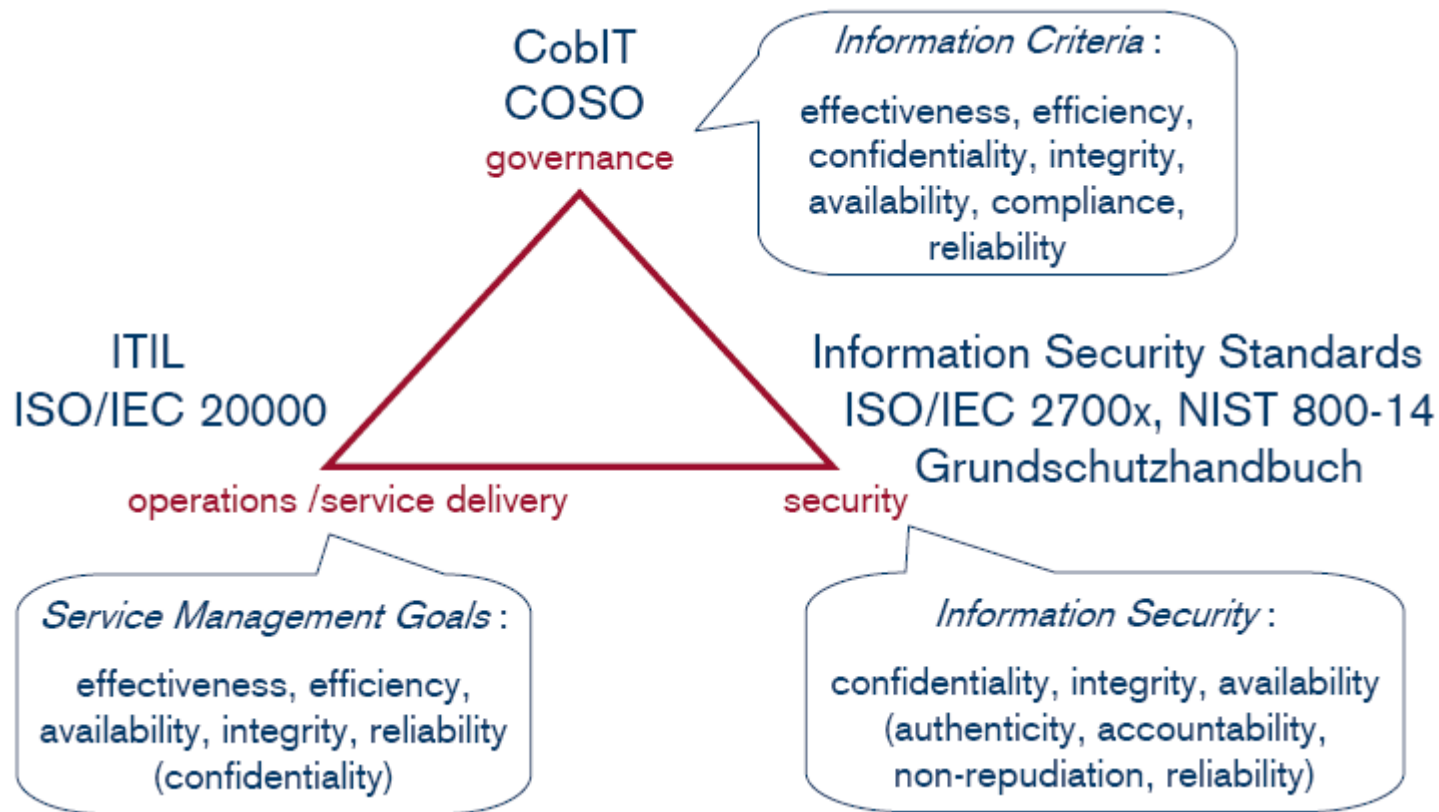
Information Security Management System

ISO/IEC 27001:2005

ISO/IEC 27002:2005

Version 3.02, March 2007

IT Management Standards



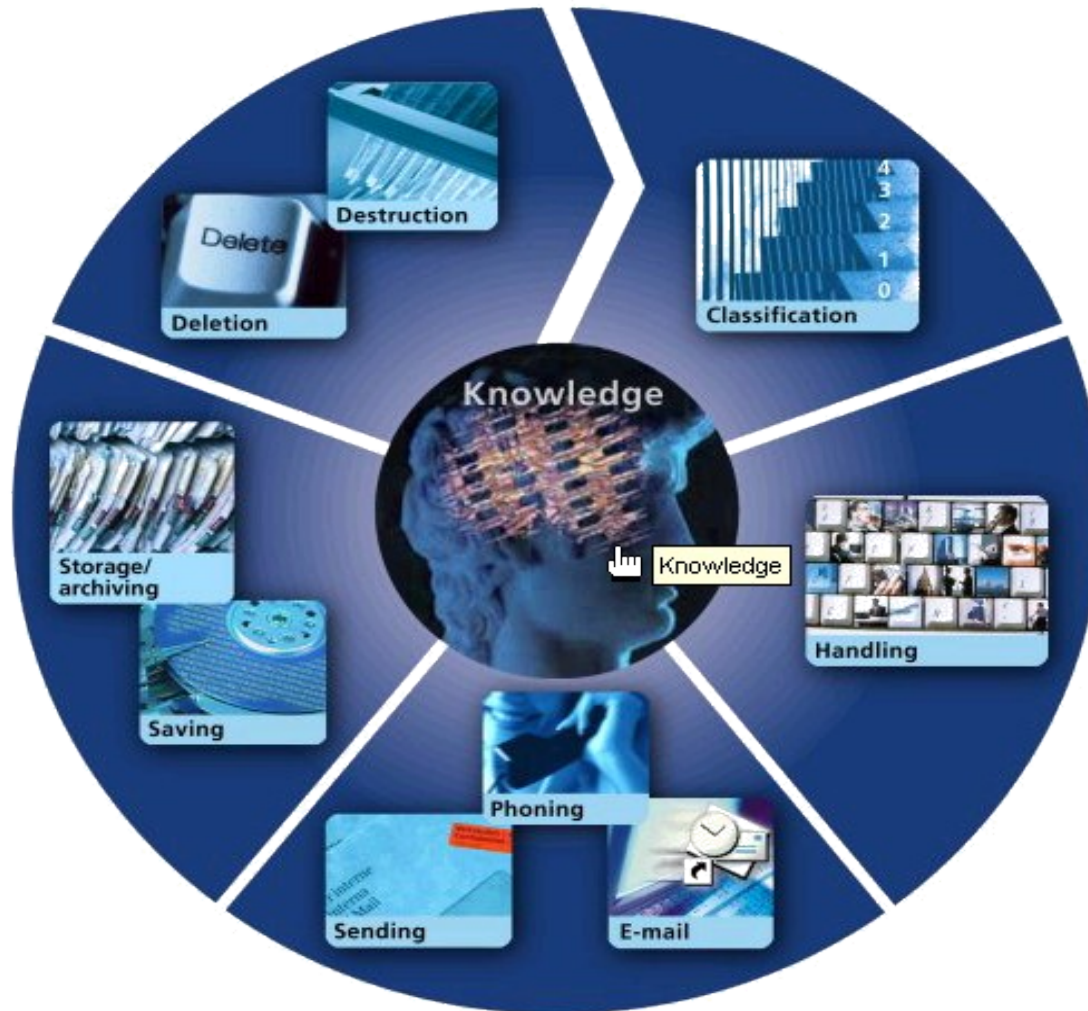
What is Information?



“Information is an asset which, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected.”

ISO/IEC 27002:2005

Information Lifecycle



Management Systems

- ISO 9001 (QMS), ISO 14001 (EMS), ISO/IEC 27001 (ISMS), ISO/IEC 20000-1 (IT Service Management)
- Documented systems
- Adopted the PDCA model (Deming cycle)
- Focus on management processes, procedures and controls
- Aim at continual improvement
- Associated with certification activities
- Core of ISO/IEC 27001 is 9 pages only

What is an Information Security Management System?

An Information Security Management System (ISMS) is an systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems



What is ISO 27002 and ISO 27001?

ISO 27002 (formerly ISO 17799)

Code of practice for information security management

ISO 27001 (formerly BS 7799)

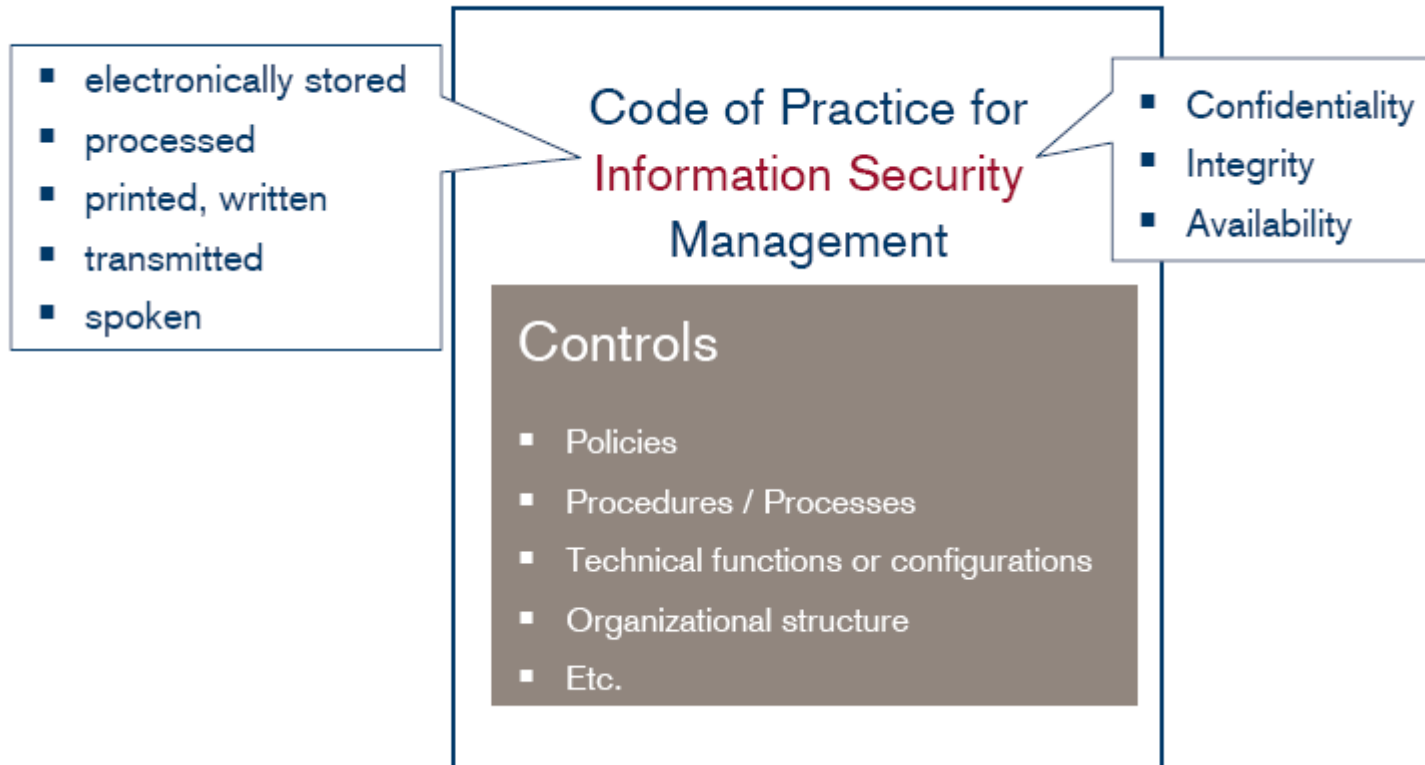
Specification for Information Security Management
Systems (ISMS)



ISO/IEC 27000-Series

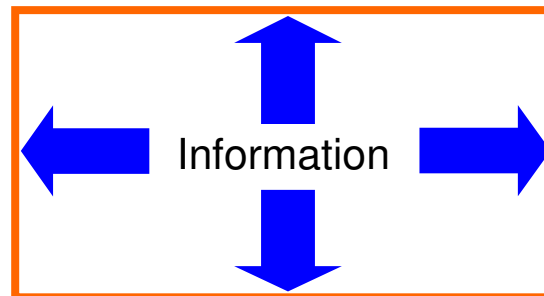
- **ISO 27000** – vocabulary and definitions (terminology for all of these standards)
- **ISO 27001** – the main Information Security Management System requirements standard (specification),
- **ISO 27002** (currently known as ISO 17799) – this is the Code of Practice describing a comprehensive set of information security control objectives and outlines a menu of best-practice security controls.
- **ISO 27003** – will contain implementation guidance
- **ISO 27004** – will be a new Information Security Management Metrics and Measurement standard to help measure the effectiveness of ISMS implementations
- **ISO 27005** – will be a new Information Security Risk Management standard (to replace BS 7799 Part 3)
- **ISO 27006** - Requirements for the accreditation of bodies providing certification of information security management systems

ISO/IEC 27002 - Scope



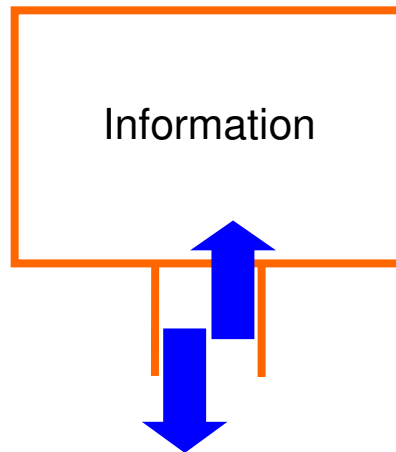
Confidentiality

- Confidentiality
ensuring that information is accessible only to those authorized to have access
(ISO/IEC 27002:2005)



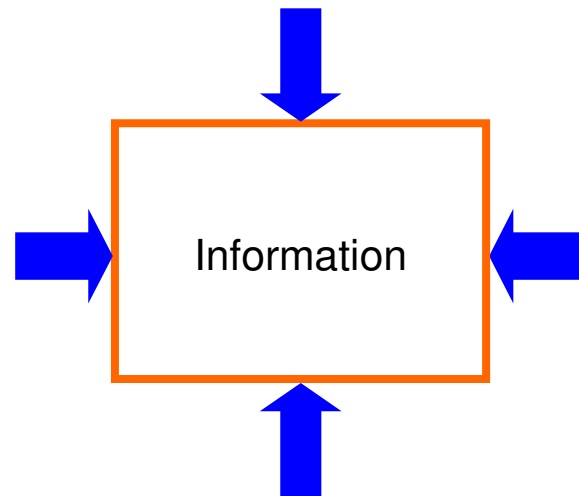
Integrity

- Integrity
safeguarding the accuracy and completeness of information and processing methods (ISO/IEC 27002:2005)



Availability

- Availability
ensuring that authorized users have access to information and associated assets when required (ISO/IEC 27002:2005)



ISO/IEC 27002:2005 - Content

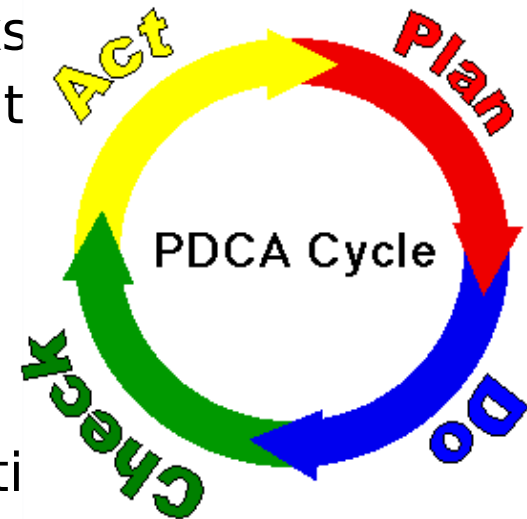


ISO/IEC 27001: ISMS Highlights


Clarifies and improves existing PDCA process requirements

- ISMS scope (inc. details & justification for any exclusions)
- Approach to risk assessment (to produce comparable & reproducible results)
- Selection of controls (criteria for accepting risks)
- Statement of Applicability (currently implement)
- Reviewing risks
- Management commitment
- ISMS internal audits
- Results of effectiveness and measurements (summarised statement on 'measures of effectiveness')
- Update risk treatment plans, procedures and controls

SQS



Contents of ISO/IEC 27001:2005

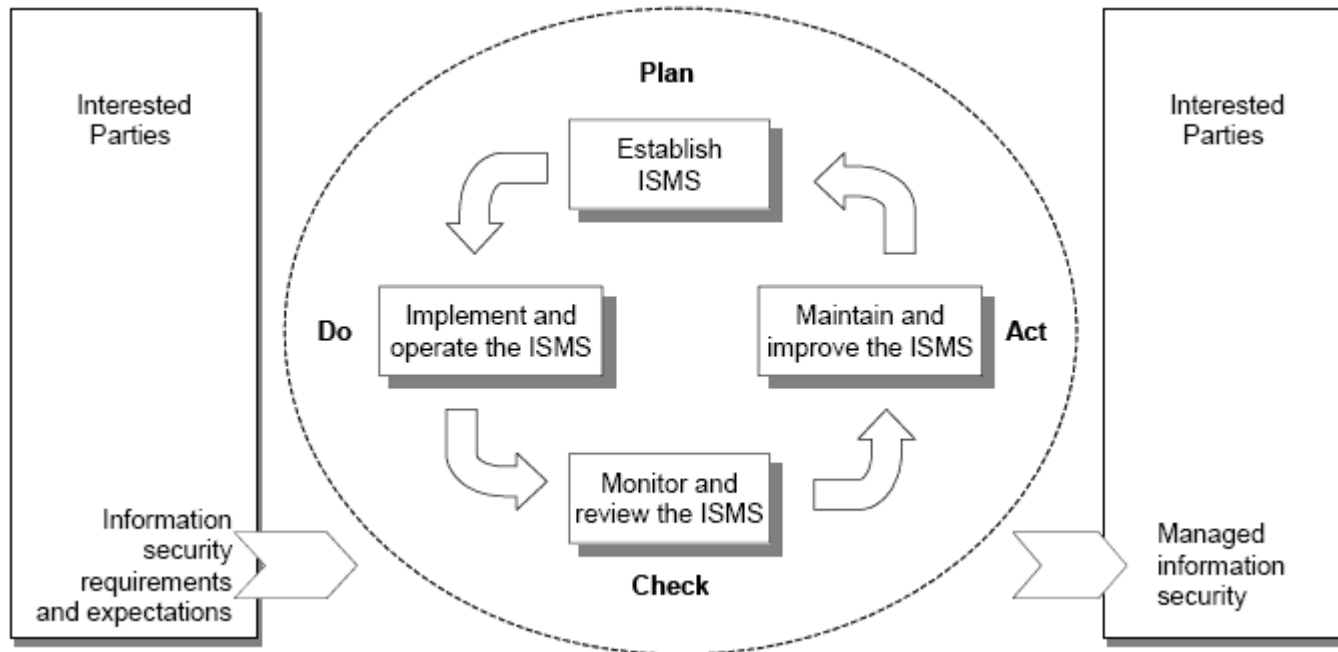
- 0. Introduction and Process approach
- 2. Scope
- 3. Normative references
- 4. Terms and definitions
- 5. Information security management system (ISMS)
- 6. Management responsibility
- 7. Internal ISMS audits
- 8. Management review
- 9. ISMS improvement
- J. Control objectives and controls
- A.5 Security policy
- A.6 Organization of information security
- A.7 Asset management
- A.8 Human resources security 
- A.9 Physical and environmental security
- A.10 Communications and operations management
- A.11 Access control
- A.12 Information systems acquisition, development and maintenance
- A.13 Information security incident management
- A.14 Business continuity management
- A.15 Compliance

Compatibility with other management systems

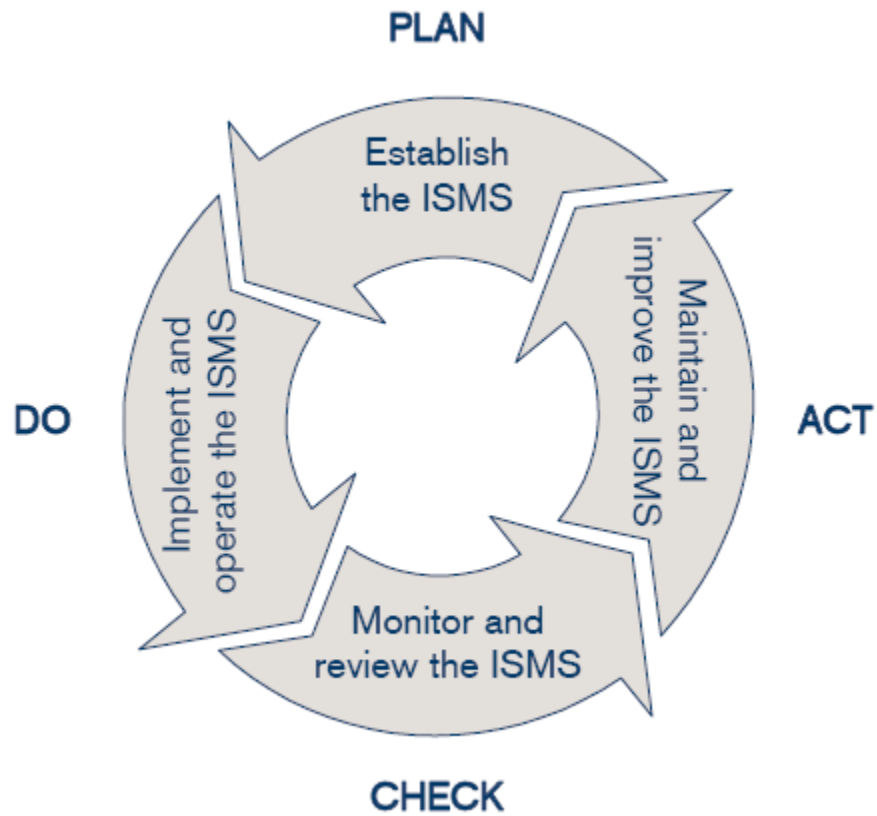


- This International Standard is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards.

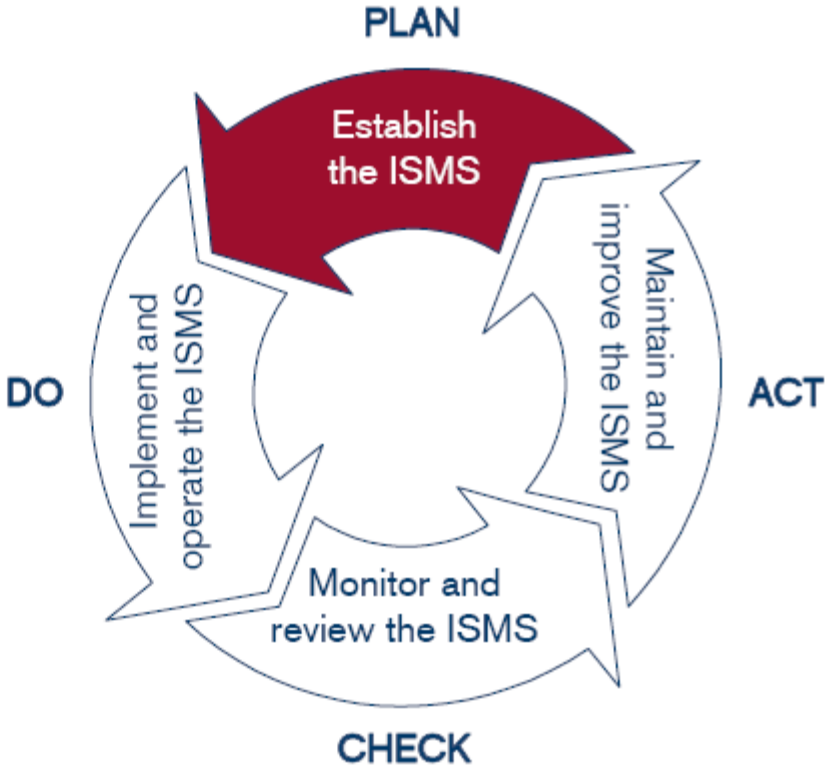
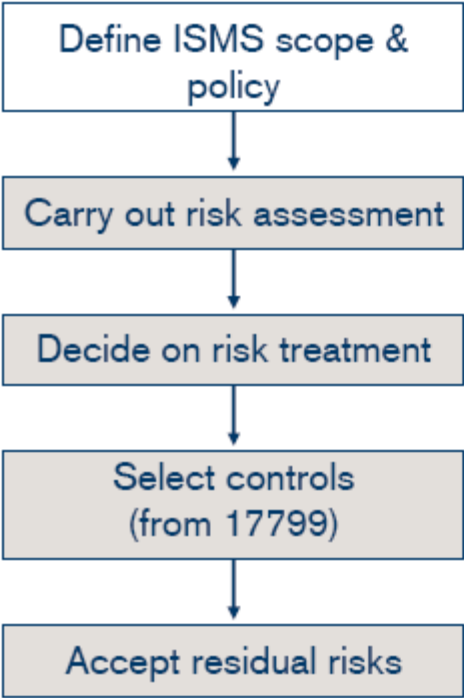
Process approach



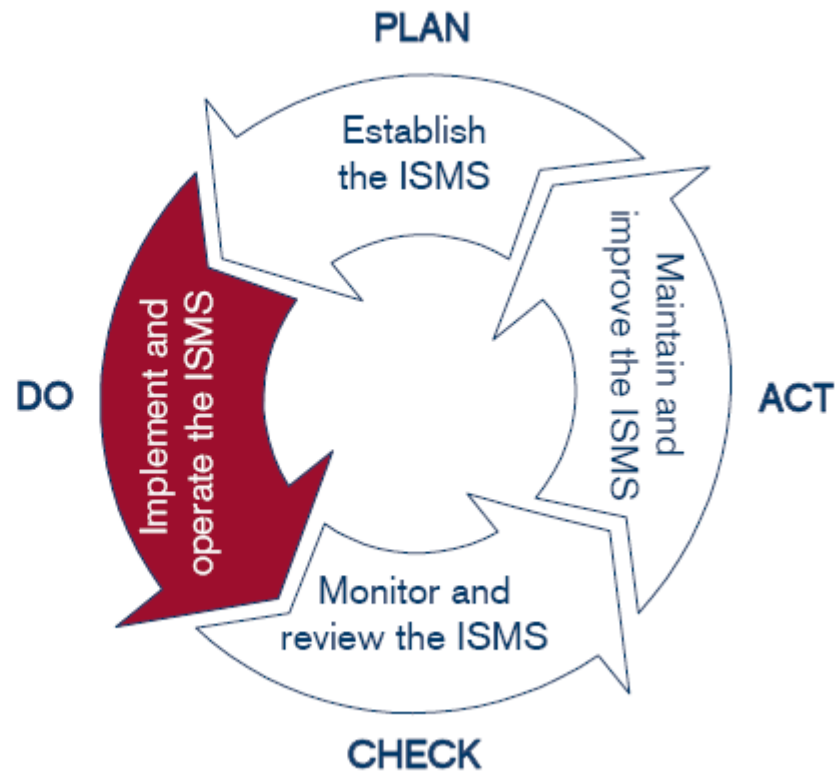
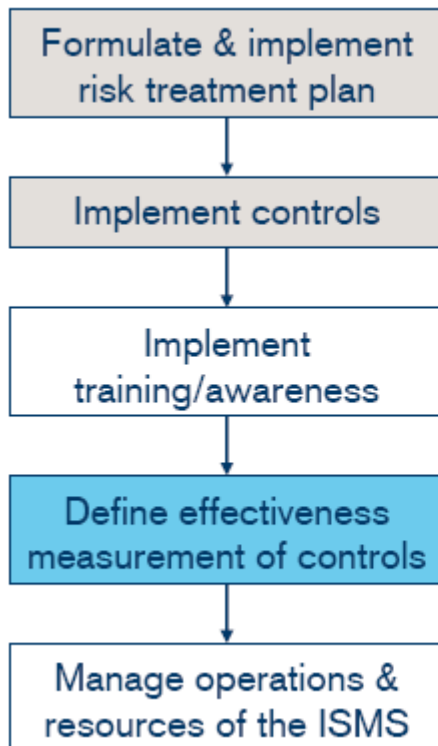
PDCA Model



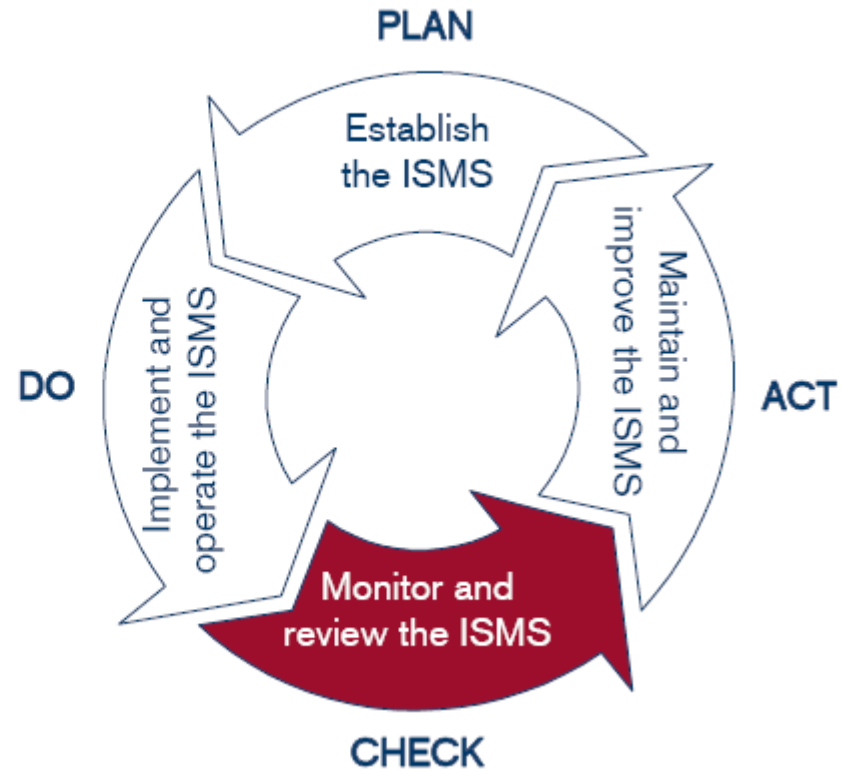
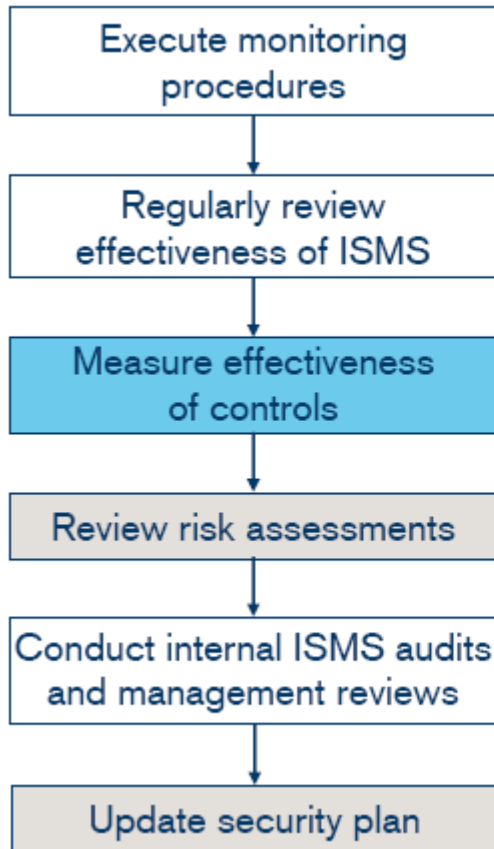
Establish the ISMS



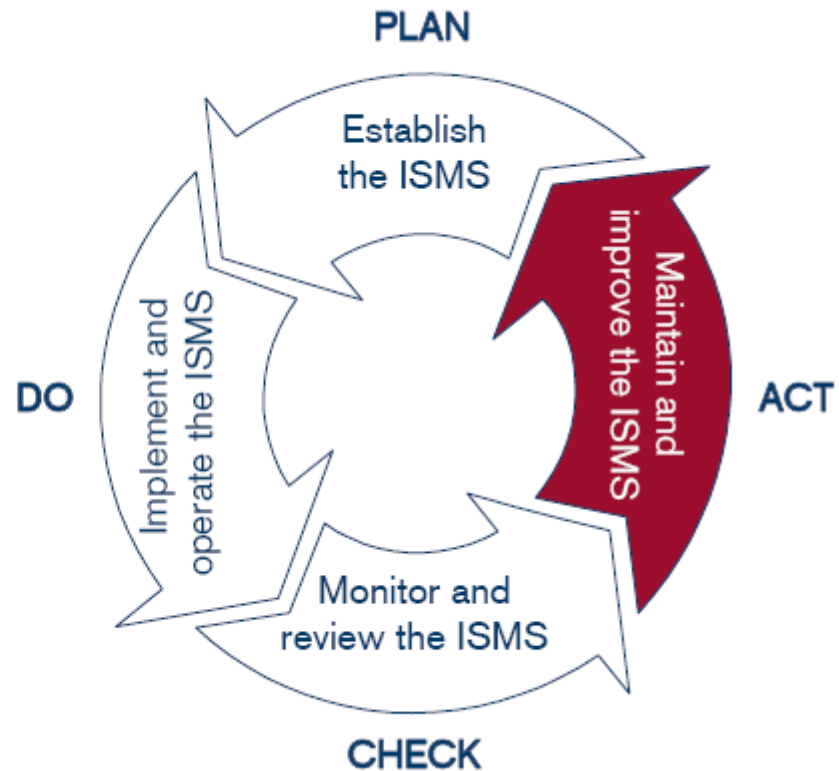
Implement and Operate the ISMS



Monitor and Review the ISMS



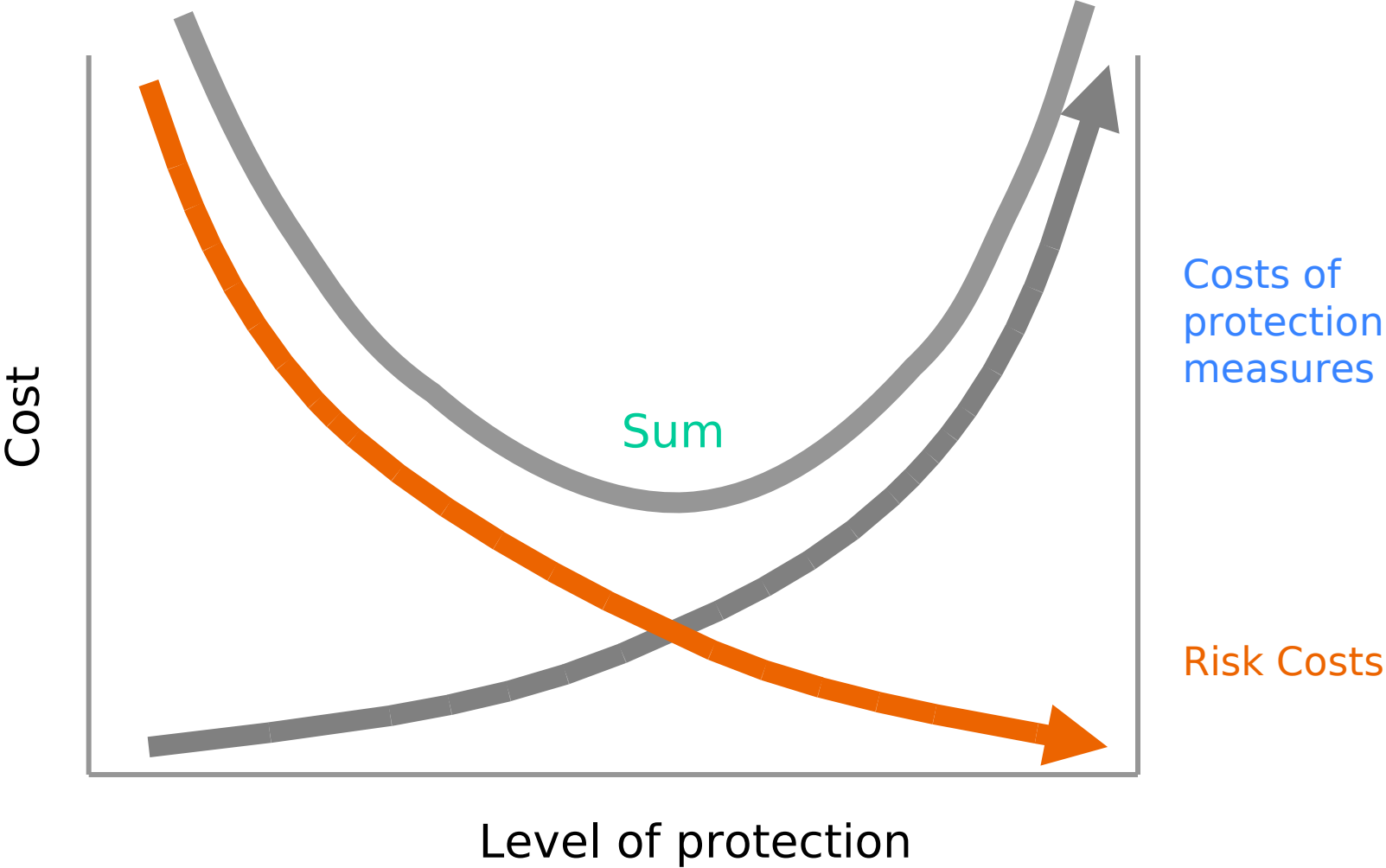
Maintain and Improve the ISMS



ISMS - Key Requirements

- **Documentation** requirements and control of documents and records, including:
ISMS policy, ISMS scope, procedures and processes supporting ISMS, risk assessment methodology and report, risk treatment plan, Statement of Applicability (re. Annex A)
- **Management responsibilities:** commitment, provision of resources and training, management reviews
- Both **management reviews and internal audits** at planned intervals

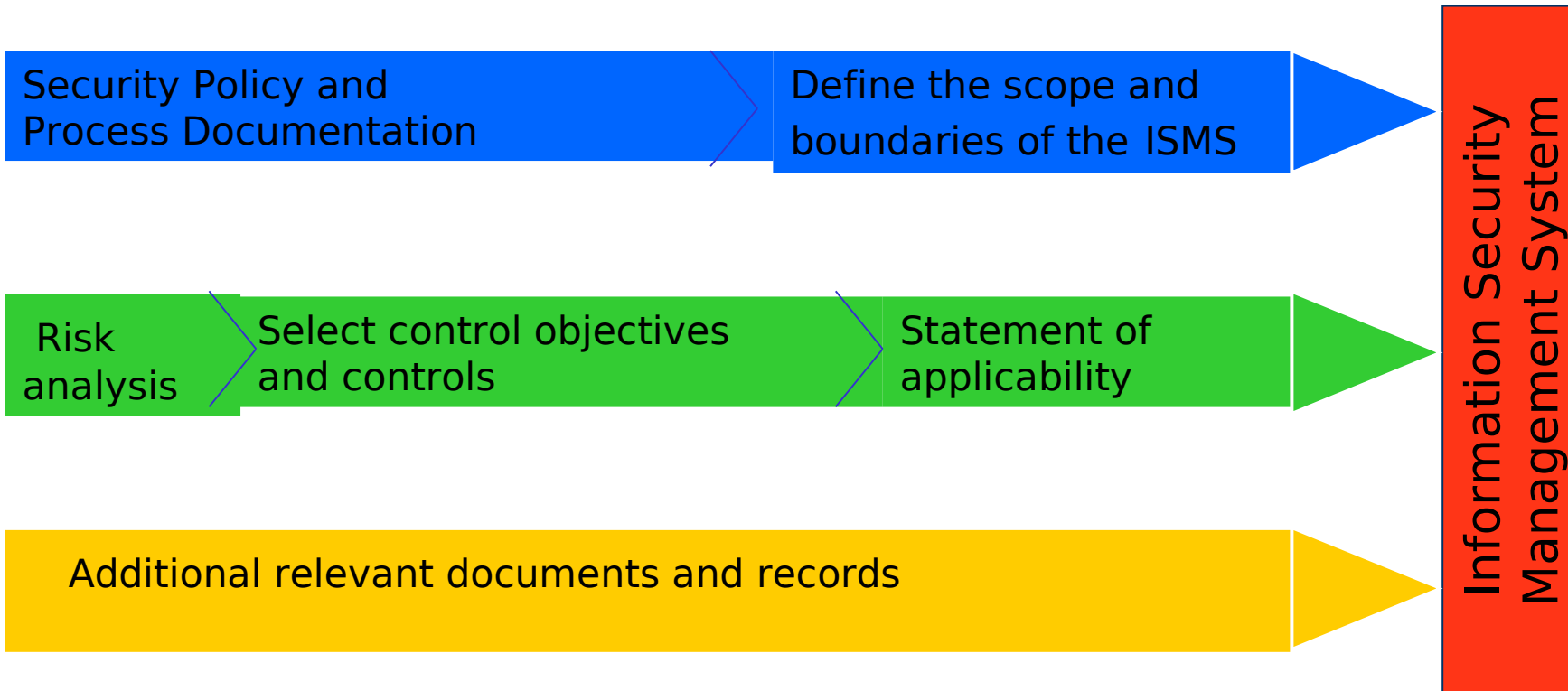
Keep in Mind:



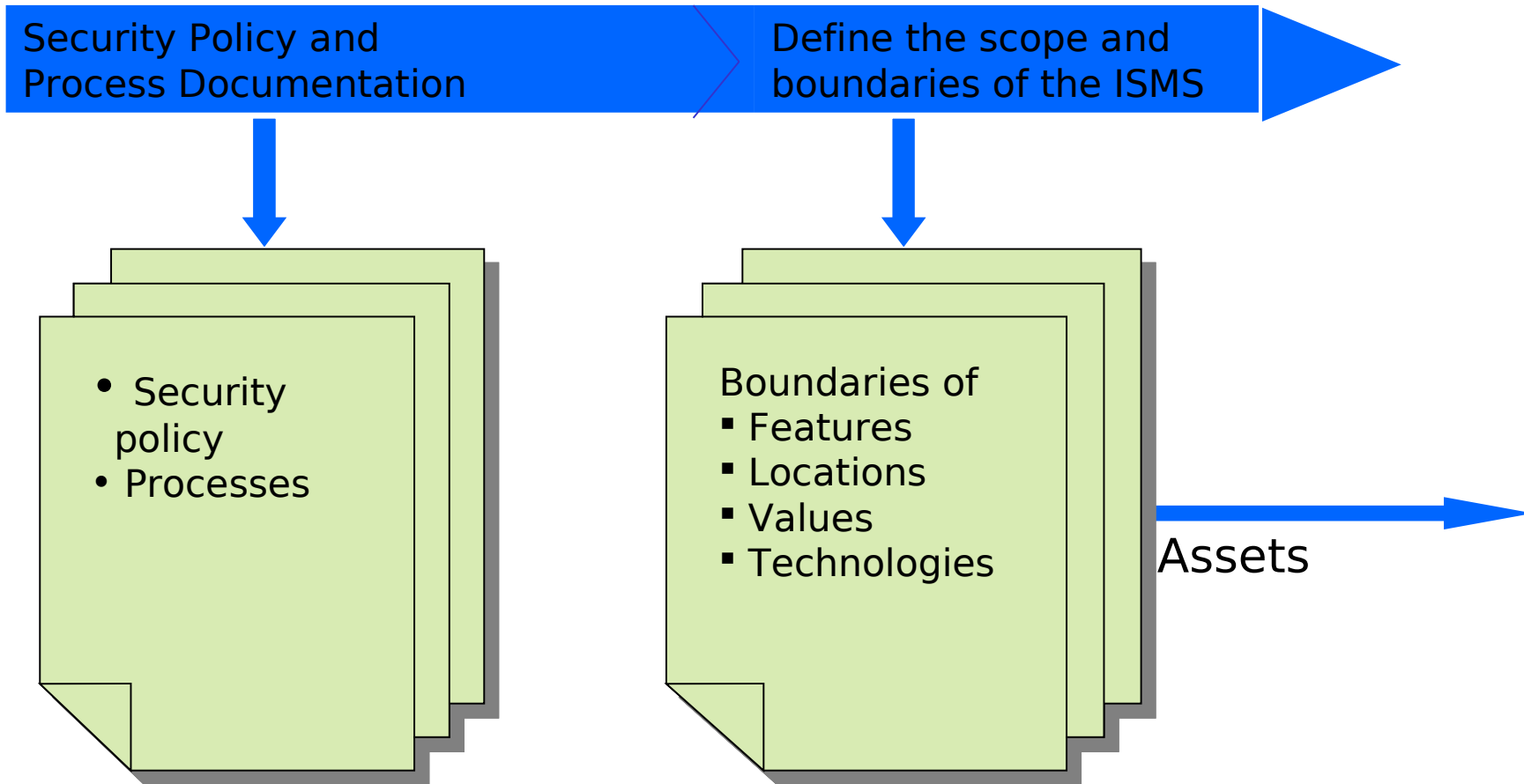
Costs of protection measures

Risk Costs

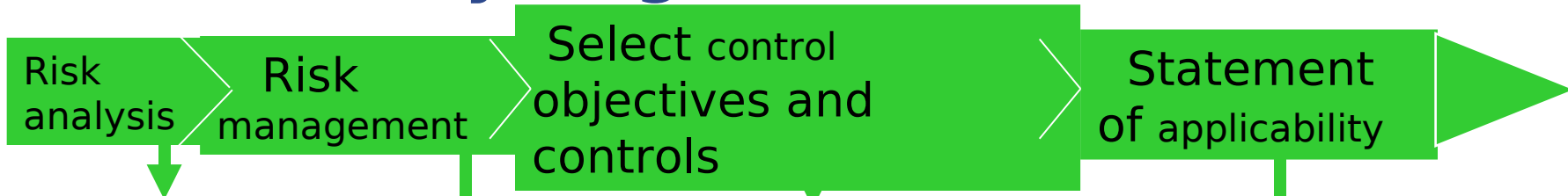
Information Security Management System (ISMS)



Mandatory Regulation for an ISMS (1)



Mandatory Regulation for an ISMS (2)



- Threats
- Nonconformities
- Impact

- Section 4 of ISO 27001:2005
- additional actions

- Procedures
- Required security level

- Selected security objectives and controls
- Reasons for their selection or exclusion

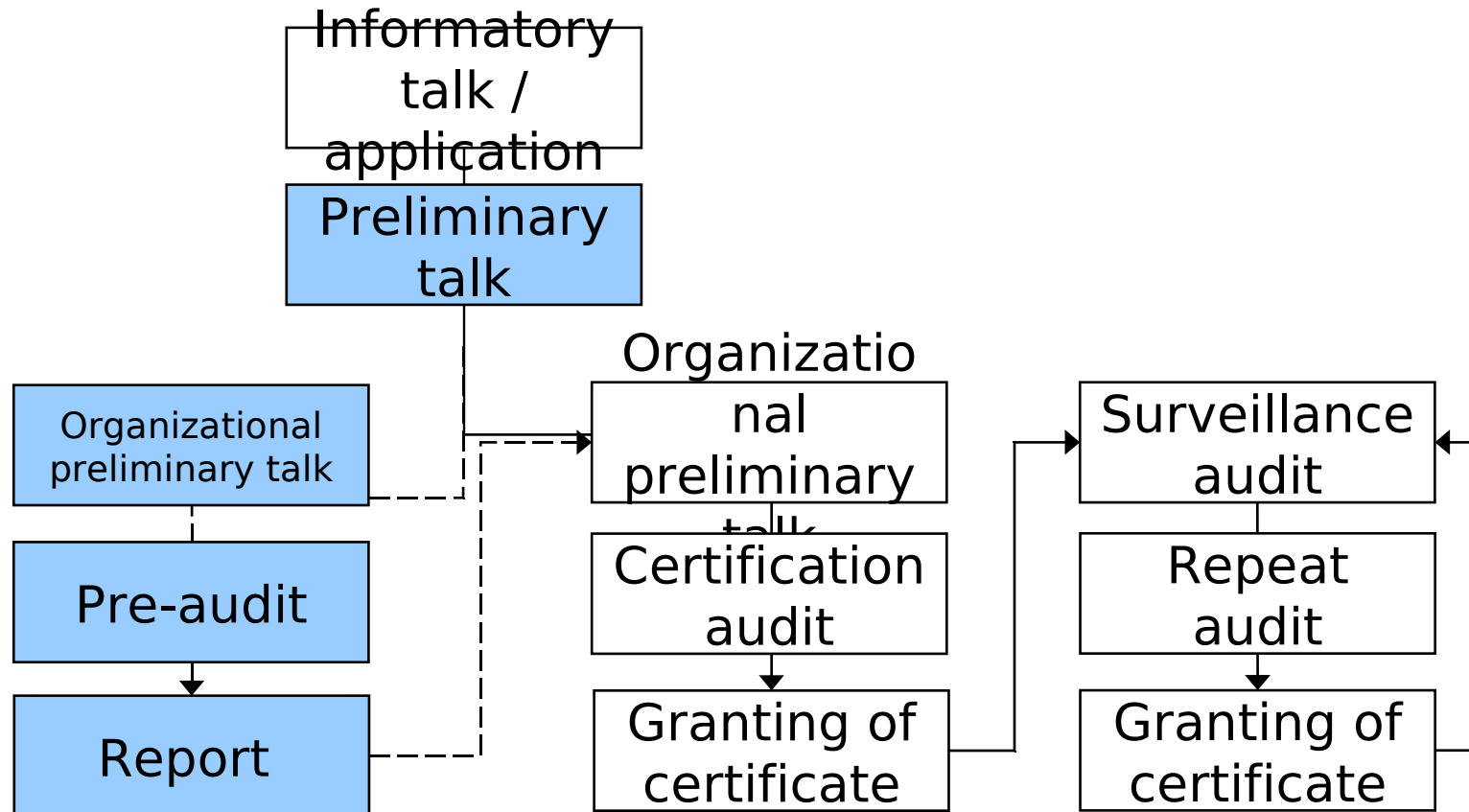
Mandatory Regulation for an ISMS (3)

Additional relevant documents and records

Legal requirements

- contractual agreements
- customer conditions
- etc.

SQS certification procedure



■ Optional, but recommended

Pre-audit (mandatory)

- A pre-audit (pre-assessment) can be carried out optionally
- A pre-audit helps:
 - To guarantee the certification maturity,
 - To identifying and remedying of still available nonconformities
 - For better preparation of employee
 - To guarantee a smoother certification

Organizational preliminary talk (mandatory)

Primary objective: Determination of the certification maturity and identify special auditor skills needed.

2. Examination

- Completeness and practicality of the ISMS documentation,
- Identified Information Security Risks,
- Statement of applicability (SoA).

3. Assessment of the certification maturity and the certification scope

4. Risk-oriented audit planning (Audit Program)

Certification audit (mandatory)

- A ISO 27001 certification audit is like a ISO 9001 certification. Depending on complexity, the audit duration is charged with factor 1.5 to 2.
- For an optimal preparation all relevant documents – like Management System, Information Security Policy, ... - are needed .
- Audit-Tools: SQS ISO 27001:2005 Checklist and Audit Program.
- Audit Report / apply for certification / Certificate printing.
- Assessments at regular intervals: each year to facilitate improvement and ensure that continuing to meet the requirements of ISO 27001 and a re-certification in three years



Reasons to get ISO 27001 certified

- Marketing purpose
- Competitive advantage
- Compliance with regulatory and contractual requirements
- Organizational optimization
- Linking with other management systems like ISO 9001 and ISO 20000



ISO/IEC 27001:2005 Certification

