INFORMATION SECURITY MANAGEMENT SYSTEMS

(ISMS)

Study supports

Ing. Václav Štverka

Ostrava 2015
Title: Information Security Management Systems
Author: Ing. Václav Štverka, CISA, CISM
Edition: first, 2015
No. of pages: 61

Academic materials for the Economics and Management of Industrial Systems study programme at the Faculty of Metallurgy and Materials Engineering.

Proofreading has not been performed.

Execution: VŠB – Technical University of Ostrava
STUDY INSTRUCTIONS

Information Security Management Systems

You are obtaining the integrated overview (Syllabus) of the Subject „Information Security Management Systems (ISMS) for both undergraduate or graduate levels.

Pre-requisite

The Subject has not any pre-requisites.

Subject aims expressed by acquired skills and competences

- The subject is coming out from the requirements of the information security management system and gives the basic survey of the specifications which are necessary to fulfil for successful implementation
- It gives the theoretic basement of the ISMS requirements, its understanding and application in to the practice
- It works with the requirements of the standards like as series of 2700x
- The subject takes into account the procedures and practices for ISMS internal audits according to the ISO/IEC 27001
- The subject is to give overall overview about requirements and range of the ISMS implementation project according to the ISO/IEC 27001 standard

Undergraduates should be able:
- to hold a position of the information security management system manager (ISMS manager),
- to execute ISMS internal audits according to the ISO/IEC 27001,
- to implement the information security management system in any organization.

Who is the course intended for

The subject is a part of Quality Management magister study but is suitable also for the other applicants from the other field of study.

The subject is focused on the basic information about implementation and maintenance of the information security management system

The Syllabus is divided in to the individual chapters which correspond logical division of the study matter but the extend is not the same.

The assumption time can be quite different and thus the every chapter is divided in to the subsections.

Method of communication with the educator

This matter is presented to students within the frame of their lectures and practical exercises, where they practically learn the topic discussed during the theoretical lectures.
STRUCTURE OF THE CHAPTERS

Study time

The time necessary to study the subject matter is given at the beginning of the chapter. The time is approximate and can serve as a rough guide for the study layout of the entire subject. The time may seem too long to some people or, on the contrary, too short to other ones. There are students who have never encountered this issue and, on the other hand, those who already have extensive experience in this field.

Objective

Immediately after, there are objectives given for you to achieve after reading this chapter - concrete skills, knowledge.

Explication

The following part is the actual presentation of the studied subject matter, the introduction of new terms, their explanations, and all is accompanied by pictures, tables, solved examples, and links to animations.

Time to think

You will encounter questions and problems within the study of the chapters that should be thought over for the sake of mastering the subject matter. Correct solutions follow the questions, so do not continue reading until you have thought everything over well.

Example from practice, Example to solve

Use practical examples of the application of the presented theoretical knowledge to better understand the discussed subject matter.

Animations, Video

The presentation is accompanied by animations to increase the plasticity of the studied subject matter and videos to illustrate and extend the knowledge.

Summary of terms
The main terms you should learn are repeated at the end of the chapter. If you still do not understand any of the terms, go back to them again.

Questions

There are several theoretical questions to verify that you have fully and well mastered the subject matter of the chapter.

References as a sources for further study

There is a list of the used reference sources, from which you can draw additional information on the issue in question, at the very end of the chapter.

Solution key

You will find the solution key to the tasks and answers to the questions at the end of the study supports.

The author of this educational material wishes you a successful and pleasant study using this textbook.

Ing. Václav ŠTVERKA, CISA, CISM
# CONTENTS

STUDY INSTRUCTIONS ......................................................... 3

STRUCTURE OF THE CHAPTERS ........................................... 4

CONTENTS ................................................................. 6

1 INTRODUCTION TO THE COURSE - INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) ....................................................... 8
   1.1 INTRODUCTION TO THE COURSE Management system standards ..................................................... 8

2 ISMS - STANDARD AND REGULATORY FRAMEWORK............. 11
   2.1 ISMS BASIC PRINCIPLES .............................................. 11
   2.2 ISMS STANDARDS ..................................................... 13

3 FUNDAMENTAL DEFINITIONS AND PRINCIPLES IN INFORMATION SECURITY (ISMS) .......................................................... 17
   3.1 Fundamental definitions .............................................. 17

4 INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) ...... 23
   4.1 Why implement ISMS? .................................................. 23

5 STANDARDS FOR ISMS IMPLEMENTATION ......................... 26
   5.1 International standards for ISMS .................................... 26

6 INFORMATION SECURITY RISK MANAGEMENT ..................... 28
   6.1 Risk management definitions ....................................... 28
   6.2 Risk management process ........................................... 28
   6.3 Information security risk analysis .................................. 29
   6.4 PC and SW tools ..................................................... 30

7 IMPLEMENTATION ISMS ACCORDING TO ISO/IEC 27001 ........ 32
   7.1 14 STEPS TO ISMS IMPLEMENTATION ................................ 32
       7.1.1 Management decision, leadership and approval of the ISMS project ........................................ 33
       7.1.2 Define the context, scope and boundaries of the ISMS ......................................................... 33
       7.1.3 Definition of Security policy (ISMS Policy) and ISMS objectives ........................................... 33
       7.1.4 Risk management approach .................................... 34
       7.1.5 Definition of the document management process ................................................................. 35
       7.1.6 Establishment of Risk treatment Plan ................................................................. 35
       7.1.7 Design of security controls and drafting of specific policies and procedures ........................... 35
       7.1.8 Implementation of selected security controls ................................................................. 36
       7.1.9 Training and awareness plan ..................................... 36
       7.1.10 Incident Management ............................................ 37
       7.1.11 Operations Management ........................................ 37
       7.1.12 Internal audit process ........................................... 37
       7.1.13 Management Review ............................................ 38
       7.1.14 Certification ..................................................... 38
8 ISO/IEC 27001 – CERTIFICATION PROCESS .......................... 51
  8.1 Certification ISMS according to ISO/IEC 27001 ........................................... 51
9 IT TECHNOLOGY MINIMUM ............................................................. 55
10 RECOMMENDED REFERENCES .................................................... 57
1 INTRODUCTION TO THE COURSE - INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Study time

1 hour

Objective

The main objective of this chapter is to acquire the knowledge of ISO standards structure

Explication

1.1 INTRODUCTION TO THE COURSE MANAGEMENT SYSTEM STANDARDS

- ISO 9001 – Quality
- ISO 14001 – Environment
- ISO 18001 – Health and Safety at work
- ISO 20000 – IT Services
- ISO 22000 – Food Safety
- ISO 22301 – Business continuity
- ISO 27001 – Information security
- ISO 28000 – Supply Chain Security

Since 1947 ISO has published over 19 000 international standards. ISO publishes standards related to traditional activities such as agriculture and construction, media devices and the most recent development in information technologies, such as the digital coding of audiovisual signals for multimedia applications.
Common structure of ISO standards

<table>
<thead>
<tr>
<th>Requirements</th>
<th>ISO 9001</th>
<th>ISO 14001</th>
<th>ISO 20000</th>
<th>ISO 22301</th>
<th>ISO 27001</th>
<th>ISO 28000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectives of the management system</td>
<td>5.4.1</td>
<td>4.3.3</td>
<td>4.5.2</td>
<td>6.2</td>
<td>4.2.1</td>
<td>4.3.3</td>
</tr>
<tr>
<td>Policy of the management system</td>
<td>5.3</td>
<td>4.2</td>
<td>4.1.2</td>
<td>5.3</td>
<td>4.2.1</td>
<td>4.2</td>
</tr>
<tr>
<td>Management continuity</td>
<td>5.1</td>
<td>4.4.1</td>
<td>4.1.0</td>
<td>5.2</td>
<td>5.0</td>
<td>4.4.1</td>
</tr>
<tr>
<td>Documentation requirements</td>
<td>4.2</td>
<td>4.4.0</td>
<td>4.3</td>
<td>7.5</td>
<td>4.3</td>
<td>4.4.4</td>
</tr>
<tr>
<td>Internal audit</td>
<td>8.2.2</td>
<td>4.5.5</td>
<td>4.5.4.2</td>
<td>9.2</td>
<td>8.0</td>
<td>4.5.5</td>
</tr>
<tr>
<td>Continual improvement</td>
<td>8.5.1</td>
<td>4.5.3</td>
<td>4.5.5</td>
<td>10.0</td>
<td>8.0</td>
<td>4.6</td>
</tr>
<tr>
<td>Management review</td>
<td>5.6</td>
<td>4.6</td>
<td>4.5.4.3</td>
<td>9.3</td>
<td>7.0</td>
<td>4.6</td>
</tr>
</tbody>
</table>

Obr. 1. Common structure of ISO standards

Integrated Management System

More and more organizations have to manage several compliance frameworks simultaneously. To simplify the work, to avoid conflicts and to reduce duplication of documents, it is recommended to implement an integrated management system. An integrated management system (IMS) is a management system which integrates all components of a business into one coherent system so as to enable the achievement of its purpose and mission. The table in the slide presents certain requirements that are common to all management systems.

There are several good reasons for integration, to:

- harmonize and optimize practices
- eliminate conflicting responsibilities and relationships
- balance conflicting objectives
- formalize informal systems
- reduce duplication and therefore costs
- reduce risks and increase profitability
- turn the focus into business goals
- create consistency
- improve communication
• facilitate training and awareness

Important note: In June 2009, the Technical Steering Committee of ISO adopted a resolution asking the committees involved in the development of standards to specify the requirements of a management system (ISO 14001, ISO 22000, ISO 27001, etc.) by following a common structure of clauses in line with ISO 9001. This Directive is applicable to the versions published after 2011. So the common elements to every management system will have the same reference. The main objective is to facilitate the combined management of a normative framework for an organization.

Summary of terms

ISO standards
Standard and regulatory framework
Common structure of ISO standards

Questions

1. What is ISO organization?
2. What is ISO standards?
3. What are system management standards?

Reference sources

[1] www.iso.org
[2] PECB ISMS lead Implementer training course
2 ISMS - STANDARD AND REGULATORY FRAMEWORK

Study time

4 hours

Objective

The aim of this chapter is to explain basic definitions and principles which are using in ISMS

Explication

2.1 ISMS BASIC PRINCIPLES

1. **Customer focus**: Organizations depend on their customers and therefore should understand current and future customer needs, should meet customer requirements and strive to exceed customer expectations.

   **Management system implications**
   - Researching and understanding customer needs and expectations.
   - Ensuring that the objectives of the organization are linked to customer needs and expectations.
   - Communicating customer needs and expectations throughout the organization.
   - Systematically managing customer relationships.
   - Ensuring a balanced approach between satisfying customers and other interested parties (such as owners, employees, suppliers, financiers, local communities and society as a whole).

2. **Leadership**: Leaders establish unity of purpose and direction of the organization. They should create and maintain the internal environment in which people can become fully involved in achieving the organization's objectives.

   **Management system implications**
   - Considering the needs of all interested parties including customers, owners, employees, suppliers, financiers, local communities and society as a whole.
   - Establishing a clear vision of the organization's future.
   - Setting challenging goals and targets.
   - Creating and sustaining shared values, fairness and ethical role models at all levels of the organization.
   - Establishing trust and eliminating fear.
   - Providing people with the required resources, training and freedom to act with responsibility and accountability.
   - Inspiring, encouraging and recognizing people's contributions.

3. **Involvement of people**: People at all levels are the essence of an organization and their full involvement enables their abilities to be used for the organization's benefit.
Management system implications
- People understanding the importance of their contribution and role in the organization.
- People identifying constraints to their performance.
- People accepting ownership of problems and their responsibility for solving them.
- People evaluating their performance against their personal goals and objectives.
- People actively seeking opportunities to enhance their competence, knowledge and experience.
- People freely sharing knowledge and experience.
- People openly discussing problems and issues.

4. **Process approach:** A desired result is achieved more efficiently when activities and related resources are managed as a process.

   Management system implications
   - Systematically defining the activities necessary to obtain a desired result.
   - Establishing clear responsibility and accountability for managing key activities.
   - Analyzing and measuring the capability of key activities.
   - Identifying the interfaces of key activities within and between the functions of the organization.

   Focusing on the factors such as resources, methods, and materials that will improve key activities of the organization.
   - Evaluating risks, consequences and impacts of activities on customers, suppliers and other interested parties.

5. **System approach to management:** Identifying, understanding and managing interrelated processes as a system contributes to the organization's effectiveness and efficiency in achieving its objectives.

   Management system implications
   - Structuring a system to achieve the organization's objectives in the most effective and efficient way.
   - Understanding the interdependencies between the processes of the system.
   - Structured approaches that harmonize and integrate processes.
   - Providing a better understanding of the roles and responsibilities necessary for achieving common objectives and thereby reducing cross-functional barriers.
   - Understanding organizational capabilities and establishing resource constraints prior to action.
   - Targeting and defining how specific activities within a system should operate.
   - Continually improving the system through measurement and evaluation.

6. **Continual improvement:** Continual improvement of the organization's overall performance should be a permanent objective of the organization.

   Management system implications
   - Employing a consistent organization-wide approach to continual improvement of the organization's performance.
   - Providing people with training in the methods and tools of continual improvement.
   - Making continual improvement of products, processes and systems an objective for every individual in the organization.
   - Establishing goals to guide, and measures to track, continual improvement.
   - Recognizing and acknowledging improvements.

7. **Factual approach to decision making:** Effective decisions are based on the analysis of data and information.
Management system implications
- Ensuring that data and information are sufficiently accurate and reliable.
- Making data accessible to those who need it.
- Analyzing data and information using valid methods.
- Making decisions and taking action based on factual analysis, balanced with experience and intuition.

8. **Mutually beneficial supplier relationships**: An organization and its suppliers are interdependent and a mutually beneficial relationship enhances the ability of both to create value.

Management system implications
- Establishing relationships that balance short-term gains with long-term considerations.
- Pooling of expertise and resources with partners.
- Identifying and selecting key suppliers.
- Clear and open communication.
- Sharing information and future plans.
- Establishing joint development and improvement activities.
- Inspiring, encouraging and recognizing improvements and achievements by suppliers.

Source: [www.iso.org](http://www.iso.org)

### 2.2 ISMS STANDARDS

Resulting from International workgroup reflections dedicated to the information security scope, the ISO 27000 family is progressively published since 2005. ISO 27001:2005 is the only certifiable standard of the ISO 27000 family. The other standards are guidelines.

- **ISO 27000**: This information security standard develops the basic concepts as well as the vocabulary that applies when analyzing Information Security Management Systems. A free copy of this standard can be downloaded from the ISO website.
- **ISO 27001**: This information security standard defines the requirements of the Information Security Management Systems (ISMS).
- **ISO 27002 (previously ISO 17799)**: Guide of best practices for the management of information security. This standard defines objectives and recommendations in terms of information security and anticipates meeting global concerns of organizations relating to information security for their overall activities.
- **ISO 27003**: Guide for implementing or setting up an ISMS.
- **ISO 27004**: Guide of metrics to facilitate ISMS management, it provides a method to define the objectives for implementation and effectiveness criteria, of follow-up and evolution measurements all through the process.
- **ISO 27005**: Guide for information security risk management which complies with the concepts, models and general processes specified in ISO 27001.
- **ISO 27006**: Guide for organizations auditing and certifying.
- **ISO 27007**: Guidelines for information security management systems auditing.
- **ISO 27008**: Guidelines for auditors on information security controls.
- **ISO 27011**: Guidelines for the use of ISO 27002 in telecommunication industry.
- **ISO 27031**: Guidelines for information and communication technology readiness for business continuity.
- **ISO 27799**: Guidelines for the use of ISO 27002 in health informatics.
ISO 27001:

- A set of normative requirements for the establishment, implementation, operation, monitoring and review to update and improve a Information Security Management System (ISMS);
- A set of requirements for selecting security controls tailored to the needs of each organization based on industry best practices;
- A management system that is integrated in the overall risk framework associated with the activity of the organization;
- An internationally-recognized process, defined and structured to manage information security;
- An international standard to suit all types of organizations (e.g. commercial enterprises, government agencies, nonprofit organizations ...), of all sizes in all industries.

ISO 27001, clause 0.1: General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization’s information security management system is influenced by the organization’s needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization’s processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization’s ability to meet the organization’s own information security requirements

ISO 27002:

This international standard provides a list of security objectives and controls generally practiced in the industry.

In particular Clauses 5 to 18 provide specific advice and an implementation guide related to the best practices to support the controls specified in Annex A of ISO 27001 (clause A.5 to A.18).

ISO 27002, clause 1: Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization’s information security risk environment(s).
This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
b) implement commonly accepted information security controls;
c) develop their own information security management guidelines.

ISO 27003, clause 1 : Scope

This International Standard focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. It describes the process of ISMS specification and design from inception to the production of implementation plans. It describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in this International Standard as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.

This International Standard is intended to be used by organizations implementing an ISMS. It is applicable to all types of organization (e.g. commercial enterprises, government agencies, non-profit organizations) of all sizes. Each organization's complexity and risks are unique, and its specific requirements will drive the ISMS implementation. Smaller organizations will find that the activities noted in this International Standard are applicable to them and can be simplified. Large-scale or complex organizations might find that a layered organization or management system is needed to manage the activities in this International Standard effectively. However, in both cases, the relevant activities can be planned by applying this International Standard. This International Standard gives recommendations and explanations; it does not specify any requirements.

This International Standard is intended to be used in conjunction with ISO/IEC 27001:2005 and ISO/IEC 27002:2005, but is not intended to modify and/or reduce the requirements specified in ISO/IEC 27001:2005 or the recommendations provided in ISO/IEC 27002:2005. Claiming conformity to this International Standard is not appropriate.

Here are some of the standards already published or under development:

- **ISO 27010**: Information security management guidelines for inter-sector communication;
- **ISO 27011**: Information security management guidelines for telecommunications organizations based on ISO 27002;
- **ISO 27013**: Guideline on the integrated implementation of ISO 20000-1 and ISO 27001;
- **ISO 27014**: Information security governance framework;
- **ISO 27015**: Information security management guidelines for the finance and insurance sectors;
- **ISO 27016**: Information security management guidelines on organizational economics;
- **ISO 27017**: Information security management guidelines on cloud computing security and privacy management system;
- **ISO 27018**: Code of practice for data protection controls for public cloud computing services;
- **ISO 27031**: Guideline for ICT readiness for business continuity (essentially the ICT continuity component within business continuity management);
- **ISO 27032**: Guidelines for cyber security;
- **ISO 27033**: IT Network security (ISO 27033-1 to ISO 27033-7);
- **ISO 27034**: Guideline for application security;
- **ISO 27035**: Security incident management;
- **ISO 27036**: Guidelines for security of outsourcing;
- **ISO 27037**: Guidelines for identification, collection and/or acquisition and preservation of digital evidence;
- **ISO 27038**: Specification for Digital Redaction;
- **ISO 27039**: Guideline for selection, deployment and operations of intrusion detection systems;
- **ISO 27040**: Guideline for storage security;
- **ISO 27041**: Guidance on assuring suitability and adequacy of investigation methods;
- **ISO 27042**: Guidelines for the analysis and interpretation of digital evidence;
- **ISO 27043**: Guideline for investigation principles and processes;
- **ISO 29100**: Information technology privacy framework.

### Summary of terms

- 8 system management principles
- ISMS principles

### Questions

What is ISO 27001?
What is ISO 27002?
What is relation between ISO 27001 and ISO 27002?

### Reference sources

[2] PECB Lead ISMS Implementer
3 FUNDAMENTAL DEFINITIONS AND PRINCIPLES IN INFORMATION SECURITY (ISMS)

Study time

4 hours

Objective

The aim of this chapter is to explain basic definitions and principles which are using in ISMS

Explication

3.1 FUNDAMENTAL DEFINITIONS

- **System**: Set of interrelated or interacting elements (ISO 9000, 3.2.1).
- **Management**: Coordinated activities to direct and control an organization (ISO 9000, 3.2.6).
- **Management system**: System to establish policy and objectives to achieve those objectives (ISO 9000, 3.2.2).
- **Information security**: Preservation of confidentiality, integrity and availability of information (ISO 27000, 2.19).

This international standard adopts the process model “Plan-Do-Check-Act” (PDCA) or the Deming cycle which is applied to the structure of all the processes in an management system.

- **Plan (establish the management system)**: Establish the policy, the objectives, processes and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.
- **Do (implement and operate the management system)**: Implement and operate the policy, controls, processes and procedures of the management system.
- **Check (monitor and review the management system)**: Assess and, if applicable, measure process performances against the policy, objectives and practical experience and report the results to management for review.
- **Act (maintain and improve the management system)**: Undertake corrective and preventive actions, on the basis of the results of the internal audit and management review, or other relevant information to continually improve the said system.

1. Asset
2. Information security
3. Vulnerability
4. Threat
5. Risk
6. Confidentiality, integrity and availability (= CIA)
7. Control measures
8. Control environment

ISO 15489-1 standard - Definition

**Information**
Knowledge element that can be represented using conventions to store, process or transmit.

**Data**
Information representation using a conventional format intended to facilitate its processing.

**Record**
Information created, received and maintained as evidence and source of information by an organization or person to prove a transaction or to serve as evidence in a legal framework.

**Information system**
Collection of material, software and organizational ways that allow to receive, store and process information.

**Distribution of information**
Distribution support
- Printed or handwritten
- Recorded using technological support
- Transmitted by email or electronically
- Shown on corporate videos
- Mentioned during conversations

ISO / IEC 27001 is an information security standard. This means it applies to the protection of information whatever its type, whether it be numeric, paper or human.

Annex A includes control objectives related to the classification of information:

ISO/IEC 27001, A7.2 – Information classification

Objective: To ensure that information receives an appropriate level of protection.

A7.2.1 Classification guidelines

Control: Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.

A7.2.2 Information labelling and handling

Control: An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
Information security
ISO 27000, clause 2.2.3,
Aims to protect information against a large range of threats, to ensure business continuity, to minimize risks, and to optimize the return on investment as well as business opportunities for the organization.

ISO 27000, clause 2.19
Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Vulnerability
ISO 27000, clause 2.46
Weakness of an asset or control that can be exploited by a threat.

Threat
Potential cause of an unwanted incident, which may result in harm to a system or organization.

ISO/IEC 27005:2008 Annex C provides a typology classification of seven types of threats that we can base ourselves on.

1. Physical damage: Fire, water damage, etc.
2. Natural disaster: Earthquake, flood, etc.
3. Loss of essential service: Air conditioning outage, power failure, etc.
4. Disruption caused by radiation: Electromagnetic radiation, thermal radiation, etc.
5. Compromised information: Electronic surveillance, document theft, etc.
6. Technical breakdown: Equipment failure, network saturation, etc.
7. Unauthorized action: Unauthorized access, use of pirated software, etc.

Obr. 1.6: Relationship – threat/vulnerability

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warehouse unprotected and without surveillance</td>
<td>Theft</td>
</tr>
<tr>
<td>Complicated data processing procedures</td>
<td>Data input error by personnel</td>
</tr>
<tr>
<td>No segregation of duties</td>
<td>Fraud, unauthorized use of a system</td>
</tr>
<tr>
<td>Unencrypted data</td>
<td>Information theft</td>
</tr>
<tr>
<td>Use of pirated software</td>
<td>Lawsuit, virus</td>
</tr>
<tr>
<td>No review of access rights</td>
<td>Unauthorized access by persons who have left the organization</td>
</tr>
</tbody>
</table>
In itself, the presence of a vulnerability does not produce damage, a threat must exist to exploit it. A vulnerability non corresponding to a threat may not require the setting up of a control, but it must be identified and monitored in case of changes.

Note that the incorrect implementation, use or malfunction of a control could, in itself, represent a threat. A control can be effective or ineffective based on the environment in which it operates. On the other hand, a threat that is not vulnerable cannot represent a risk.

**Information security risk**
ISO 27005, clause 3.2
Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization
Note: It is measured in terms of a combination of the likelihood of an event and its consequence.

**Confidentiality**
ISO 27000, clause 2.9
Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Confidentiality: Ensure that the information is only accessible to authorized individuals (individuals with a real need).
For example: the personal data of salaried employees must only be accessible to authorized Human Resources Department personnel.

**Integrity**
ISO 27000, Clause 2.25
Property of protecting the accuracy and completeness of assets (2.3)
Integrity: Data must be complete and intact.
For example: Accounting data must comply to reality (complete and exact). The exactness is translated by the absence alterations in the information.

**Availability**
ISO 27000, Clause 2.7
Property of being accessible and usable upon demand by an authorized entity.
Availability: Information must be easily accessible by individuals who need it.
For example, data related to customers must be accessible to the marketing department.

**Controls**
ISO 27000, clause 2.10-11
Means to manage a risk
Includes policies, procedures, guidelines and practices or organizational structures
Synonym: measure, counter-measure, security device.
1. **Technical controls**: Controls related to the use of technical measures or technologies such as firewalls, alarm systems, surveillance cameras...

2. **Administrative controls**: Controls related to administration and administrative support, including the organization of employees, the control of resources, etc...

3. **Managerial controls**: Controls related to the management of personnel, including training and personnel management...

4. **Legal controls**: Controls related to the applications of a legislation.

Strategic controls are under the responsibility of management and include the follow-up of strategies, organization structures, personnel and standards. More important still, their objective is to align IT objectives to the global strategy of the organization to ensure an effective contribution to the attainment of the organization objectives. They are the controls related to clauses 4 to 8 of ISO 27001. Many organizations use COBIT to implement and manage their governance controls.

General controls define the detailed mechanisms with which an organization guarantees the delivery of IT services that it needs. These controls manage the risks that could have an impact on the IT services the organization depends on. IT controls put the emphasis on human activities as well as on technology to provide the company with a general level of risk management. These are the ISO 27001 Annex A controls. As the case maybe, controls can be selected in other guides or standards or even still to specify new control measures to satisfy specific requirements of the organization.

Application controls are automated controls included in a specific information system (for example: accounting, logistics or sales software). These controls are specific to each system or process and constitute sub-controls of the general controls. For example, that authenticates a user at the opening of a session on an ERP software package is part of the access controls.
Summary of terms

- Vulnerability
- Threat
- Confidentiality
- Availability
- Integrity
- ISMS
- Risk
- Security control

Questions

1. What confidentiality, integrity and availability?
2. What is security control?
3. What are types of security controls?
4. What is a risk?

Reference sources

[3] ISO 27000 Definitions
4 INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

Study time: 4 hrs

Objective:
How to implement ISMS
Advantages of the ISMS

Explication

4.1 WHY IMPLEMENT ISMS?

An ISMS is important to both public and private sector businesses.

An ISMS is a driver that supports e-business and is essential for risk management activities.

The interconnection of public and private networks and sharing of information assets increases the difficulty of managing access to information resources.
The mobile storage devices and cloud solutions can weaken the effectiveness of traditional controls.

**Improvement of security:**
- General improvement of the effectiveness of security;
- Independent review of your security management system;
- Better awareness to security;
- Mechanisms to measure the effectiveness of the management system.

**Good governance:**
- Awareness and empowerment of personnel regarding security;
- Decrease of lawsuit risks against upper management in virtue of the “due care” and the “due diligence” principles;
- The opportunity to identify the weaknesses of the SMS and to provide corrections;
- Increase of the accountability of top management for security.

**Conformity:**
- To other ISO standards;
- To industry standards
- To national and regional laws.

**Cost reduction:**
- Decision makers often ask to justify the profitability of projects and demand concrete and measurable return-benefits. A new financial evaluation concept has emerged to treat specifically the security field: Return on Security Investment (ROSI). ROSI is a concept derived from Return on Investment (ROI). It can be interpreted as the security project’s financial profit taking into account its total cost over a given period of time.

**Marketing:**
• Differentiation provides a competitive advantage for the organization;
• Satisfaction of requirements of customer and/or other stakeholders;
• Consolidating confidence of customers, suppliers and partners of the organization.

Summary of terms

An Information Security Management System (ISMS) is the part of the global management system based on a risk based approach to establish, implement, operate, monitor review, update and improve information security.

The ISMS is used to ensure a selection of adequate and proportionate security controls that protect the assets and bring assurance to the stakeholders.

Questions

What are the reasons to adopt ISO 27001?
What is the advantage of the certified ISMS?
How can the organization measure this advantage?

Reference sources

[3] ISO 27000 Definitions
5  STANDARDS FOR ISMS IMPLEMENTATION

Study time

5 hrs

Objective

Obtain approval of management through approval of a formal project charter, which show, for example, that the proposed ISMS is part of a portfolio of projects already approved.
2. Give authority and credibility to the project manager to enable him to succeed.
3. Legitimizing the ISMS project to the stakeholders of the organization.

Explication

5.1 INTERNATIONAL STANDARDS FOR ISMS

Pic.: ISO/IEC 27000 Family

ISO 27001:2013 is the standard for certification. The other standards are guidelines.
• ISO 27000: This information security standard develops the basic concepts as well as the vocabulary that applies when analyzing Information Security Management Systems. A free copy of this standard can be downloaded from the ISO website.

• ISO 27001: This information security standard defines the requirements of the Information Security Management Systems (ISMS).

• ISO 27002: Guide of best practices for the management of information security. This standard defines objectives and recommendations in terms of information security and anticipates meeting global concerns of organizations relating to information security for their overall activities.

• ISO 27003: Guide for implementing or setting up an ISMS.

• ISO 27004: Guide of metrics to facilitate ISMS management, it provides a method to define the objectives for implementation and effectiveness criteria, of follow-up and evolution measurements all through the process.

• ISO 27005: Guide for information security risk management which complies with the concepts, models and general processes specified in ISO 27001. • ISO 27006: Guide for organizations auditing and certifying ISMS’s. • ISO 27007: Guidelines for information security management systems auditing.

• ISO 27008: Guidelines for auditors on information security controls.

Summary of terms

An Information Security Management System (ISMS) is the part of the global management system based on a risk based approach to establish, implement, operate, monitor review, update and improve information security. The ISMS is used to ensure a selection of adequate and proportionate security controls that protect the assets and bring assurance to the stakeholders.

Questions

What are the reasons to adopt ISO 27001?

What is the advantage of the certified ISMS?

How can the organization measure this advantage?

Reference sources

[3] ISO 27000 Definitions
6 INFORMATION SECURITY RISK MANAGEMENT

Study time: 8 hours

Objective:

- Get knowledge of the information risk management
- Overview of the risk management processes

Explication

6.1 RISK MANAGEMENT DEFINITIONS

ISO 27000 - Definitions


2.62. Risk acceptance: Decision to accept a risk.

2.63. Risk analysis: process to comprehend the nature of risk and to determine the level of risk

2.64. Risk assessment: Overall process of risk identification, risk analysis and risk evaluation.

2.67. Risk evaluation: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

2.69. Risk management: Coordinated activities to direct and control an organization with regard to risk.

2.71. Risk treatment: Process of selection and implementation of measures to modify risk.

6.2 RISK MANAGEMENT PROCESS

The main objectives of this process is:

- Select and define an approach to risk assessment that is aligned with the management of the organization.
- Select and define a methodology of risk assessment adapted to the needs of the organization

According to ISO 27001, clause 6.1.2 Information security risk assessment the organization shall define and apply an information security risk assessment process that:
a) establishes and maintains information security risk criteria that include:

1) the risk acceptance criteria; and
2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
2) identify the risk owners;

d) analyses the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;
2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and
3) determine the levels of risk;

e) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and
2) prioritize the analyzed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

Information risk management process may be established according to ISO 31000 and ISO 27005.

Based on ISO 31000 framework, the ISO 27005 standard explains in detail how to conduct a risk assessment and a risk treatment, within the context of information security. This is the implementation of the continual improvement cycle PDCA (Plan, Do, Check, Act) for risk management as it is used in all standards of management systems. In this case, it can be fairly easily connected to the corresponding clauses in the ISO 27001 on risk management (clauses 4.2.1 c to h and 4.2.3 d), ultimately leading to the certification of the organization.

6.3 INFORMATION SECURITY RISK ANALYSIS

The risk analysis (identification and assessment) can be undertaken at various levels of detail depending on the criticality of assets within the scope and complexity of risk scenarios to be analyzed. A methodology for assessment may be qualitative or quantitative, or a combination of both, depending on the circumstances.

In a qualitative approach, we develop risk scenarios by assigning a level of importance on threats, vulnerabilities and potential impact to achieve a level of risk. In the end, we calculate the risk and we recommend appropriate control measures. It should be noted that the results of a qualitative approach is relevant when we can compare the risk scenarios to each other. That is to say that the risk described as "medium" level or "3" means...
nothing by itself. This risk value makes sense when compared with another risk called "low, medium or high" level or "1, 2, 3 etc.

The quantitative risk analysis uses mathematical and financial analysis by assigning a monetary value to each component of the risk assessment and to the potential losses. Information security risk analysis is define by the following expression:

![Image](probability_consequence_risk.png)

### 6.4 PC AND SW TOOLS

The computer assisted support and SW tools are using in some cases for risk analysis process.

There are many SW tools for computer assisted Risk analysis:

@Risk, COBRA, CONTROL-IT, CoP-IT, CORAS, CRAMM, CRITI CALC, IS CASE, IST/RAMP, RA/SYS, RANK-IT, RISAN, Risiko, RiskCALC, RiskPAC, Riskwatch, SISSI, etc.

Here are some most common tools:

**OCTAVE** (Operationally Critical Threat, and Vulnerability Evaluation): allows to evaluate the values threatened, the most formidable risks, as well as the vulnerability of the defense based on a standardized knowledge base (standard catalogue of information) included in the method.

**CRAMM** (*CCTA Risk Analysis and Management Method*): The CRAMM is a three- phase structure: definition of values threatened, risk and vulnerability analysis and definition and selection of security measures.

<table>
<thead>
<tr>
<th>Summary of terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this International Standard.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the qualitative approach for risk analysis?</td>
</tr>
<tr>
<td>What standards are usually used for designing of the risk management process?</td>
</tr>
<tr>
<td>What are the basic steps in risk assessment according to ISO 27001?</td>
</tr>
</tbody>
</table>
Reference sources

[2] PECB Lead ISMS Implementer
7 IMPLEMENTATION ISMS ACCORDING TO ISO/IEC 27001

7.1 14 STEPS TO ISMS IMPLEMENTATION

Study time: 12 hrs

Objective:
- Definition of the individual steps for ISMS implementation project
- Description of the main activities related to ISMS implementation

Explication

STEP 1 – Management decision, leadership and approval of the ISMS project
STEP 2 – Define the scope and boundaries of the ISMS
STEP 3 – Definition of Security policy (ISMS Policy) and ISMS objectives
STEP 4 – Risk management approach
STEP 5 – Definition of the document management process
STEP 6 – Establishment of Risk treatment Plan
STEP 7 – Design of security controls and drafting of specific policies & procedures
STEP 8 – Implementation of selected security controls
STEP 9 - Training and awareness plan
STEP 10 - Incident Management
STEP 11 - Operations Management
STEP 12 - Internal Audit
STEP 13 - Management Review
STEP 14 - Certification
7.1.1 Management decision, leadership and approval of the ISMS project

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
b) ensuring the integration of the information security management system requirements into the organization’s processes;
c) ensuring that the resources needed for the information security management system are available;
d) communicating the importance of effective information security management and of conforming to the information security management system requirements;
e) ensuring that the information security management system achieves its intended outcome(s);
f) directing and supporting personnel to contribute to the effectiveness of the information security management system;
g) promoting continual improvement
h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

As this course main purpose is to explain the methodology for the ISMS management implementation the most used method how to implement ISMS is based on project management.

There are several project management standards for ISMS implementation project like as PRINCE2, PMI, PMBOK etc. It depends on the organization what approach and method choice for the project management.

7.1.2 Define the context, scope and boundaries of the ISMS

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

The organization shall determine:

a) interested parties that are relevant to the information security management system; and
b) the requirements of these interested parties relevant to information security.

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues
b) the requirements
   c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

7.1.3 Definition of Security policy (ISMS Policy) and ISMS objectives

This ISMS policy shall:
- Include a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security.
- Take into account business and legal or regulatory requirements, and contractual security obligations.
- Align with the organization’s strategic risk management context in which the establishment and maintenance of the ISMS will take place.
- Establish criteria against which risk will be evaluated.
- Be approved by management.

An objective is the result that the organization wants to achieve. These objectives are generally clear, quantified and time bound (SMART).

Implications for risk management: As for strategy, risk management must know and be aligned with business objectives to achieve its objectives by identifying information risk that the organization must manage.

The objectives of a information security management program are the expression of the intent of the organization to treat the risks identified and / or to comply with requirements of organizational security. Initially, it is necessary to establish the objectives of ISMS in consultation with the interested parties.

The objectives of the ISMS are needed to determine the scope and must be validated at the highest level of the organization. Goals can be refined during the project, particularly after the completion of the risk analysis. It is clear that the objectives should be formally documented.

### 7.1.4 Risk management approach

As a minimum, any risk analysis must take into account the following evaluation criteria, required by ISO/IEC 27001 standard:

1. Determination of the risk acceptance criteria and identification of acceptable risk levels
2. Identification of assets
3. Identification of threats to which assets are confronted
4. Identification of vulnerabilities that could be exploited by threats
5. Identification of impacts that loss of confidentiality, integrity and availability can have on assets
6. Analysis and evaluation of the impact on the organization’s activity that could derive from a security failure, taking into account the consequences of a loss of confidentiality, integrity or availability of assets
7. Analysis and evaluation of the realistic probability of a security failure of this nature on the basis of predominant threats and vulnerabilities, associated impacts to these assets and controls currently in place
8. Estimation of risk levels
9. Determination of acceptable risk thresholds on the basis of established risks
10. Identification and evaluation of risk treatment options
11. Selection of security and control objectives for treating risks
7.1.5 Definition of the document management process

The ISMS shall include:

- documented information required by ISO/IEC 27001 Standard; and documented information determined by the organization as being required for the effectiveness of the ISMS.
- The extent of documented information for a ISMS can differ from one organization to another due to
  - the size of organization and its type of activities, processes, products and services,
  - the complexity of processes and their interactions, and
  - the competence of persons.

7.1.6 Establishment of Risk treatment Plan

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

c) compare the security controls determined in b) above with those in Annex A of the ISO 27001 and verify that no necessary controls have been omitted;

   NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.

   NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

d) produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A

e) formulate an information security risk treatment plan; and

f) obtain risk approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

7.1.7 Design of security controls and drafting of specific policies and procedures

Initially, the organization must review the 114 security controls in Annex A to identify those that are applicable and those that will not be considered in the context of the ISMS. The choice whether to apply a security control should be justified primarily by the risk assessment.

The Statement of Applicability is created in this phase of ISMS implementation process.

ISO 27001 does not specify the form of the statement of applicability. It simply requires making a list of security controls, selected or not, the reasons for these choices and actions being implemented to meet the security controls being selected in the document. The additional controls put in place must also appear in the statement of applicability.

It is good practice to include in the statement of applicability, the title or function of the responsible person per control and the list of documents or records relating to it. The model proposed by PECB includes the following sections:

1. Security control: Indicates the reference to Annex A of the security control

2. Applicable: Indicates whether the security control is applicable or not.
3. **Brief description:** Describes briefly in a few sentences the control and how it is implemented in the organization. A simple way to do this is to use the method of the 6 W’s (Who, What, When, Where, Why, How). It should be noted that the "why" is addressed in the column "justification".

   For example: A security policy information (What), approved by management (who) is in force since December 21, 2008 (When). A copy was sent (how) to all employees and stakeholders (Who). The official version is available on the Intranet (Where).

4. **Justification:** Describes the reasons for selecting or exclusion of the security control

5. **Documentation:** Indicates documents (policies and procedures) or records related to this security control.

6. **Responsible:** The owner of the control is the person who is responsible. This must be a person whose name and position in the organization are included in the document. If the security control is not applicable, please indicate the person able to prove its non-applicability to facilitate the work of auditors (internal and external) and know who to address for information during the subsequent revisions of the statement of applicability.

7.1.8 **Implementation of selected security controls**

   Main objectives of the process of implementation processes and security controls

   1. Ensuring the effective protection of assets of the organization through the implementation of security controls
   2. Ensuring the effective protection of assets of the organization

7.1.9 **Training and awareness plan**

   **The main objectives** of the training and awareness plan are to ensure the competence of those employees and interested parties involved in the operations of the ISMS.

   A program of information security cannot achieve its objectives without the commitment of all stakeholders. Whether an internal actor (employee, executive, union) or an external one (customers, suppliers) is involved, training, awareness and communication are crucial for the successful implementation of the ISMS.

   A user who has not been properly informed, trained and made aware to the importance of information security is a potential risk to the security of the organization and therefore its business processes. The incidents of information security due to handling errors or behavior might be minimized or avoided by implementing a rigorous program of training, and awareness on information security.

   It appears necessary to develop and disseminate a training and awareness program for stakeholders. They can then contribute to the success of the process of managing information security in the organization.

   An organization wishing to comply with ISO 27001 shall at least:

   3. Identifying the skills needed to ensure the proper functioning of the ISMS.
   4. Implement a training program for personnel performing work affecting the ISMS.
   5. Implement an awareness program on information security appropriate to different stakeholders.
   6. Implement a communication program to inform stakeholders of the ISMS about changes that may affect them.
   7. Evaluate the effectiveness of actions taken and keep records.
7.1.10 Incident Management

There are several definitions using in incident management process. Here are definitions:

- **Information security event**: Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant (ISO27000, 2.31 and ISO 27035, 3.3)

- **Information security incident**: single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security (ISO 27000, 2.32 and ISO27035, 3.4)

- **Information Security Incident Response Team**: Team of appropriately skilled and trusted members of the organization, which will handle information security incidents during their lifecycle (ISO 27035, 3.2)

- **Information security incident management**: Processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (ISO 27000, 2.33)

Before implementing a process for effective management of incidents, a risk analysis to identify risk scenarios that could affect the organization should have been carried out.

The information from the risk management process is an important input to the continuous improvement process of the organization

**Input**

- Policies, processes and security procedures of the organization
- Risk Analysis report

**Activities**

Implementation of ways to detect and respond to incidents, appropriate training, communication about incidents, management and learning from experience

**Output**

- Processes and procedures for managing incidents
- Incident Management Team

7.1.11 Operations Management

The main activities of the operation management process are:

- Transfer the ISMS project to the operation environment of the organization.
- To keep the ISMS up-to-date in a long-term perspective

An organization wishing to comply with ISO 27001 shall at least:

- Ensure effective management of operations related to ISMS.
- Ensure the provision of adequate resources for the functioning of the ISMS

7.1.12 Internal audit process

Internal audits are used to assess the level of fulfillment of the requirements of the standard relating to the management system. Regular internal audit activities allow assessing continuously the effectiveness of the management system and identifying opportunities for improvement.
The organization must implement an internal audit programme to determine if the management system reaches the defined objectives of the organization, remains conform to the standard as well to other internal, legal, regulatory and contractual requirements and is kept up-to-date in an efficient manner.

The audit program shall, as a minimum, contain:

1. Definition of the criteria, the scope, the frequency, the methods and the audit procedures;
2. Definition of the roles and responsibilities of the internal auditors;
3. Documentation ensuring the objectivity and impartiality of the audit process (examples: audit chart, work contract, code of ethics of internal auditors, etc.);
4. Planning of audit activities;
5. Follow-up activities to audit the business actions following the detection of non conformities;
6. Procedure to keep the records of audit activities and safekeeping of records.

7.1.13 Management Review

Management reviews allow the management of the organization to periodically review the level of performance (relevance, appropriateness, effectiveness and efficiency) of the management system in place. These reviews allow the organization to adapt or refocus quickly and efficiently the management system towards internal or external changes.

A management review shall be done at least once a year. Management reviews must be documented and then should be distributed to all interested participants.

7.1.14 Certification

The certification process is the final phase of the whole ISMS project effort. This is not an obligatory requirement in the ISMS project but it is highly recommended. The certification is independent assessment to confirm that the organization’s ISMS is in compliance with the ISO 27001 standard.

7.2 114 SECURITY CONTROLS (ISO 27001, ANNEX A)

Information security controls are set of security controls listed in Annex A of the ISO 27001.

Below is an overview of all controls:

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
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

A.5.1 Information security policies

A.5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 Policies for information security

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

A.5.1.2 Review of the policies for information security

The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

A.6. Organization of information security

A.6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A.6.1.1 Information security roles and responsibilities

All information security responsibilities shall be defined and allocated.

A.6.1.2 Segregation of duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the assets.

A.6.1.3 Contact with authorities

Appropriate contacts with relevant authorities shall be maintained.

A.6.1.4 Contact with special interest groups

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6.1.5 Information security in project management

Information security shall be addressed in project management, regardless of the type of the project.

A.6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

A.6.2.1 Mobile device policy

A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

A.6.2.2 Teleworking

A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

A.7. Human resource security

A.7.1 Prior to employment
**Objective:** To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

**7.1.1 Screening**
Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

**A.7.1.2 Terms and conditions of employment**
The contractual agreements with employees and contractors shall state their and the responsibilities for information security

**A.7.2 During employment**
**Objective:** To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

**A.7.2.1 Management responsibilities**
Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

**A.7.2.2 Information security awareness, education and training**
All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

**A.7.2.3 Disciplinary process**
There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

**A.7.3 Termination and change of employment**
**Objective:** To protect the interests as part of the process of changing or terminating employment.

**A.7.3.1 Termination or change of employment responsibilities**
Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

**A.8 Asset management**
**A.8.1 Responsibility for assets**
**Objective:** To identify organizational assets and define appropriate protection responsibilities.

**A.8.1.1 Inventory of assets**
Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

**A.8.1.2 Ownership of assets**
Assets maintained in the inventory shall be owned.

**A.8.1.3 Acceptable use of assets**
Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

**A.8.1.4 Return of assets**
All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

A.8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

A.8.2.1 Classification of information
Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

A.8.2.2 Labelling of information
An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.8.2.3 Handling of assets
Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

A.8.3.1 Management of removable media
Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

A.8.3.2 Disposal of media
Media shall be disposed of securely when no longer required, using formal procedures.

A.8.3.3 Physical media transfer
Media containing information shall be protected against unauthorized access, misuse or corruption during transportation

A.9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

A.9 Access control

A.9.1.1 Access control policy
An access control policy shall be established, documented and reviewed based on business and information security requirements.

A.9.1.2 Access to networks and network services
Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

A.9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

A.9.2.1 User registration and de-registration
A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

A.9.2.2 User access provisioning
A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

A.9.2.3 Management of privileged access rights
The allocation and use of privileged access rights shall be restricted and controlled.

A.9.2.4 Management of secret authentication information of users
The allocation of secret authentication information shall be controlled through a formal management process.

A.9.2.5 Review of user access rights
Asset owners shall review access rights at regular intervals.

A.9.2.6 Removal or adjustment of access rights
The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9.3 User responsibilities
Objective: To make users accountable for safeguarding their authentication information.

A.9.3.1 Use of secret authentication information
Users shall be required to follow the organization’s practices in the use of secret authentication information.

A.9.4 System and application access control
Objective: To prevent unauthorized access to systems and applications.

A.9.4.1 Information access restriction
Access to information and application system functions shall be restricted in accordance with the access control policy.

A.9.4.2 Secure log-on procedures
Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

A.9.4.3 Password management System
Password management systems shall be interactive and shall ensure quality passwords.

A.9.4.4 Use of privileged utility Programs
The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

A.9.4.5 Access control to program source code
Access to program source code shall be restricted.

A.10 Cryptography
A.10.1 Cryptographic controls
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1 Policy on the use of cryptographic controls
A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.10.1.2 Key management
A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

A.11 Physical and environmental security
A.11.1 Secure areas
Objective: To prevent unauthorized physical access, damage and interference to the information and information processing facilities.

A.11.1.1 Physical security perimeter
Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

A.11.1.2 Physical entry controls
Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

A.11.1.3 Securing offices, rooms and facilities
Physical security for offices, rooms and facilities shall be designed and applied.

A.11.1.4 Protecting against external and environmental threats
Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

A.11.1.5 Working in secure areas
Procedures for working in secure areas shall be designed and applied.

A.11.1.6 Delivery and loading areas
Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

A.11.2 Equipment
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the operations.

A.11.2.1 Equipment siting and protection
Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

A.11.2.2 Supporting utilities
Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

A.11.2.3 Cabling security
Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

A.11.2.4 Equipment maintenance
Equipment shall be correctly maintained to ensure its continued availability and integrity.

A.11.2.5 Removal of assets
Equipment, information or software shall not be taken off-site without prior authorization.

A.11.2.6 Security of equipment and assets off-premises
Security shall be applied to off-site assets taking into account the different risks of working outside the premises.

A.11.2.7 Secure disposal or reuse of equipment
All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

A.11.2.8 Unattended user equipment
Users shall ensure that unattended equipment has appropriate protection.

A.11.2.9 Clear desk and clear screen policy
A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

A.12 Operations security
A.12.1 Operational procedures and responsibilities
Objective: To ensure correct and secure operations of information processing facilities.

A.12.1.1 Documented operating procedures
Operating procedures shall be documented and made available to all users who need them.

A.12.1.2 Change management
Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

A.12.1.3 Capacity management
The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

A.12.1.4 Separation of development, testing and operational environments
Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

A.12.2 Protection from malware
Objective: To ensure that information and information processing facilities are protected against malware.

A.12.2.1 Controls against malware
Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

A.12.3 Backup
Objective: To protect against loss of data.

A.12.3.1 Information backup
Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

A.12.4 Logging and monitoring
Objective: To record events and generate evidence.

A.12.4.1 Event logging
Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.4.2 Protection of log information
Logging facilities and log information shall be protected against tampering and unauthorized access.

A.12.4.3 Administrator and operator logs
System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

A.12.4.4 Clock synchronization
The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.

A.12.5 Control of operational software
Objective: To ensure the integrity of operational systems.

A.12.5.1 Installation of software on operational systems
Procedures shall be implemented to control the installation of software on operational systems.

A.12.6 Technical vulnerability management
Objective: To prevent exploitation of technical vulnerabilities.

A.12.6.1 Management of technical vulnerabilities
Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A.12.6.2 Restrictions on software installation
Rules governing the installation of software by users shall be established and implemented.

A.12.7 Information systems audit considerations
Objective: To minimise the impact of audit activities on operational systems.

A.12.7.1 Information systems audit controls
Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

A.13 Communication security
A.13.1 Network security management
Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.1.1 Network controls
Networks shall be managed and controlled to protect information in systems and applications.

A.13.1.2 Security of network services
Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

A.13.1.3 Segregation in networks
Groups of information services, users and information systems shall be segregated on networks

A.13.2 Information transfer

**Objective:** To maintain the security of information transferred within an organization and with any external entity.

A.13.2.1 Information transfer policies and procedures

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

A.13.2.2 Agreements on information transfer

Agreements shall address the secure transfer of business information between the organization and external parties.

A.13.2.3 Electronic messaging

Information involved in electronic messaging shall be appropriately protected.

A.13.2.4 Confidentiality or nondisclosure agreements

Requirements for confidentiality or non-disclosure agreements reflecting the needs for the protection of information shall be identified, regularly reviewed and documented.

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems

**Objective:** To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A.14.1.1 Information security requirements analysis and specification

The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

A.14.1.2 Securing application services on public networks

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

A.14.1.3 Protecting application services transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay

A.14.2 Security in development and support processes

**Objective:** To ensure that information security is designed and implemented within the development lifecycle of information systems.

A.14.2.1 Secure development policy

Rules for the development of software and systems shall be established and applied to developments within the organization.

A.14.2.2 System change control procedures

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
A.14.2.3 Technical review of applications after operating platform changes
When operating platforms are changed, business critical applications shall be reviewed and tested
to ensure there is no adverse impact on organizational operations or security.

A.14.2.4 Restrictions on changes to software packages
Modifications to software packages shall be discouraged, limited to necessary changes and all changes
shall be strictly controlled.

A.14.2.5 Secure system engineering principles
Principles for engineering secure systems shall be established, documented, maintained and applied to
any information system implementation efforts.

A.14.2.6 Secure development environment
Organizations shall establish and appropriately protect secure development environments for system
development and integration efforts that cover the entire system development lifecycle

A.14.2.7 Outsourced development
The organization shall supervise and monitor the activity of outsourced system development.

A.14.2.8 System security testing
Testing of security functionality shall be carried out during development.

A.14.2.9 System acceptance testing
Acceptance testing programs and related criteria shall be established for new information systems,
upgrades and new versions

A.14.3 Test data
Objective: To ensure the protection of data used for testing.

A.14.3.1 Protection of test data
Test data shall be selected carefully, protected and controlled

A.15 Supplier relationship
A.15.1
Objective: To ensure protection of the assets that is accessible by suppliers.

A.15.1.1 Information security policy for supplier relationships
Information security requirements for mitigating the risks associated with access to the asset
shall be agreed with the supplier and documented.

A.15.1.2 Addressing security within supplier agreements
All relevant information security requirements shall be established and agreed with each supplier that
may access, process, store, communicate, or provide IT infrastructure components for, the
information.

A.15.1.3 Information and communication Technology supply chain
Agreements with suppliers shall include requirements to address the information security risks
associated with information and communications technology services and product supply chain.

A.15.2 Supplier service delivery management
Objective: To maintain an agreed level of information security and service delivery in line with
supplier agreements.

A.15.2.1 Monitoring and review of supplier services
Organizations shall regularly monitor, review and audit supplier service delivery.

A.15.2.2 Managing changes to supplier services
Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

A.16 Information security incident management
A.16.1 Management of information security incidents and improvements
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.16.1.1 Responsibilities and procedures
Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A.16.1.2 Reporting information security events
Information security events shall be reported through appropriate management channels as quickly as possible.

A.16.1.3 Reporting information security weaknesses
Employees and contractors using the information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

A.16.1.4 Assessment of and decision on information security events
Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

A.16.1.5 Response to information security incidents
Information security incidents shall be responded to in accordance with the documented procedures.

A.16.1.6 Learning from information security incidents
Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

A.16.1.7 Collection of evidence
The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

A.17 Information security aspects of business continuity management
A.17.1 Information security continuity
Objective: Information security continuity shall be embedded in the business continuity management systems.

A.17.1.1 Planning information security continuity
The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

A.17.1.2 Implementing information security continuity
The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

A.17.1.3 Verify, review and evaluate information security continuity
The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations

A.17.2 Redundancies
Objective: To ensure availability of information processing facilities.

A.18.1 Compliance with legal and contractual requirements
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.1.1 Identification of applicable legislation and contractual requirements
All relevant legislative statutory, regulatory, contractual requirements and the approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

A.18.1.2 Intellectual property rights
Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

A.18.1.3 Protection of records
Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.

A.18.1.4 Privacy and protection of personally identifiable information
Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

A.18.1.5 Regulation of cryptographic controls
Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations

A.18.2 Information security reviews
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

A.18.2.1 Independent review of information security
The approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

A.18.2.2 Compliance with security policies and standards
Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

A.18.2.3 Technical compliance review
Information systems shall be regularly reviewed for compliance with the information security policies and standards.

Summary of terms

1. An Information Security Management System (ISMS) is the part of the global management system based on a risk based approach to establish, implement, operate, monitor review, update and improve information security.
2. The ISMS is used to ensure a selection of adequate and proportionate security controls that protect the assets and bring assurance to the stakeholders.
3. Controls are used to ensure that the conduct of business processes is performed in a secure manner in terms of information exchange. These security processes and controls are dependent of business processes because they are integrated to them.
4. An organization that requests certification must be conform to all the clauses defined in Clauses 4 to 10 of ISO 27001, declaring the applicable controls together with the reasons for their selection and justifying the excluded controls of Annex A in the statement of applicability.
5. Security objectives and security controls themselves must be selected and implemented to meet the requirements identified by the risk assessment process and risk management process. This selection must take into account the risk acceptance criteria as well as the legal, regulatory and contract requirements.
6. The organization must continually improve the effectiveness of its ISMS through its policy and objectives, its internal audits as well as by the preventive and corrective controls initiated by management reviews.

Questions

From the information provided in the case study on the functioning of the change management process, please rate the maturity level of this process. Also, the management of the organization would like to receive recommendations from you to improve the processes in place to comply with the requirements of ISO 27001 on change management.

Reference sources

[3] ISO 27000 Definitions
8 ISO/IEC 27001 – CERTIFICATION PROCESS

8.1 CERTIFICATION ISMS ACCORDING TO ISO/IEC 27001

Study time: 2 hrs

Objective:
- Determine activities in every stage of the certification
- Describe advantages of implemented and certified ISMS

Explication

Certification process covers the following stages:

1. Certification process
2. Certification schema
3. Certification authority
4. Certification organization
5. People certification organization

Graphical representation of the certification process is on the following picture:
Description of the individual steps:

Selection of the certification organization (registrar): Each organization can select the certification body (registrar) of its choice.

Pre-evaluation (optional): An organization can choose to do a pre-audit to measure the gap between its current ISMS and the ISO 27001 requirements.

Documentary audit (Phase 1): It is the conformity review of the documents related to the ISMS management. It is not mandatory for auditors to be on site to conduct this phase of the audit to term. The objective being to verify that the documents meet to the requirements of the audit criteria.

On-site audit (Phase 2): The on-site audit objective is to evaluate if the declared ISMS is conform to all ISO/IEC 27001 requirements, is actually implemented in the organization and can allow the organization to reach its security objectives. Phase 2 takes place at the site(s) of the organization where the ISMS is implemented.

Follow-up audit and confirmation of registration: If the auditee has nonconformities that require a new audit before being certified, the auditor will perform a follow-up visit to validate only the action plans linked to the nonconformities (usually one day). If the organization has complied to the conditions of the standard, the registrar confirms the registration and publishes the certificate.

Continuous improvement and monitoring audit: Once an organization is registered, monitoring activities are conducted by the certification body to ensure that the ISMS still complies with the standard. The monitoring activities must include on-site audits (at least 1/year) that allow to verify the conformity of the certified client’s management system and can also include: investigations following a complaint, review of a Website, a written request for follow-up, etc.

The certification process involves the following parties:

- Accreditation organizations (responsible for the assessment and the accreditation of certification organizations) (CIA, UKAS, COFRAC);

- Certification/Registration organizations (responsible for managing the certification activities of their customers and performing audits on their customers’ management system) (CQS, V4 Systems, BSI, Bureau Veritas, DNV, TUV, etc.);
• Organizations whose management system is subject to certification and who are customers of certification organizations.

Certification organizations are responsible for the registration of companies to ISO/IEC 27001:2013 and to employ auditors.

Accreditation authority
• Organization at the national level that supervises certification programs (organizations and auditors) and who makes sure that national or international criteria are respected.
• Only one accreditation authority exist per country

Here is a list of accreditation authorities for several countries (see complete list on IAF site):
• CIA: Czech Institution for Accreditation, www.cia.cz
• ANAB: ANSI-ASQ National Accreditation Board (United States), www.anab.org
• SAS: State Secretariat for Economic Affairs, Swiss Accreditation Service, www.sas.ch
• UKAS: United Kingdom Accreditation Service (UK), www.ukas.com

Accreditation Authority Groups
• EA: European Co-operation for Accreditation, “EA is the European network accreditation organizations nationally recognized based in the European geographic sector” (members such as CIA, UKAS, COFRAC). www.european-accreditation.org
• IAF: International Accreditation Forum, www.iaf.nu: IAF is an international association of accreditation organizations for systems in management, product, services, individuals and other programs of this type. The objective of IAF is to ensure that the member national certification organizations only certify competent organizations an establish agreements of mutual recognition among its members. www.iaf.nu

Summary of terms

Certification process
Accreditation institution roles and responsibilities
Organization of the audit led by certification body

Questions

What is first party audit?
What is second party audit?
What is third party audit?
Is there obligation to undergo third party audit?

What are advantages of the third party audit?

Reference sources

[3] ISO 27000 Definitions
9 IT TECHNOLOGY MINIMUM

Study time: 60 min

Objective:

- Knowledge of basic definitions in IT networking
- Knowledge of the basic structure of IT networking
- Overview of the basic components of IT

Explication

In modern telecommunications networks, information is transferred as data. The processing of these data has resulted in the creation of integrated circuits (IC) that are optimized to deal with this form of packet data. Network Processors have specific features or architectures that are provided to enhance and optimize packet processing within these networks.

Some IT terms are used in the ISMS implementation project and thus is necessary to understand them such as:

- Routers, software routers and switches
- Firewalls
- WIFI
- Network monitoring systems
- Servers

These devices mentioned above in connection with passive networking parts (cables, patch pannels etc.) are creating network, LAN or WAN. The word „logic perimeter“ is related to logical boundaries of the ISMS in defined organization.

Summary of terms

- Routers and switches
- Firewalls
- WIFI
- Network monitoring systems
- Servers
Questions

What is function of the firewall?
What is WIFI?
What is cloud?

Reference sources

[3] ISO 27000 Definitions
10 RECOMMENDED REFERENCES

International standards


BSI Guides

- PD 3004:2002 – Guide to the implementation and auditing of BS 7799 controls.
- PD 3005:2002 – Guide on the selection of BS 7799 controls

Internet references

- www.27001.com
- www.bsi-global.com
Normative references used in this course

1. Main standards

ISO 19011:2011, Guidelines for auditing management systems.


2. Other standard references


ISO 17021:2011, Conformity assessment Requirements for bodies providing audit and certification of management systems.

ISO 17024:2003, Conformity assessment General requirements for bodies operating certification of persons.


ISO 22000:2005, Food safety management systems Requirements for any organization in the food chain.


ISO/IEC 27006:2011, Information technology Security techniques Requirements for bodies providing audit and certification of information security management systems.


List of acronyms and abbreviations used in this training

**BCMS:** Business continuity management system

**CERT:** Computer Emergency Response Team

**CobiT:** Control Objectives for Business and related Technology

**DMS:** Document Management System

**EMS:** Environment management system

**GAAS:** Generally Accepted Auditing Standards

**IAF:** International Accreditation Forum

**IFAC:** International Federation of Accountants

**IMS2:** Integrated Implementation Methodology for Management Systems and Standards

**ISMS:** Information security management system

**ISO:** International Standards Organization

**ITIL:** Information Technology Infrastructure Library

**LA:** Lead auditor

**NC:** Non-conformity

**NIST:** National Institute of Standards and Technology

**OHSAS:** Occupational Health and Safety Assessment Series

**OECD:** Organization for Economic Co-operation and Development

**PCI-DSS:** Payment Card Industry Data Security Standard

**PDCA:** Plan-Do-Check-Act

**QMS:** Quality management system

**ROI:** Return on Investment

**ROSI:** Return on Security Investment

**SMS:** Service management system

**SoA:** Statement of applicability