Information Security Policy

based on the ISO/IEC 27002:2005

→ THE tool for today's (C)ISO ←

Introduction

To protect its assets (information and systems) on a daily basis an organisation has to:

- **organise** its security by documenting the **countermeasures** or controls to **protect** the **confidentiality**, **integrity** and **availability** of the assets, in a security policy,
- with the prime goal to **manage** and **reduce** its **risks**.

Two more definitions

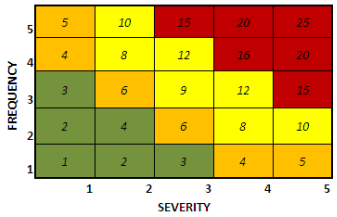
- **Asset** anything that has value to the organization.
- **Control** means of **managing risk**, including **policies**, **procedures**, **guidelines**, **practices** or organizational structures, which can be of administrative, technical, management, or legal nature.
  NOTE: Control is also used as a synonym for safeguard or countermeasure.

Information security policy

- defines the **business rules**, **principles** and standards defining the organisation's approach to managing information security, provides **management direction** and support for information security in accordance with **business requirements** and **relevant laws and regulations**,
- defines **control objectives** and **controls** intended to be implemented to meet the requirements identfied by a **risk assessment**,
- needs **approval** by the **highest level of management**.

beforehand…

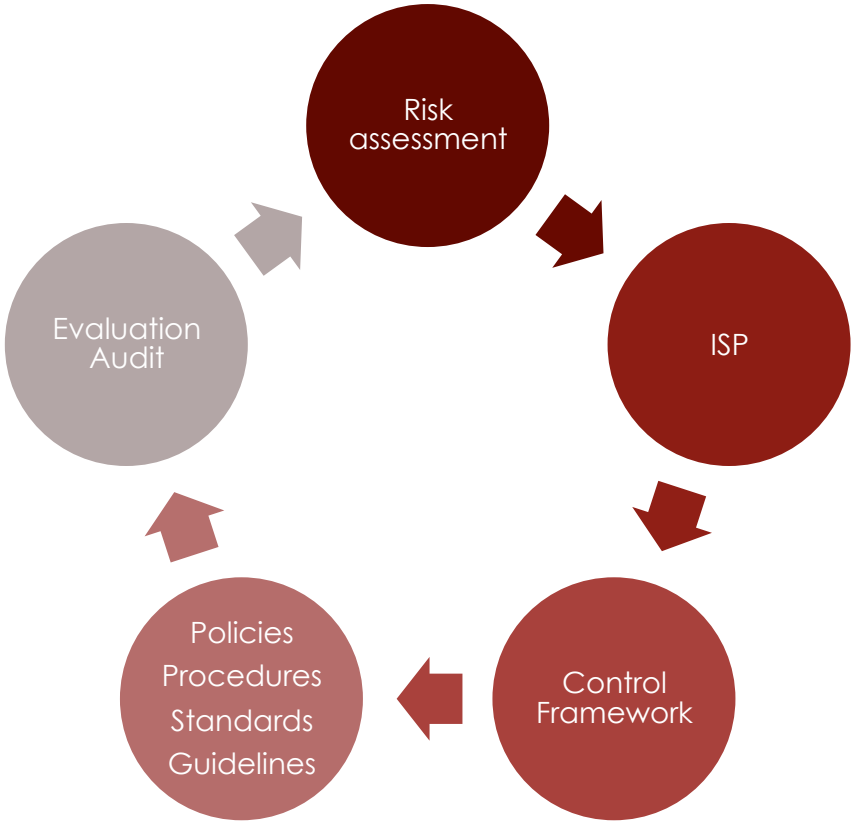
1. One source is derived from assessing risks to the organization :
   - **Risk = Vulnerability * Threat * Impact**
2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.
3. A further source is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations.



even beforehand...

- Before one can identify, quantify, and prioritize risks it is a good practice to identify the organisations **important/critical assets** on which the risks appose (→ *asset management/classification*). Examples are:
  - business critical informations,
  - physical and logical (software...) resources (computers, network equipment...),
  - personnel (most important and critical resources!),
  - image, reputation,
  - know-how, "business" intelligence.

Complete lifecycle



ISO/IEC 27002:2005

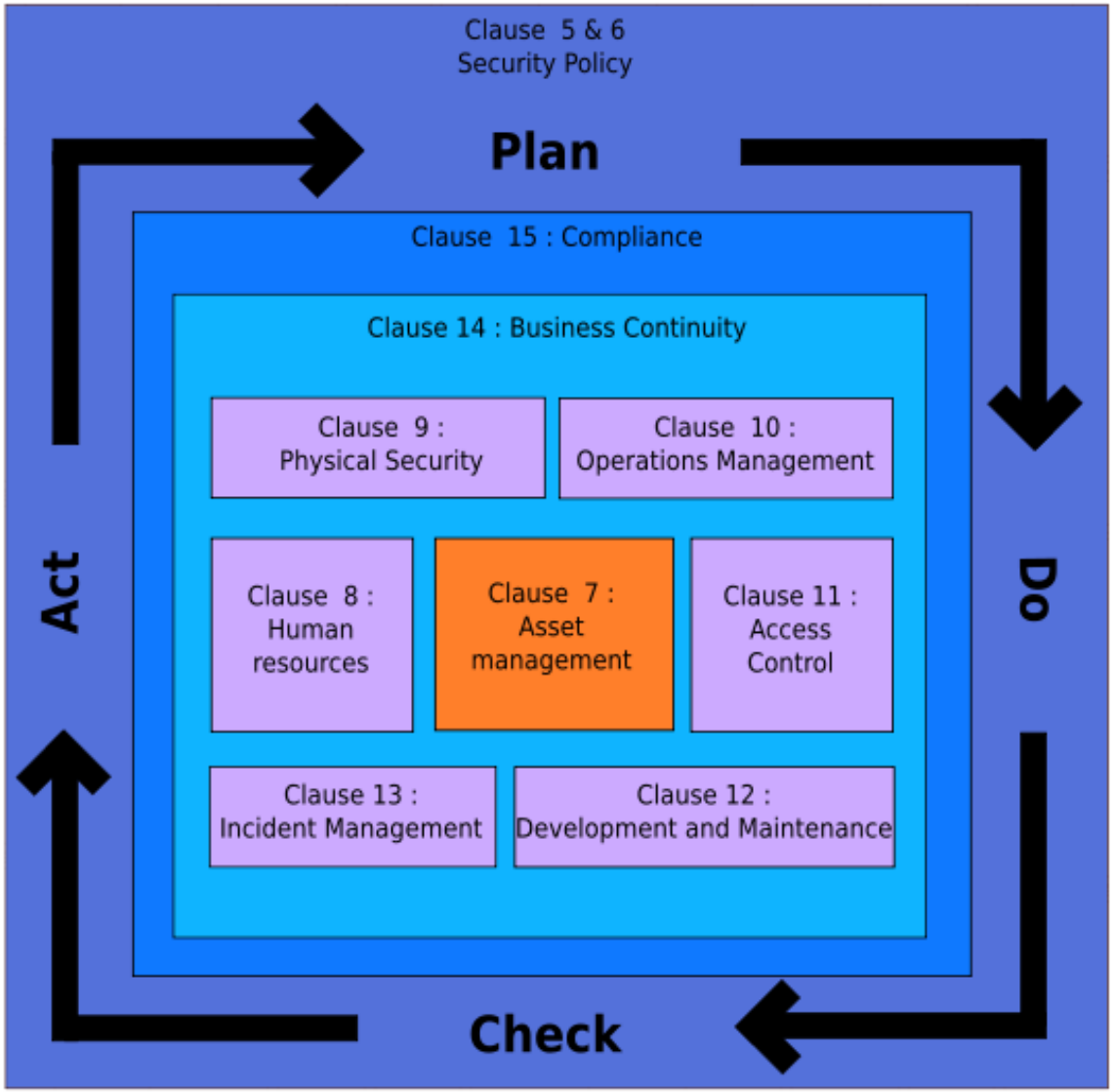
"Code of practice for information security management"
(formerly known as ISO/IEC 17799 and BS7799)

Scope

- "This International Standard establishes **guidelines and general principles** for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management."

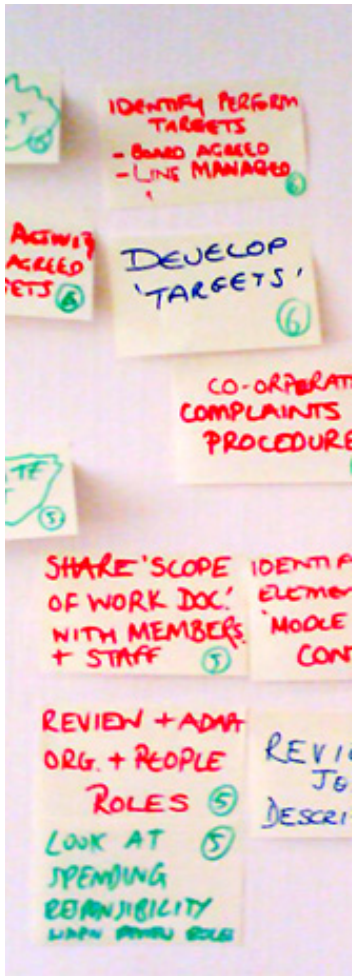
- "The **control objectives** and **controls** of this International Standard are intended to be implemented to meet the **requirements identified by a risk assessment**. This International Standard may serve as a practical guideline for developing organizational **security standards and effective security management practices** and to help build confidence in inter-organizational activities."

Overview


Clause 5 & 6
Security Policy
Plan
Clause 15 : Compliance
Clause 14 : Business Continuity
Clause 9 :
Physical Security
Clause 10 :
Operations Management
Clause 8 :
Human
resources
Clause 7 :
Asset
management
Clause 11 :
Access
Control
Clause 13 :
Incident Management
Clause 12 :
Development and Maintenance
Act
Do
Check

Clause 5
Security Policy

- a **definition** of information security, its overall **objectives and scope** and the importance of security as an enabling mechanism for information sharing;
- a statement of **management intent**, supporting the goals and principles of information security in line with the business strategy and objectives;
- a **framework** for setting control objectives and controls, including the structure of risk assessment and risk management;
- a brief explanation of the security policies, principles, standards, and compliance **requirements** of particular importance to the organization
  - compliance with legislative, regulatory, and contractual requirements;
  - security education, training, and awareness requirements;
  - business continuity management;
  - consequences of information security policy violations;
- a definition of general and specific **responsibilities** for information security management, including reporting information security incidents;
- references to **documentation** which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.
- and get periodic or if significant changes occur **reviews**.



Clause 6
Organising Information Security

- **Management commitment** to information security
- Information security **co-ordination (CISO/RSSI)**
- Allocation of information security **responsibilities** (data owners)
- Confidentiality or non-disclosure **agreements** (reflecting the organisation's needs)
- Contact with **authorities** and special **interest groups**
- **Independent review** of information security
- **External parties** (customers, partners, third parties...)

Clause 7
Asset management

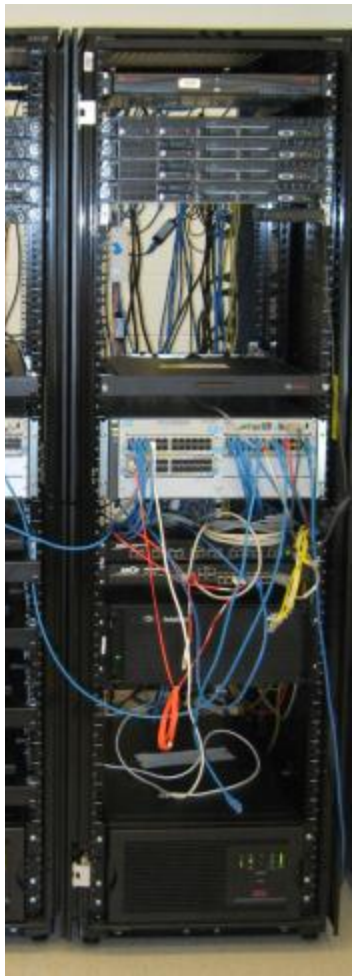
- Responsibility for assets
- Information classication

Clause 8
Human resources

- Roles and responsibilities
- Screening
- Terms and conditions of employment
- Information security awareness, education, and training
- Disciplinary process
- Termination
  - Return of assets
  - Removal of access rights

Clause 9
Physical security

- Physical security perimeter and areas
- Equipment security
  - Security of equipment off-premises
  - Secure disposal or re-use of equipment



Clause 10
Communications & Operations Management

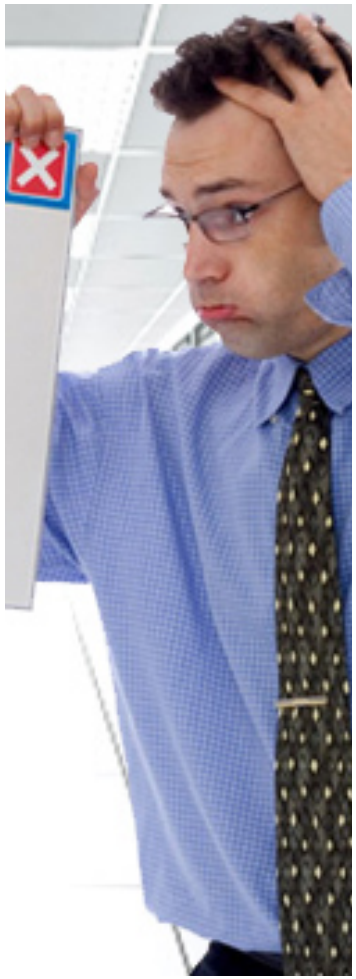
- Change management
- Separation of development, test, and operational facilities
- Third party service delivery management
- Protection against malicious and mobile code
- Back-up
- Network security management
- Management of removable media
- Information exchange policies and procedures
- Electronic messaging
- On-Line Transactions
- Publicly available information
- Monitoring

Clause 11
Access control

- User access management
  - User password management
- Clear desk and clear screen policy
- Network access control
  - User authentication for external connections
  - Segregation in networks
- Operating system access control
  - User identication and authentication
  - Password management system
- Mobile computing and communications

Clause 12
Acquisition, Development and Maintenance

- Security requirements analysis and specification
- Correct processing in applications
- Cryptographic controls
- Security in development and support processes
- Technical Vulnerability Management



Clause 13
Incident management

- Reporting information security events and weaknesses
- Management of information security incidents and improvements

Clause 14
Business continuity

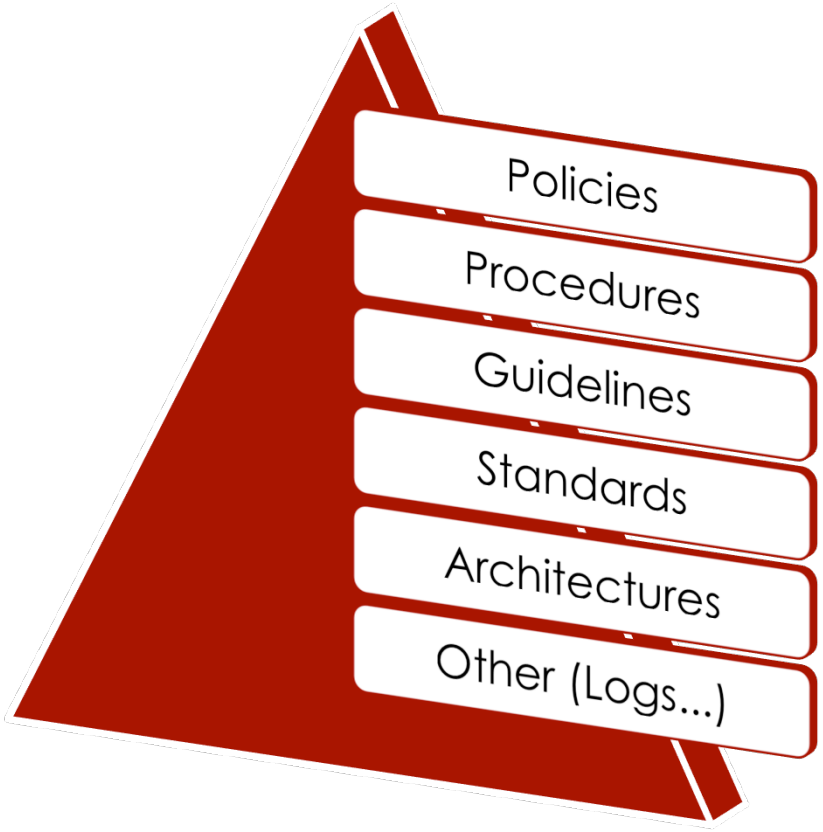
- Developing and implementing continuity plans including informationsecurity
- Testing, maintaining and re-assessing business continuity plans

Clause 15 Compliance

- Compliance with legal requirements
  - Intellectual property rights (IPR)
  - Data protection and privacy of personal information
- Compliance with security policies and standards and technical compliance
- Information systems audit

Control framework

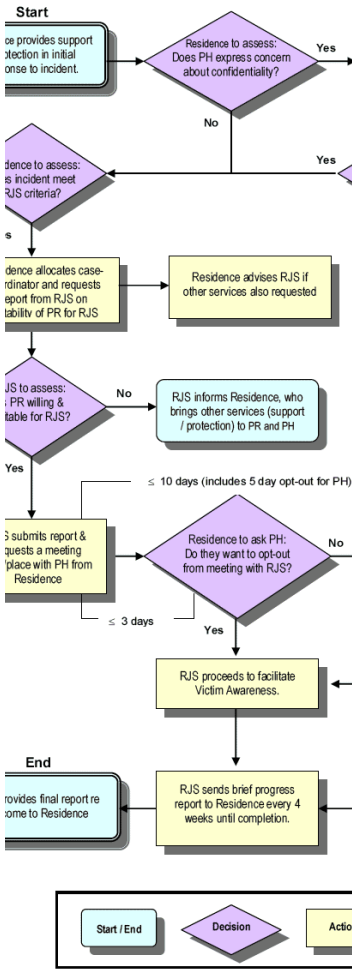
Components


Policies
Procedures
Guidelines
Standards
Architectures
Other (Logs...)

Policies

- These are the **high level** (strategic) documents generally addressing a number of controls (often structured according to the 11 chapters of the 27002), spread across various areas of activity.

Example: Access Control Policy (chap. 11 of 27002)



Procedures

- Procedures further detail aspects of the policy statements describing **realistic processes** covering daily management activities and dening responsabilities.

Example: Remote Access Control Procedure (part of chap. 11.4 of 27002)

Guidelines & Work instructions

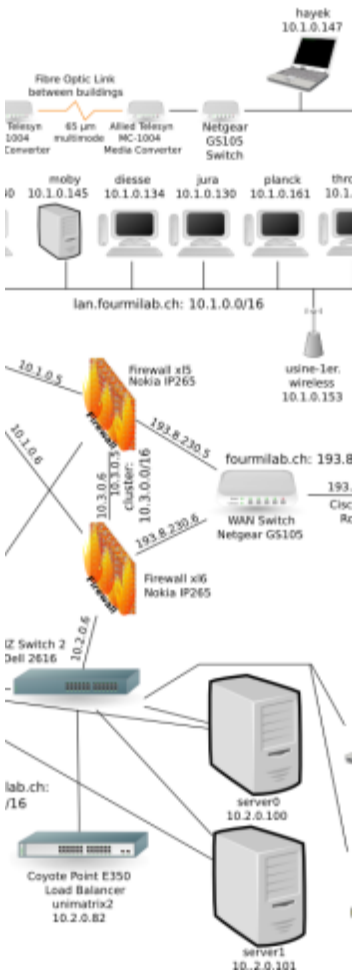
- Sometimes, procedures don't provide enough detail to get the job done. This is particularly true for highly complex tasks that require **detailed step-by-step instructions**.
- Work instructions provide more detail. As a consequence, such instructions are often tightly bound to a particular implementation.
- Guidelines are useful for providing advice in a less formal way - there is no requirement to sign-off guidelines.

Example: Acces Control Instructions for mobile devices

Standards

- Information security standards translate policy/ procedure requirements into **operational instructions**.

Example: List of authorized remote access mechanisms/tools



Architectures

- Most medium and large organisation have a complex IT infrastructure that has evolved over time.
- Each of these systems has an associated security model.
- The goal of a security architecture is to **combine processes and tools** into a framework that mitigates risk.

Example: Remote Acces Architecture

Other Documents

- Examples of the types of documents that the (CI)ISO will be involved with, include:
  - Legal & regulatory documentation, including contracts
  - Security monitoring data and security reports
  - Log files, access control lists (physical and/or logical)
  - Project plans and status reports
  - Financial plans and budgets
  - Vendor-related documentation and licences
  - Documentation owned by other operational units

Good practices

DO's and DON'T's
Lessons Learned

DO's and DON'Ts

- DO:
  - Keep the volume of documentation down to a strict minimum.
  - Check regularly to see that documentation is being used.
  - Ensure that documents are reviewed and approved by all concerned parties.
  - Take time to organise the way documents are stored and retrieved
  - create a well-structured set of directories.
- DON'T:
  - Try to document everything.
  - Document material that is already in user guides (e.g. successive screen shots).
  - Try to have sign-off on everything! Restrict yourself to approving key documents.
  - Use documents to communicate when you should be talking face-to-face.

Lessons learned

- Involve the right people
  - NEVER develop policies in isolation
- Respect the company culture
- Work in iterations, ask for feedback at each step
  - Use milestones to show progress
- Sign-off is critical
- Planning is key
- Publication, diffusion
- Prepare with awareness campaigns

Summary

A global information security process/approach should follow these steps:

1. Risk assessment/analysis
2. Awareness raising campaign
3. (Information) Security Policy
4. ISMS (Information Security Managment System)
5. ISO/IEC 27001 (ISMS) certification