Security Management

03: ISO 2700x
ISO / IEC 27000 Family of Security Standards (3)

Terminology
Requirements
Guidelines for operation and audit of ISMS

27000 Overview

27001 ISMS Requirements
27006 Accreditation Requirements

27002 Code of Practice
27003 Implementation
27004 Measurements and Metrics
27005 Risk Management
27007 Audits

Standards for particular security measures
ISO / IEC 27000 Family of Security Standards (1)

- **[ISO27000]** “Information security management systems—Overview and vocabulary”
  - Provides overview of information security management systems
  - Defines vocabulary and definitions used in the 27000 standard family

- **[ISO27001]** “Information security management systems—Requirements”
  - Specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System.

- **[ISO27002]** “Code of practice for information security management”
  - Provides guidelines for information security management in an organization
  - Contains a list of best-practice security controls.
  - Formerly known as ISO17799.

- **[ISO27003]** “Information security management system implementation guidance”
  - Details process from inception to production of implementation plans of an Information Security Management System specification and design.
ISO / IEC 27000 Family of Security Standards (2)

- **[ISO27004] “Information security management—Measurement”**
  - Provides guidance to help organizations measure and report on the effectiveness of their Information Security Management System processes and controls.

- **[ISO27005] “Information security risk management”**
  - Provides guidelines on the information security risk management process.
  - It supersedes ISO13335-3/4

- **[ISO27006] “Requirements for bodies providing audit and certification of information security management systems”**
  - Specifies requirements and provides guidance for these bodies.

- **[ISO 27007] “Auditing Guidelines“**
ISO 27000

- Short document that summarizes the 27000 family of standards
- Gives an overview on 27000 family and classifies all respective standards
- Refers to OECD Guidelines for the Security of Information Systems and Networks
- Contains basic terms and definitions for the areas:
  - Information security (e.g., confidentiality)
  - Management (e.g., effectivity)
  - Security risks (e.g., vulnerability)
  - Auditing (e.g., Audits)
  - Documentation (e.g., security policy)
Evolution of BS 7799

Code of practice

- BS 7799-1
- ISO 17799:2000
- ISO 17799:2005
- ISO 27002:2007
- ISO 27002:2013

ISMS specification

- BS 7799-2
- BS 7799-2:2002
- ISO 27001:2005
- ISO 27001:2013
ISO 27001

- **ISMS (Information Security Management System)**
  - Standard based on BS 7799-2
  - Describes the requirements towards an ISMS on the basis of a process-based approach
  - Is, exactly as ISO 9001, a management system standard
  - Basis for certification
  - Generic requirements, no technical details

- **Definition: ISMS**
  - „that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security“

**NOTE:** The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
Deming Circle (PDCA) for ISMS

Plan
- design

Do
- implement

Check
- monitor

Act
- maintain and improve

Removed from ISO 27001 standard in version 2013 to allow for more flexibility in choosing method for continual improvement.
ISO 27002

- Information technology — Security techniques — Code of practice for information security management
  - »Guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization«
  - International »Code of practice« for managing information security

- Volume of version 2013
  - 90 pages, 14 sections (management areas) and 114 management tasks (Controls)

- Continuous Update
  - No fixed cycles defined, but planned for
  - Not absolutely necessary, as generic formulation
ISO 27002 - Risk Assessment and Treatment

- Defines basic requirements;
  Refers to ISO/IEC TR 13335-3 for exemplary methods

- Requirements for the assessment of security risks
  - Systematic approach for assessment of size of risks
  - Process for criteria-based comparison of risks
  - Periodic repetition
  - Well-defined area/scope

- Requirements for treating security risks
  - Definition of criteria for accepting risks
  - Individual decision on risk treatment for specific risk
    - Avoidance
    - Reduction
    - Acceptance
    - Transfer
  - If necessary implementation of control(s)

Schaumüller-Bichl 1992
## Comparison of different Versions of ISO 27002

<table>
<thead>
<tr>
<th></th>
<th><strong>Version 2000</strong></th>
<th><strong>Version 2005</strong></th>
<th><strong>Version 2013</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Classification &amp; Control</td>
<td>Asset Management</td>
<td>Human Resources Security</td>
<td>Human Resources Security</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>Human Resources Security</td>
<td>Asset Management</td>
<td>Asset Management</td>
</tr>
<tr>
<td>Physical &amp; Environmental Security</td>
<td>Physical &amp; Environmental Security</td>
<td>Access Control</td>
<td>Access Control</td>
</tr>
<tr>
<td>Communications &amp; Operations Management</td>
<td>Communications &amp; Operations Management</td>
<td>Cryptography</td>
<td>Cryptography</td>
</tr>
<tr>
<td>Access Control</td>
<td>Access Control</td>
<td>Access Control</td>
<td>Access Control</td>
</tr>
<tr>
<td>Systems Development &amp; Maintenance</td>
<td>Information Systems, Acquisition, Development and Maintenance</td>
<td>Information Systems Acquisition, Development, Maintenance</td>
<td>Information Systems Acquisition, Development, Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Supplier Relationships</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Information Security Incident Management</td>
</tr>
<tr>
<td>Compliance</td>
<td>Compliance</td>
<td>Compliance</td>
<td>Compliance</td>
</tr>
</tbody>
</table>
ISO 27002 - Structure of Controls

- Controls = Measures

Control

+ Implementation Guidance

+ Other Information

What?

How?
Example of a Control

Information security awareness, education and training

Control
All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Implementation guidance
An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

An information security awareness programme should be established in line with the organization’s information security policies and relevant procedures, taking into consideration the organization’s information to be protected and the controls that have been implemented to protect the information. The awareness programme should include a number of awareness-raising activities such as campaigns (e.g. an “information security day”) and issuing booklets or newsletters. [...]

Other information
When composing an awareness programme, it is important not only to focus on the ‘what’ and ‘how’, but also the ‘why’. It is important that employees understand the aim of information security and the potential impact, positive and negative, on the organization of their own behaviour. Awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education and training activities should be suitable and relevant to the individual’s roles, responsibilities and skills. An assessment of the employees’ understanding could be conducted at the end of an awareness, education and training course to test knowledge transfer.

8.2.2 in ISO27002:2005
7.2.2 in ISO27002:2013
Security policy

Defines fundamental position of the organization regarding information security

- Creation of a policy document
  - Defining information security from the perspective of the organization
  - Goals and principles regarding information security
  - Allocation of responsibilities for information security
  - References to documents that are used for implementation of policy

- Frequent review and adaption towards new circumstances
Organization of information security

- Internal Organization
  - Management framework for implementing information security within organization
  - Controls
    - Roles and responsibilities for information security
    - Segregation of duties
    - Contact with authorities
    - Contact with special interest groups
    - Information security within the project management

- Mobile devices and teleworking
  - Originally from Access Control (until 2005)
    - Mobile device policy
    - Teleworking
Human Resources Security

- Prior to employment
  - Controls
    - Define and document tasks and responsibilities
    - Security check of employees (screening)
      - Check correctness of references, CV, qualification, identity, details
    - Terms and conditions of employment
      - Clause in employment contract that point to adherence of security measures
Human Resources Security

- **During employment**
  - Management responsibilities
  - Information security awareness, education, and training
  - Disciplinary process

- **Termination and change of employment**
  - Define responsibilities for termination
  - Return of company equipment / assets
  - Canceling access permissions

  e.g., password rules
Asset Management (1)

- **Responsibilities for assets**
  - **Inventory of assets**
    - **Information assets**
      - Databases, data, system documentation, training material, emergency plans, archived data
    - **Software assets**
      - Application and system software, development tools, utilities
    - **Physical assets**
      - Computer technology (incl. Hardware), communication technology (router, fax, telephone system, ...), storage media, power supply, air conditioner, furniture, rooms
    - **Services**
      - Communication and data processing services, general facilities (e.g., heating, light, power, air conditioning)
    - **Persons**
      - And their qualifications, skills, and experience
    - **Intangible assets**
      - E.g., good reputation and image of company
Asset Management (2)

- **Responsibilities for assets (cont.)**
  - **Ownership for assets**
    - All information and assets in connection with information processing facilities should be owned by a particular part of organization.
  - **Acceptable use of assets**
    - Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented, and implemented.
  - **Return of assets**
    - All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract, or agreement.
Asset Management (3)

- **Information classification**
  - Identification of necessity and importance of information
  - Controls:
    - Determination of necessary protection level
      - From sensitive/critical ······· unimportant/I don’t care
    - No concrete guidelines for classification
    - Taking into account that protection requirements change over time
      - E.g., information on a new product
    - »Over-classification« can cause unnecessary costs

- **Media handling**
  - Deletion of media that is not used anymore
  - Authorization for deletion and disposal
  - Storage in a safe, secure environment, ...
Access control

- **Business requirements of access control**
  - Access control policy

- **User access management**
  - User registration and de-registration
  - User access provisioning
  - Management of privileged access rights
  - Management of secret authentication information of users
  - Review of user access rights
  - Removal or adjustment of access rights

- **User responsibilities**
  - Use of secret authentication information
  - Behavior when leaving device

- **System and application access control**
  - Networks
  - Operating systems
  - Devices
Cryptography

- Controls for the right and effective usage of cryptography to protect confidentiality, integrity of data and accountability for entities

- 2 Controls
  - Policy on the use of cryptographic protocols
  - Key management
Physical and environmental security

Secure areas

- **Controls**
  - Physical security perimeter
    - Walls, doors, alarm systems, sensors
  - Physical entry controls
    - Creating visiting areas, Badges
  - Securing offices, rooms, and facilities
    - Audit-Trails of all security relevant events
  - Protecting against external and environmental threats
    - Equipment for fire fighting, Backups
  - Working in secure areas
    - Confidentiality of their existence and tasks
  - Delivery and loading areas
    - Locks, registration of incoming and outgoing commodities

\[e.g., \text{physical protection}\]
Physical Security: Basic Functions

- **Observing attacks (eavesdropping):**
  - **Shielding** (electromagnetic emanation, energy consumption – independent from the secrets that need to be protected)

- **Modification attacks:**
  - Detecting, assessing, delaying and if necessary deleting secret information

Diagram:
- Delaying (e.g., tough material)
- Detection (e.g., shock and pressure sensors)
- Shielding, assessing
- Delete secrets
Physical Security: Basic Functions

- Security Modul

- Fire protection
- Access Control
- Air conditioning
- Independent power supply

Picture: www.lampertz.de
Physical and environmental security (1)

Security of equipment: To prevent loss, damage, theft, or compromise of assets and interruption to operation of organization

- **Controls**
  - General recommendations
    - »Do not eat in front of a computer«
  - Supporting utilities
    - UPS, emergency power
  - Cabling security
    - Only patch plug sockets that are actually needed
    - Redundant wiring
    - Use glass fiber
  - Equipment maintenance
    - Sensible data on storage devices, protection from data loss
  - Removal of assets
    - Equipment, information or software should not be taken off-site without prior authorization
Physical and environmental security (2)

- **Controls for security of equipment (cont.)**
  - Security of equipment and assets off-premises
    - Taking into account different risks of working outside the organization’s premises
  - Secure disposal or re-use of equipment
    - All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
  - Unattended user equipment
    - Users should ensure that unattended equipment has appropriate protection
  - Clear desk and clear screen policy
    - Clear desk: For papers, removable storage media
    - Clear screen: for information processing facilities
Operations Security (1)

Operational procedures and responsibilities

- Controls
  - Documented operating procedures (processes)
  - Change management
  - Capacity management
    - Deletion of obsolete data, optimization of applications, systems, batch processes, schedules
  - Separation of development, testing, and operational environments
    - Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.
Operations Security (2)

- **Protection from Malware**
  - One control with numerous guidance;
  - Examples:
    - Antivirus scanner for files, E-Mails
    - Update management
    - Ensuring that warnings are correct

- **Backup**
  - Define necessary backup level
  - Documented restoration procedures
  - Frequent check of backup media
  - Physical protection of backup media
  - Encrypt backups if required

---

**e.g., Hoaxes**

http://www.hoax-info.de/
http://hoaxmap.org/
Hoaxes

- Propagation: via human misconception and error
- Hoax-List: http://www.hoax-info.de/

Von: Doris Külper
Datum: 04.03.2004 11:25:12
Betreff: WICHTIGE INFO

Handy Fangnummern im Umlauf

Für alle zur Info

Wenn auf dem Handydisplay die Mitteilung "Anruf in Abwesenheit" und dann die Nummer: +49137799090269 oder +4917232233333 erscheint, nicht zurückrufen. Es handelt sich hierbei um eine Fangnummer, die den Anruf bis zu einer Stunde und länger hält.

Der Anrufer selbst hat keine Möglichkeit, den Anruf zu beenden.

Bitte geben Sie diese Nummer jedem weiter, den Sie kennen, damit böse Überraschungen im Vorfeld schon vermieden werden.

Mit freundlichem Gruss

Doris Külper
Staatsanwaltschaft Hamburg
Operations Security (3)

- **Logging und Monitoring**
  - Audit protocols
  - Event logging
  - Protection of log information
  - Administrator and operator logs
  - Clock synchronization

- **Control of operational software**
  - Installation of software on operational systems
  - Update management
  - Rollback

- **Technical vulnerability management**
  - Management of technical vulnerabilities
  - Restrictions on software installations

- **Information systems audit considerations**
  - Information systems audit controls
Communications security

- **Network security management**
  - Network controls (/security measures)
  - Security of network services
  - Segregation in networks
  - Security measures to ensure confidentiality and integrity
  - Encryption during transmission
  - Adequate logging and monitoring

- **Exchange of information**
  - Information transfer policies and procedures
  - Agreements on information transfer
  - Transport of storage devices
  - Electronic messaging
  - Confidentiality or non-disclosure agreements
System Acquisition, Development and Maintenance

- **Controls**
  1. Defining security requirements of information systems upon their design
  2. Security in development and support process
     - Protection of system files (e.g., used libraries)
  3. Test data

- **Addresses development of secure systems**
  - Affects especially organizations that develop SW on their own
  - Structured development process

**Show:**
Security is a cross-sectional topic!
Supplier Relationships

To ensure protection of the organization’s assets that are accessible by suppliers and other external entities

- **Controls**
  - Identify risks in combination with external suppliers
  - Addressing security when interacting with customers
  - Addressing security in agreements with third parties

- **Examples**
  - Customers
  - Outsourcing, hardware- and software support
  - Cleaning workers
  - Trainees, student workers, contract workers / temporary staff
  - Consultants
Information Security Incident Management

- Management of information security incidents and improvements
  - Management responsibilities and procedures
  - Reporting security events and weaknesses
    - Reporting mechanism: e.g., forms
    - Criteria for correct behavior
  - Assessment of and decision on security events
  - Response to security incidents
  - Learning from security incidents
  - Collection of evidence
Business continuity management

Protection from the disruption of business activities: to protect critical business processes from the impact of bigger failures/disturbances of information systems or disasters and to ensure timely restoration

- Controls
  - Process for information security continuity
  - Redundancies
    - Addresses availability
Compliance

- Compliance with legal and contractual requirements
  - Copyright, software law
  - Privacy and data protection
  - Misuse, criminal prosecution, ...

- Review if implemented controls for information security map with security policy (security reviews)
  - If necessary: changes
For which areas is ISO 27002 .............. suitable?

- Types of organizations / companies
  - Server provider
  - Service provider
  - Organizations as users
  - Software companies
  - ISPs

- Within the organization / company
  - Company management
  - Project management
  - IT management
  - IT Security Officer
  - Administrators
  - Auditors
Rating of ISO 27002 (1)

- **Intended audience**
  - Organizations and authorities of all sizes
    - However, more suitable for large organizations
    - High effort for small organizations
  - Not suitable for private users

- **Alternative:**
  - IT baseline protection of the BSI (IT-Grundschutz)
Rating of ISO 27002 (2)

- **System and product types**
  - Created for assessing a socio-technological overall system
    - Top-Down approach for establishing information security
    - Mainly generic security measures (controls)
  - Less suitable for the certification of single products
  - Good: Embedding of products in an overall system

- **Problem:**
  - When disassembling the system in subsystems there are no suitable recommendations for measures that support the secure assembling of all subsystems
Rating of ISO 27002 (3)

- **Usage**
  1. Usage as reference book for questions regarding single (high-level) measures/controls
  3. Setup of an ISMS that can be certified

- 2. and 3. require the systematic and complete implementation of recommended controls
Rating of ISO 27002 (4)

- **Achievable security level**
  - Comprehensive catalogue of controls
  - Defines mainly standard security measures
  - High security requires further measures
  - However: Management of high security is supported by management approach

- **Implementation effort**
  - Depends on degree of organization of company
  - High degree of organization – less effort
  - Implementation of controls can be supported by tools
References


