ISO/IEC JTC 1/SC27 N6216

ISO/IEC JTC 1/SC 27/WG1 N16216

REPLACES: N5853

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Text for Working Draft

TITLE: Text for ISO/IEC 5th WD 27003 - Information technology -- Security techniques -- Information security management system implementation guidance

SOURCE: Project Editors (J. Branzell, U. Chandrashekhar, O. Weissmann, S. Yamasaki)

DATE: 2008-03-06

PROJECT: 27003

STATUS: In accordance with resolution 4 (see SC 27 N6306) of the 35th SC27 WG1 Plenary Meeting held in Luzerne (October 2007), this document is being circulated by the convener to the experts of WG1 for **PREPARATION of the next WG1 Meeting in Kyoto April 2008**.

PLEASE NOTE: For comments please use **THE SC 27 TEMPLATE** separately attached to this document.

ACTION: **COM**

DUE DATE:

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
T. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1+112

ISO/IEC TC JTC 1/SC 27 N 6216 Working

Date: 2008-03-06

ISO/IEC WD 27003

ISO/IEC TC JTC 1/SC 27/WG 1

Secretariat: DIN

Information technology — Security techniqes — Information security management system implementation guidance

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Copyright notice

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for **whom** a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27003 was prepared by Technical Committee ISO/TC JTC 1, Subcommittee SC 27, Information technology – Security Techniques.

Introduction

The purpose of this standard is to provide practical guidance for the implementation of an Information Security Management System (ISMS) based on ISO/IEC 27001. ISO/IEC 27001 represents the business outlook for managing information security within an organization. The term information security is based on information being considered as an asset which has an assigned value and hence should have appropriate protection. The protection of valuable information should be aligned with its associated risks, costs, and business acceptance level. Information security aims to:

a) Protect information against a number of different threats (e.g. malfunctioning, loss of information and services, theft, and espionage)
b) Safeguard continuity,
c) Minimize damage; and
d) Facilitate efficiency.

It is the intention of this standard to support the process of information security management which gives the stakeholders the assurance that their information assets, including the information processes, are meeting the level of acceptable risks as defined by the organization.

The phases and process defined in this document provides guidance on the implementation of the organization’s information security management system.
The implementation process described within this standard has been designed to provide the:

a) description of the organization's information security management system, represented as a fundamental set of policies, procedures and controls;

b) basis for continued planning and improvement; and

c) Harmonized framework where consideration is based on the results from business objectives, current situation gap analysis, and risk analysis.

The implementation guidance addresses the Plan-Phase from the Plan- Do- Check- Act life cycle. All necessary steps for the planning as well as the final first implementation of an ISMS are discussed in this document. The subject matter such as Risk Management, or Measurements are covered in other standards within ISMS Family Standards are referenced where appropriate.

This standard does not cover the operation or monitoring of an ISMS. The final implementation of the ISMS is an implementation project on technical and organizational level where normal project management principles and methodologies apply (see ISO Standards on project management).

Adapting to ISO/IEC 27001 should be considered a natural choice for most organizations, both for business and public administration including companies, public bodies, charities etc. An increased acceptance of this standard is critical especially with the use of and dependence on IT, in addition to the threats and risks associated with information processing.

Information Technology— Security Techniques —Information Security Management System Implementation Guidance

1 Scope

This international standard provides practical implementation guidance for planning and structuring the implementation of an information security management system in accordance with ISO/IEC 27001.

This standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) of all sizes and types of business. This document is intended to be used by organizations implementing an information security management system in accordance with ISO/IEC 27001 as well as provide guidance to security professionals.

2 Normative References

- ISO/IEC 27001
- ISO/IEC 27002

3 Terms and definitions

For the purposes of this document, the terms and definitions in the following apply:

- ISO/IEC 27000
- ISO/IEC 27001

4 Overview

This document describes the implementation of an Information Security Management System focusing on the Plan Phase of the PDCA process as described in ISO/IEC 27001. The implementation is a onetime activity and as such described as a project activity in this document. The implementation project is divided into different phases and these phases are also chapters in this document. The entire project is described in a diagram which illustrates the different phases and the outputs. Also each phase has diagrams to illustrate the different working blocks within the phase. As the implementation of an ISMS according to ISMS Family Standards is based on other standards in the series, references to these standards where applicable is also described in the diagrams as useful input.

4.1 Diagrams

4.1.1 Diagram legend

Figure 4.1 provides a legend for the symbols used in the subsequent flow charts in this document. These diagrams provide visual guidance and a process for implementing the ISMS.

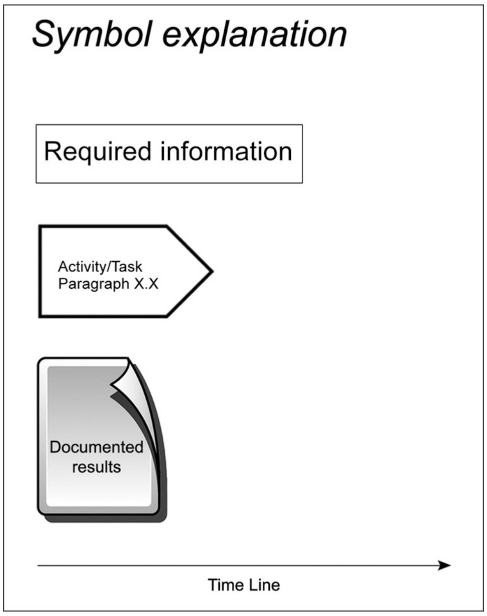


Figure: 4.1 Flow diagram legend

The syntax and semantics for the flow charts in this international standard is based upon the following structural concepts:

- Rectangle Box (Unshaded): The rectangle box provides a description of information. When the information outside the scope of this standard is required for carrying out the tasks it is in a non filled boxes depicted as "Required information" in Figure 4.1. This required information could be reference to other standards such as ISO/IEC 27002.
- Rectangle Box (Shaded): The rectangle box where the information is grey filled and results in a document that is created as part of this standard known as "Documented results".
- Arrow Box: The arrow box represents an activity or work performed. The verbiage that is entered in such a box is a verb or verb phrase, such as "Develop policy", that is descriptive of the function that the box represents.
- Arrowed box can be divided into sub tasks/activities and are then shown as new arrowed boxes. All arrow boxes have a number in the bottom right representing the paragraph of this standard (represented by the "x.x" in figure 4.1).
- The project flow is a sequential flow of activities and is represented by the arrowed boxes. This phase can be done in parallel.
- The arrow in the diagrams represents the time and goes from left to right. The arrow also indicates that certain activities should be done before the next one starts or can be done in parallel.

4.1.2 Disposition and diagrams

All the phases are designated as a chapter. Each chapter has diagrams which illustrate the phase and the main activities within that phase. Each main activity within a phase is then a sub paragraph within the chapter. If there are many subjects in an activity, they are then presented as sub clauses to the paragraph but they will not be represented by a diagram. Other figures or types of diagrams may be included to support the text but may not follow the legend set for the main diagrams, as described in figure 4.1.

Each phase and activity has an objective in the beginning and the content should support the objective.

Additional supportive information such as examples is provided in Annexes.

4.2 The overall implementation diagram of ISMS

Figure 4.2 illustrates the phases of ISMS implementation plan which is the scope of ISO/IEC 27003.

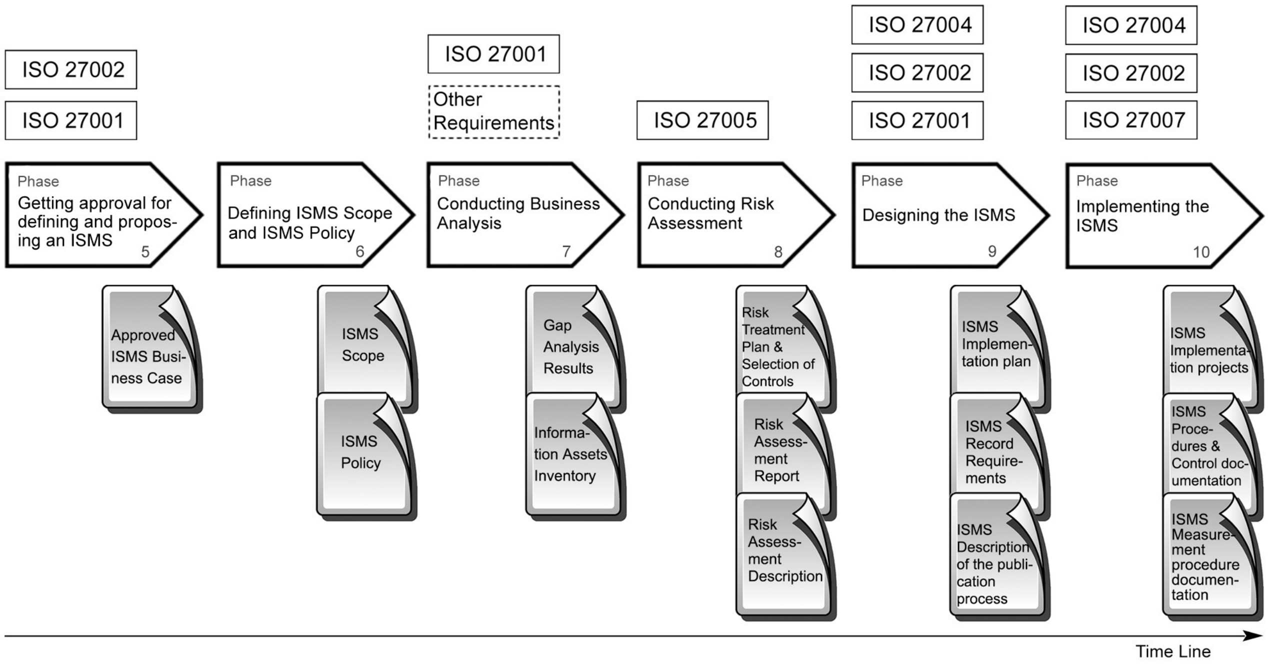

ISO 27002
ISO 27001
ISO 27001
Other Requirements
ISO 27005
ISO 27004
ISO 27002
ISO 27001
ISO 27004
ISO 27002
ISO 27007
Phase
Getting approval for defining and propos-ing an ISMS
5
Phase
Defining ISMS Scope and ISMS Policy
6
Phase
Conducting Business Analysis
7
Phase
Conducting Risk Assessment
8
Phase
Designing the ISMS
9
Phase
Implementing the ISMS
10
Approved ISMS Busi-ness Case
ISMS Scope
ISMS Policy
Gap Analysis Results
Informa-tion Assets Inventory
Risk Treatment Plan & Selection of Controls
Risk Assess-ment Report
Risk Assess-ment Description
ISMS Implemen-tation plan
ISMS Record Require-ments
ISMS Description of the publi-cation process
ISMS Implementa-tion projects
ISMS Proce-dures & Control doc-umentation
ISMS Measure-ment procedure documen-tation
Time Line

Figure 4.2. The ISMS Project Overview & Results of Each Phase

Overview of the objectives linked to each Phase in figure 4.2 is as follows:

- For Ch. 5 “Getting Approval for Defining and Proposing an ISMS” is the objective:
  - Define objectives for implementing an ISMS
  - Get the top management to sign a business case for carrying out an ISMS implementation.

- For Ch. 6 “Defining ISMS Scope and ISMS Policy” are the objectives:
  - Define clear boundaries for the scope of the ISMS
  - Get acceptance for the ISMS Policy

- For Ch. 7 “Conducting Business Analysis” are the objectives:
  - Get a mapping of relevant requirements that will affect the ISMS
  - Get the current information security status within the scope
  - Create an information asset inventory

- For Ch. 8 “Conducting Risk Assessment” are the objectives:
  - Establish and document the information security risks
  - Create a risk treatment plan
  - Create the Selection of controls

- For Ch. 9 “Designing the ISMS” are the objectives:
  - Create an Implementation plan
  - Establish the formal and practical requirements for the ISMS documentation
  - Describe the publication process

- For Ch. 10 “Implementing the ISMS” are the objectives:
    - Execute project for implementing ISMS
    - Set up of ISMS procedures and control documentation
    - Set up of Measurement procedure documentation

4.3 General Information

Organizations may have a management system for information security in place that may affect the ISMS implementation work. In addition, the size of the organization, the complexity of information processes and resources may also affect the implementation work.

For practical purposes, the structure of this document does not consider in detail the different situations that a specific organization faces regarding implementation instead focuses on a general approach to support a step by step procedure where an organization can evaluate each step as it relates to their environment. This chapter provides guidance on the following:

- Overview of the full PDCA on a high level
- Roles and Responsibilities for Information Security
- Considerations for Small and Medium enterprises

4.3.1 Implementation of an ISMS and the PDCA Model

This standard covers the actual implementation phases of an ISMS. The objective of an implementation is to achieve a continual improvement state which is aligned with ISO/IEC27001. For a successful implementation, it is important to understand the full Plan Do Check Act (PDCA) cycle and relationship when executing the implementation phases first time (Plan and Do phases).

Information Security continues to be dynamic and needs to be designed to accommodate change. Every organization is subject to internal and external changes. Many of these changes also affect information security due to changes in the business processes, regulatory environment, tasks, infrastructure, organizational and environmental structures and information technology. Some changes to the prevailing conditions can also occur, for example, the statutory or contractual stipulations, information available, and communications technologies can go through major changes. It is necessary to manage and maintain information security to meet the organization’s business objectives and their risk tolerance.

It is important not just to plan the implementation of business processes and the introduction of a new information system with the agreed information security controls, but to also it should be operated and examined regularly to ensure the effectiveness, and applicability as applied. If vulnerabilities or opportunities for improvements are discovered, the controls should be adapted and improved. The processes should support the planning and implementation of these modifications. When a business process is terminated or components and/or information systems are replaced or shut down, it is also necessary to consider the associated information security issues, such as the withdrawal of authorization or the secure erasure of hard drives.

Figure 4.3 shows a high level ISMS implementation roadmap which illustrates the activities supporting the development and management of an ISMS.

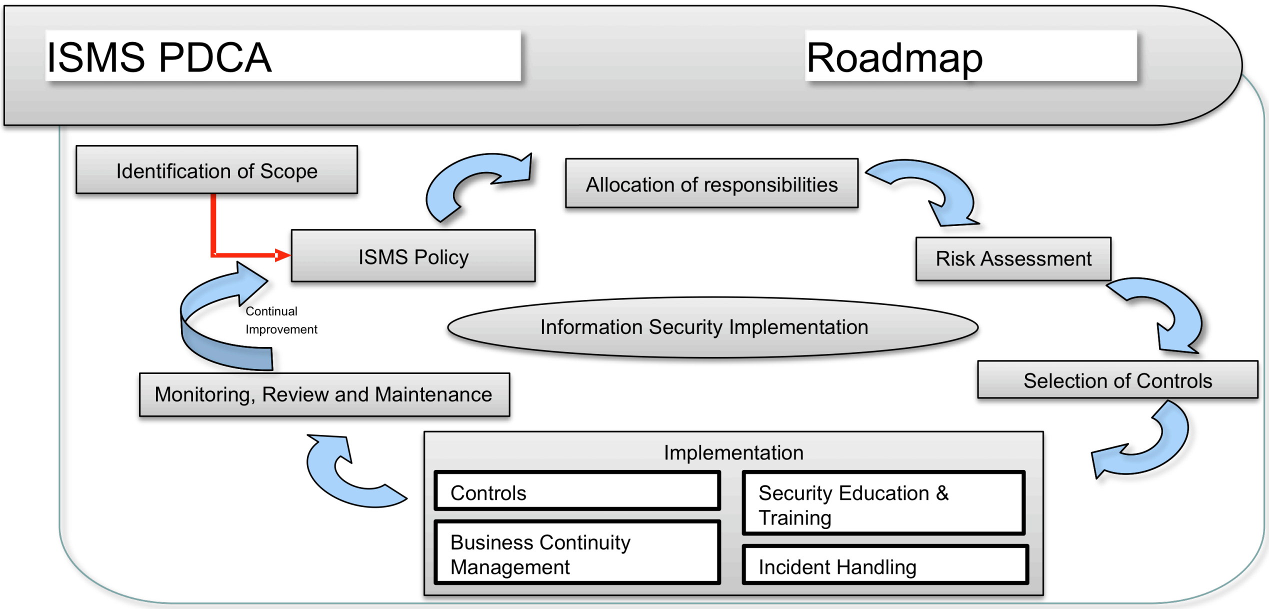

ISMS PDCA
Roadmap
Identification of Scope
ISMS Policy
Allocation of responsibilities
Risk Assessment
Continual Improvement
Information Security Implementation
Selection of Controls
Monitoring, Review and Maintenance
Implementation
Controls
Security Education & Training
Business Continuity Management
Incident Handling

Figure 4.3 ISMS Implementation Roadmap

Both IT systems and the entire information security process have a lifecycle. The dynamics of the information security process can be visualized as a continuous cycle. Within the cycle, the information security process may like other management processes be divided into the following 4 phases:

1. Plan – Prepare for the ISMS
2. Do - Implement the plan and execute the project
3. Check - Performance review and monitor the achievement of objectives
4. Act - Eliminate discovered flaws, weaknesses and continue to optimize and improve the ISMS

Phase 4 describes the immediate elimination of minor flaws. If fundamental or extensive changes are needed, then the cycle begins with revisiting the planning phase. Figure 4.3 depicts a pictorial roadmap of the overall PDCA as it relates to implementing the ISMS. Additional details will not be described in this standard as the focus is on the initial Plan and Do phase for implementing an ISMS.

4.3.2 Examples of Roles for information security

Information security is a wide area that affects the whole organization. As such roles and responsibilities are essential for a successful implementation. As roles and descriptions may vary from organization an understanding of the different roles is fundamental for understanding some of the activities described later in this standard. In order to support this understanding a table below outlines roles and a description. It should be noted that these roles are general and specific description are needed for each individual implementation of an ISMS.

Role	**Responsibilities**
Senior Management (e.g. COO,	The senior management is responsible for vision, strategic decisions and coordinates activities to direct and control the

Role	Responsibilities
CEO, CSO and CFO)	organization.
Chief Information Security Officer	The Chief Information Security Officer has the overall responsibility for the tasks that address security of the information. (and therefore information security).
Information Security Committee (member of)	The committee is responsible for handling the information assets and has a leading role for the ISMS in the organization.
Information Security Planning Team (member of)	The planning team is responsible for operations while the ISMS is being established. The planning team works across departments and resolves conflicts until the ISMS is established.
Process Owner	A "process owner" is the contact person for a business process and specialist application. The process owner is responsible, for example, for delegating tasks and handling information within the business processes to which they have been assigned.
Stakeholder	In the context of the other roles descriptions the Stakeholders concerning information security is primarily here defined for persons/bodies outside the normal operations such as the board, owners (both in terms of organizational owners if the organization is part of a group or a government organization and/or direct owners as share holders in a private company). Other examples of stakeholders could be affiliated companies, clients, suppliers or more public organizations such as governmental financial control agencies or relevant stock exchange if the organization is listed.
System administrator	The system administrator is responsible for an IT system.
IT	The manager of all IT resources (e.g. IT department Manager)
Physical Security	The person responsible for the physical security, e.g. buildings etc., often referred to as a Facility Manger.
Risk Management	The person/persons responsible for the organization’s overall risk evaluation
Legal Advisor	Many information security risks have legal aspects and legal advisor is responsible for taking these into consideration.
Human Resources	The overall responsible for the staff
Archive	All organizations have archives containing vital information. This information needs to be stored for long term that is. The information could be on multiple medias and a person should be responsible for this storage.
Personal Data	If required by national law there may be a person responsible for being the contact for data inspection board or similar official organization handling personal integrity and privacy issues.
System developer	If an organization develops their own information systems, someone has the responsibility for this development

Role	Responsibilities
Specialist / Expert	The specialists and experts, responsible for some operations in an organization should be referred to in terms of their intention about the ISMS matters as it relates to use in their specific fields.
External Consultant	External consultants can give decisions based on their macroscopic points of view of an organization and industry experience. However, consultants may not have the depth knowledge of the business and operations of the organization. organization
Employee / Staff / User	Each employee is equally responsible for maintaining information security in the workplace and in their environment.
Auditor	The auditor is responsible for assessing and evaluating the ISMS.
Trainer	The trainer implements training and awareness programs.
Local IT or IS responsible	In a larger organization there is often somebody in the local organizations that has the role of having responsibility of often IT security matters but may also be information security.
Champion (Influential Person)	This is not a responsible role as such but in a larger organization it may be of great help in the implementing stage to have people who have a deep knowledge about the implementation of an ISMS and can support the understanding and reasons behind the implementation. They may influence the opinion in a positive way and may also be called “Ambassadors”.

Table 4.3.2 Examples of Roles and Responsibilities for Information Security

4.3.3 Considerations for Small and Medium Enterprises (SME)

An implementation project as described in this standard may seem to be complex as it involves more or less the whole organization. It should be mentioned that in practical terms it is more complex for larger organization to implement an ISMS than a smaller one. In a smaller organization there are not as many roles and the actual boundaries for the ISMS are quite obvious to define as well as the control of the information assets may be easier to achieve.

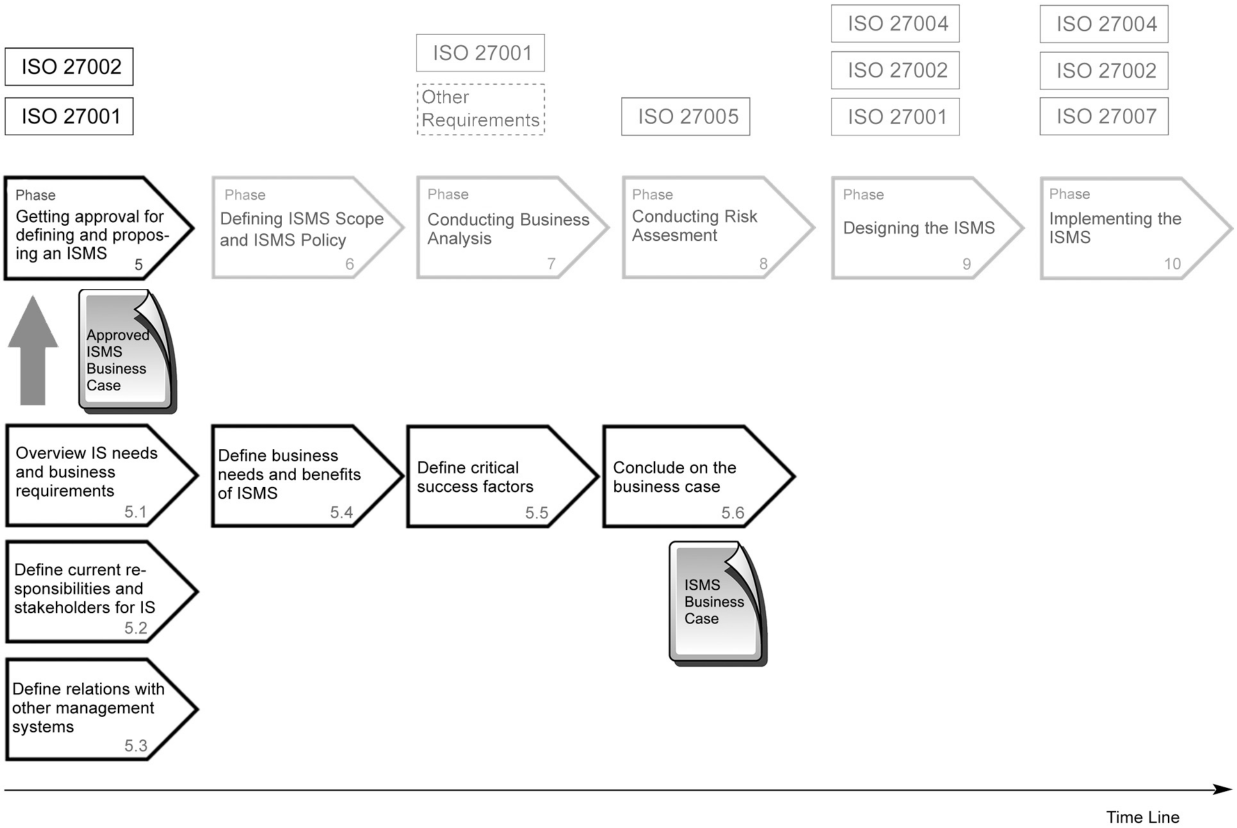
This standard describes activities needed to implement an ISMS especially as the company is medium to large size enterprise. A smaller organization will find that the activities noted in this standard are applicable to them and may be simplified.

The definition of a Small Enterprise is an enterprise with less than 100 employees and the definition of a Medium Enterprise is an enterprise with less than 500 employees. Anything greater than 500 employees is considered to be a large enterprise. Whether it is a SME or large enterprise the complexity and risks are unique for a specific organization and the specific requirements will drive guidance of the implementation.

5 Getting Approval for Defining and Proposing an ISMS

The objectives of the "Getting Approval for Defining and Proposing an ISMS" Phase are:

- Define objectives for implementing an ISMS
- Get top management approval for business case and ISMS implementation.



ISO 27002
ISO 27001
ISO 27001
Other Requirements
ISO 27005
ISO 27004
ISO 27002
ISO 27001
ISO 27004
ISO 27002
ISO 27007
Phase
Getting approval for defining and proposing an ISMS
5
Phase
Defining ISMS Scope and ISMS Policy
6
Phase
Conducting Business Analysis
7
Phase
Conducting Risk Assesment
8
Phase
Designing the ISMS
9
Phase
Implementing the ISMS
10
Approved ISMS Business Case
Overview IS needs and business requirements
5.1
Define business needs and benefits of ISMS
5.4
Define critical success factors
5.5
Conclude on the business case
5.6
ISMS Business Case
Define current responsibilities and stakeholders for IS
5.2
Define relations with other management systems
5.3
Time Line

Figure 5.1 Overview of the Getting Approval for Defining and Proposing an ISMS

5.1 Overview Information Security Needs and Business Requirements

Activity Objective: To define information security needs and business requirements

A key question to answer in order to defining information security needs and business requirements for the ISMS includes determining *"How to reach Compliance and conformity with other regulations and industry references?"*

Organizations choosing to implement an ISMS also ask "*How can an organization implement the ISMS standard and also conform to government laws, sector or industry specific regulation?*" This includes meeting standards, contractual commitments, and an externally-imposed policy, or any other applicable reference. Specific details on how to identify and use extended controls which address industry specific needs in the implementation of the ISMS is discussed as part of the Plan and Do phase. Industry examples of implementation are shared in the Annex to help users of this document better implement an ISMS.

Further motives for implementing an ISMS should be considered by answering questions such as:

- Risk control- how will an ISMS generate better control of information security risks?
- Efficiency – how can an ISMS improve the handling of information security?

- Business advantage – how can an ISMS create a business advantage?

By setting up some basic assumptions as answers to the above questions the activity objective of defining information security needs and business requirements at a high level can be completed . This provides the organization insight on what they will gain from an ISMS implementation.

5.2 Define Current Responsibilities and Stakeholders for Information Security

Activity Objective: To define the roles, their responsibilities, and stakeholders that is critical for implementing an ISMS.

Information security is of particular importance to the whole organization. This organization-wide character of the ISMS makes it necessary to specify particular roles within the organization.
Appropriate tasks must be assigned to each role, and these roles must be served by staff with these skills. This is the only way to ensure that all important aspects are taken into consideration and that all tasks are carried out efficiently and effectively.
The organizational structure required to promote and implement the ISMS is referred to as the information security committee. The number of people dealing with information security, the organizational structure and resources vary with the size, type and structure of the organization. In a smaller organization several roles may be carried out by the same person. However, a chief information security officer should always be appointed as the key person responsible for information security.
At management level the information security role should be assigned to one manager who is the Chief Information Security Officer.
The most important considerations in the definition of roles in information security management are:

- Overall responsibility for the proper and secure provision of tasks (and therefore information security) remains at the management level.
- At least one person (usually the Chief Information Security Officer) is to be appointed to promote and co-ordinate the information security process.
- Each employee is equally responsible for their original task and for maintaining information security in the workplace and in his or her environment.

The following central roles with their appropriate tasks are typical of many organizations and are used in this document:

Role	Responsibilities
Senior Management (e.g. COO, CEO, CSO and CFO)	The senior management is responsible for strategic decisions and coordinates activities to direct and control an organization.
Chief Information Security Officer	The Chief Information Security Officer has the overall responsibility for the proper and secure provision of tasks (and therefore information security).
Information Security Committee (member of)	The committee is responsible for handling the information assets and has a leading role for the ISMS in an organization.
Information Security Planning Team (member of)	The planning team is responsible for operations while the ISMS is being established. The planning team works across boundaries of departments to resolve conflicts during the ISMS implementation.
Process Owner	The "*process owner*" is the contact person for a business process specialist application. This person is responsible for delegating tasks and handling information within the business processes to which they have

	been assigned.
Specialist / Expert	The specialists, are responsible for some operations and are experts in an organization. They should be referred to in terms of their intention about the ISMS matters as it relates to use in their specific fields.
External Consultant	External consultants can give decisions based on their macroscopic points of view of an organization, and industry experience. However, consultants may not have the depth knowledge of the business and operations of the organization. organization
Employee / Staff / User	Each employee is equally responsible maintaining information security in the workplace and in his or her environment.
Auditor	The auditor is responsible for assessing and evaluating the ISMS.
Trainer	The trainer implements training and awareness programs.

Table 5.2 Centralized Roles and Responsibilities for Information Security

At this point in the activity, it is important to have the following defined roles agreed too:

- Chief Information Security Officer (ISO) – there should be one person approved by the management for this task
- Information Security Planning Team – For implementation the CISO above needs a planning team
- Experts - The need of external or internal expertise should be addressed at this stage in order to get the right experience when setting up the planning team.

Stakeholders – The stakeholders should be defined especially to support the management approval process to implement the ISMS.
It is often the case that in order to get proper documentation for an ISMS implementation approval, discussion with other roles are may be needed (reference table 4.3.2) For example, the Process Owners of the critical processes may be a role that needs to be consulted with in order to get documentation for ISMS approval

5.3 Define Relationships with Other Management Systems

Activity Objective: To determine the relationships with other Management Systems required for the ISMS implementation. This is input to the business case.

When considering the implementation of ISO/IEC 27001 the organization should first identify common elements that have already been implemented as a result of the deployment of other management system standards throughout the organization. Once the common elements from the different management systems have been identified, the organization should then proceed to perform a gap analysis between the already implemented management system element(s) and those elements required. After the gap analysis is completed the organization can then proceed to either adapt these existing elements or add new elements to allow compliance with ISO/IEC 27001.

If the organization has already implemented another management systems conformant to standards, then it should consider if it is appropriate to integrate the existing Management System with the ISMS. Some areas to consider in making this decision include:

  - Is the responsibility of the systems under different management teams (e.g. in different subsidiaries or different departments)?
  - How is the presentation material produced and needed (e.g. the existing Management System is on paper and it is desired that the ISMS be built as a hypertext document)?

The common elements of the existing Management System(s) and the proposed ISMS should be identified.

If the all systems are to be integrated then the existing System should be adapted or added to allow compliance with ISO/IEC 27001. If the Systems are not to be integrated consideration should be given to reusing common elements.

5.4 Define Business Needs and Benefits of ISMS

Activity Objective: To define business objectives and the benefits for implementing an ISMS

Basic needs of an ISMS should include a more specified list of considerations regarding information security that the organization faces compared to the high level objectives determined in Section 5.1. Topics the organization needs to address include the following topics:

- Relevant laws that requires information security.
  - What laws are relevant to the organization?
  - Is the organization part of a public global company requiring financial external reporting?
- Relevant contractual (business agreements) that may lead to legal actions due to poor information security.
  - What are the storage requirements?
  - Are there any privacy or quality (e.g. service level agreement-SLA) contractual requirements?
- Relevant industry requirements that requires information security.
  - What sector specific industry requirements apply to the organization?
- Relevant environment requirements that require information security.
  - What kind of protection is needed & against what threats?
  - What are the distinct types of information groupings that need to be protected?
  - What are the distinct types of information activities that need to be protected?

The critical processes that are affected in the organization as a result of answering the above points and the objectives defined in Section 5.1 will be defined.

To determine the benefits the consequences of poor information security should be discussed with the relevant Process Owners of the critical processes. Examples of benefits for each process are:

- Legal Compliance –Ensuring good information security may lead to meeting regional and local laws.
- Contractual Compliance - Ensuring good information security may improve meeting the contractual commitments.
- Industry Standards Compliance – Building industry standards into information security processes and requirements results in addressing compliance to the standards.
- Efficiency –Designing for information security may also result in efficient use of multiple processes for security.

- Business Advantages - Implementing information security may support growth of taking new orders and being able to calculate information security into the cost.
- Risk Control - As the information security is addressed properly it also supports managing risk
- Trust - Implementing an ISMS will support the organization in gaining more trust from the business environment as it will be able to respond more easily to other control organizations (external audits), increase quality response (trust).

Environment understanding: Critical information activities and protecting this type of information supports handling of ongoing threats. This activity should result in confirming or fine tuning the objective in Section 5.1. The final result of this activity is the high level objective for implementing an ISMS, the list of needs, and the benefits linked to the critical processes.

In a smaller organization this activity is often done in conjunction with Section 5.1 and Section 5.5 due to the fact that there are not so many process owners. It is also likely that persons in the Management of a smaller organization are also Process Owners.

5.5 Define Critical Success Factors

Activity Objective: To define critical factors for a successful implementation of an ISMS.

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

a) Information security policy, objectives, and activities that reflect business objectives;
b) An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;
c) Visible support and commitment from all levels of management;
d) A good understanding of the information security requirements, risk assessment, and risk management;
e) Effective marketing of information security to all managers, employees, and other parties to achieve awareness;
f) Distribution of guidance on information security policy and standards to all managers, employees and other parties;
g) Provision to fund information security management activities;
h) Providing appropriate awareness, training, and education;
i) Establishing an effective information security incident management process;
j) Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

For the decision to implement the Information Security Management System, it is important for the implementers to recognize the critical success factors needed for successful ISMS rollout. This section reviews the critical factors needed to successfully implement and realize the benefits of ISMS. The benefits involved in the process of justifying the decisions for implementing the ISMS are related to several issues. Managing these issues and their results are related to the critical success factors. In addition to the critical success factors noted in ISO/IEC 27002, it is important to also consider them as it relates to implementation of the ISMS.
Critical Success factors for implementation of the ISMS are:

a. Management Commitment
b. Governance
c. Financial Considerations

d. Industry/Sector Specific Considerations
e. Risk Considerations
f. Cooperation with other Organizations
g. Recognizing need for change or update
h. Stakeholder involvement

Management Commitment

Management commitment begins with the organization's need to take, decision on the implementation of an ISMS and continues with using the ISMS to help manage and grow the business.

Management commitment often depends on ISMS objectives being described in business terms that are meaningful to the management in question. It is thus important to be able to translate information security objectives to business objectives, which are relevant to management.

Management commitment can easily be lost when implementation or operational problems arise. It can also be lost if management priorities shift from information security to other business priorities.

Maintenance of management commitment is critically dependent on keeping management informed of the status of ISMS activity and ensuring that management is actively involved in associated decision-making.

Management should demonstrate through their actions commitment to establish, implement, and operate effective ISMS.

Critical success factors that show management commitment include:

- Periodic executive reviews and action plan that ties the ISMS success to the business
- Management approval and monitoring of ISMS implementation
- Separate budget allocated for ISMS implementation
- Creation of an Information Management Security Forum which includes the key stakeholders of the organization where the process owners and managers share operational issues
- Review of residual risks that are (or expected to be) below the acceptable risk level and are above the acceptable criteria but management decides not to take any actions for.
- Adequate and skilled resources for ISMS implementation.

Governance

Governance is an important and critical success factor to implement the ISMS. In particular, the organization should have clear understanding of the roles, responsibilities, stakeholders, their compliance with legal requirements and the relationship to the ISMS implementation. Governance here is referred to as a set of processes, policies, laws, and institutions in which the organization is directed, administered or controlled. It includes defining the goals of the corporation, knowing the stakeholders, and their relationships to the ISMS.

The tasks and duties regarding information security can be summarized in the following points:

- Responsibility for information security

  The management of every organization is responsible for the correct operation of the organization in accordance with their objectives. They are also responsible for assuring information security internal and external to their organization. Depending on the country and type of organization, there can be regulations and various laws that need to be understood. The management should clearly demonstrate its commitment to their responsibility and explain the importance of information security to all staff members.

  If an ISMS is created for a part of the whole organization then this success factor only applies to the area of their delegated responsibility.

- Integrating information security

  Information security should be considered and integrated as appropriate in all the organization's business activities including third party engagement in which information is processed and information technology is utilised. This means for example that security requirements should be considered when procuring IT as well as when designing business processes, training staff members.
- Managing and maintaining information security

  Management should ensure that responsibilities and ownership of Information Security (IS) tasks are allocated appropriately to knowledgeable personnel and accepted by the same for all IS related strands of work. This would include:
  - Developing, implementing and maintaining the IS Strategy
  - Risk identification, risk assessment, and risk management
  - Provision of adequate resources to support and manage IS functions
- Setting achievable goals

  The objectives and goals of activities within the ISMS should have a well-defined and documented relationship with the primary objectives of the organization. It is thus important to clearly describe how security objectives and goals support the achievement of the main goals and objectives of the business. This set of relationships should be credible and the resultant security activities should be realistic and achievable.
- Information security cost benefit analysis

  It is essential to understand the dependence of the business processes, assets, and tasks upon information processing so that appropriate information security controls can be selected to manage and maintain the implementation of ISMS.
- The function of role model

  The management should lead by example, when it comes to information security. This requires, among other things, that the management also complies with all the specified security regulations and takes part in training events.

Financial Considerations

Financial considerations are also considered to be a critical success factor for implementation of an ISMS. In particular, the organization should have mechanisms in place to monitor:

- Return on investment as the ISMS is implemented and managed
- Cost of not meeting the business's security strategy or failure to maintain the ISMS

Industry/Sector Specific Considerations

Critical success factor for ISMS implementation should also include looking at the specific industry or sector standards, and guidelines associated with the enterprise's business. It is important to recognize the regulatory environment and how the implementation of ISMS needs to support the business operations. For additional information related to sector specific documents and the roadmap of ISMS Family Standards refer to ISO/IEC 27000.

Risk Considerations

Risk considerations are a critical success factor. Information on the risks within scope of an ISMS, and appropriate measures to reduce the risks to acceptable levels should be complied and approved by management.

At this stage an evaluation of how the information security risks will be handled in relation to existing risk management processes and possible gains that can be achieved should be noted.

Cooperation within the Organization and with other Organizations

Cooperation within and across other organizations is an important critical success factor for ISMS implementation. In particular, the following should be reviewed and addressed:

- Synergy with existing security policies, guidelines, and instructions
- Linkages across organizations and success criteria related to ISMS
- Security requirements needed to meet stakeholder concerns
- Documentation form of the ISMS – paper, electronic documents or hypertext: how the ISMS is to be linked to other necessary documents etc.

Recognizing Need for Change or Updates

Another important success factor is the ability to recognize when a change or update is needed in the ISMS.

Stakeholder involvement

The different stakeholders as defined and their view on a successful ISMS should be considered. These views could be:

- Reports on information security performance (including the results of the implementation project)
- Costs for information security
- Reached benefits for information security

Further the Stakeholders involvement should be addressed as their involvement may support the actual implementation in terms of:

- As part of a steering committee for the ISMS implementation
- Demonstrating their interest by addressing the importance of information security in other operational activities

5.6 Conclude on the Business Case

Activity Objective: To complete ISMS implementation business case and gain approval by top management

The results from the previous activities should be gathered in a document for management approval as a business case. This should include estimated time plan and resources needed for the main activities noted in Chapters 6 to 9 of this standard. In the business case at this stage it is not possible to specify them in detail as many factors are not yet known, rather an estimate should be given for the future implementing activities.
This document serves both as base for the project, but also ensures management commitment and approval of resources needed for the ISMS implementation

The business case for implementing an ISMS could consist of the following subjects:

- High level objective
- Specific objectives
- Critical processes involved
- Defined roles and responsibilities
- Implementation organization

- Implementation considerations
- Assumed time plan (may be divided in the phases as set forth in this standard)
- Assumed cost frame
- Defined critical success factors

After the management approval a Project plan should be specified including relevant activities of phases in chapter 6-9 set forth in this standard. Chapter 10 covers the implementation of controls.

6 Defining ISMS Scope and ISMS Policy

It is assumed at this point the business case for ISMS has been written and approved. Now the details of scope definition and ISMS policy should be defined.

The objectives of the “Defining ISMS Scope and ISMS Policy” phase are:

- o Define clear boundaries for the scope of the ISMS
- o Get acceptance for the ISMS Policy

To achieve the objectives of this phase it is important to obtain the supporting information that helps in the design of the organization’s information security management system, its boundaries, and its relevant processes.

1. Information is collected for the establishment of the ISMS
   - o Analyze the situation of an organization’s business to define the scope and boundaries of the ISMS its policy. The supporting information from the business points of view to establish the ISMS should be collected throughout this Phase. These include information from:
     - ▪ Critical business processes
     - ▪ Setup of the physical environment
     - ▪ Organization borders

2. Define the scope and boundaries of the ISMS
   - o Define the scope and boundaries of the ISMS according to the decisions of the management and the information collected throughout the analysis from above

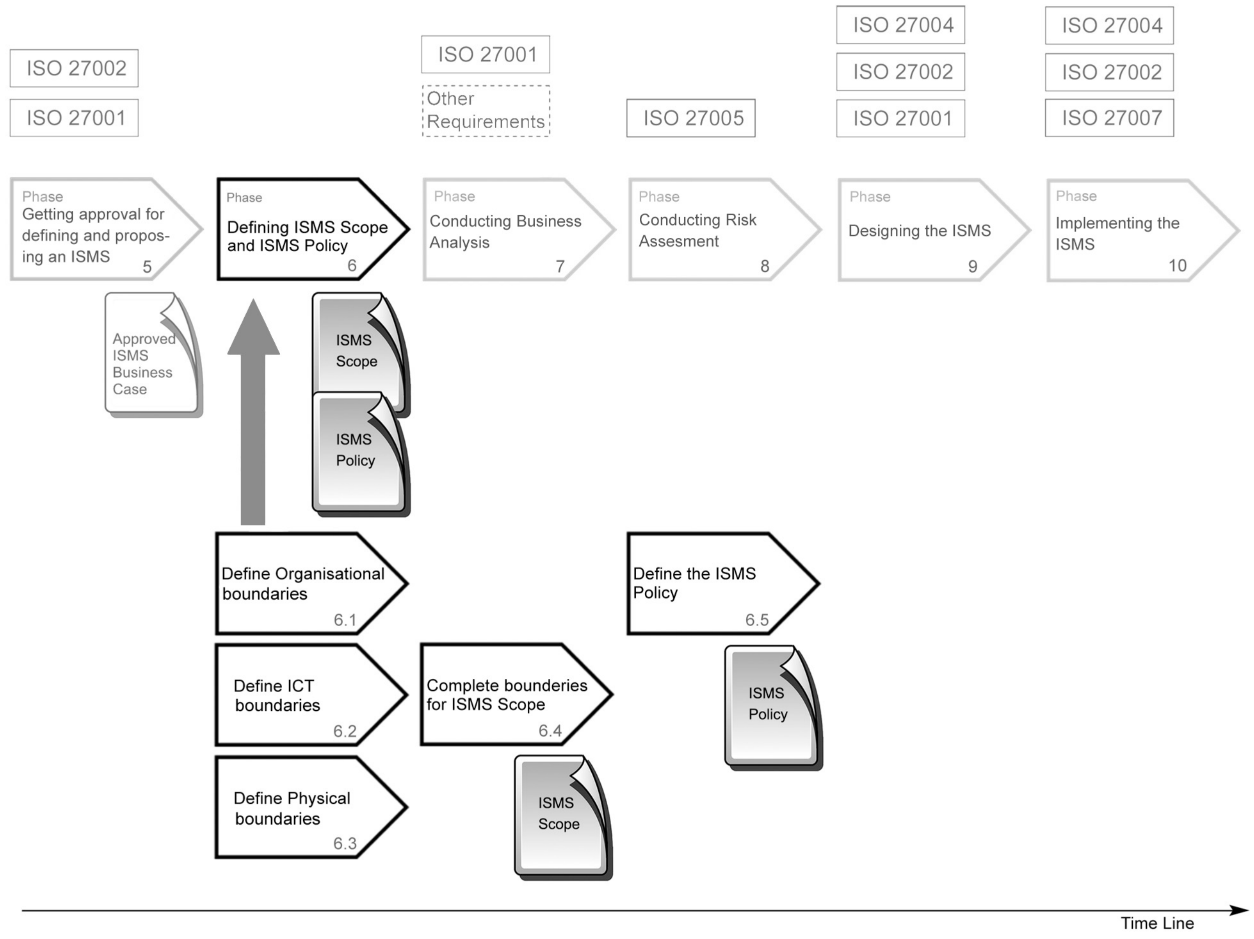


Figure 6.1. Overview of the Definition of ISMS Scope and ISMS Policy Phase

To build an effective management system in the organization the appropriate scope of the ISMS should be determined by considering critical information assets for the target businesses. It is also important to have a common terminology and systematic framework, for identifying information assets and assessing viable security mechanisms, in order to ensure that critical business areas are included in the scope. A common framework enables ease of communication and fosters consistent understanding through all the phases of the implementation.
It is also possible to define the entire enterprise as a scope of the ISMS, or a part of business division as a scope of the ISMS. Like the case of "services" provided to customers, a cross-functional management system (an entire division or part of a division) can be made a scope of the ISMS, regarding the management systems of some divisions like an organizational structure.
When the scope of the ISMS is defined, it is important that it has one complete management system and that its boundaries are clear enough to be explained logically. The ISMS scope and boundaries should be reasonably defined to generate the following;

The ISMS scope should contain:

a. Characteristics of the organization's business (specifications of the businesses, services, the assets, and the range of the responsibility of each asset)
b. List of the critical business processes
c. Documents of the organization's structure
d. Map of the site and the layouts of the floors etc.
e. Configurations of equipments and networks
f. List of the assets

The effort to implement the ISMS is dependent on the scope size. This can also affect all the activities for maintaining the information security of applicable objects, including controls, managing operations, and tasks such as identifying information assets and risk assessment. Anything excluded from the ISMS scope, should be explained.

6.1 Define Organizational Boundaries

Activity objective: To define the organizational boundaries for the ISMS

One approach how to define organizational boundaries is, to identify the areas of responsibility which are non-overlapping within an organization. These areas of responsibility which contain critical business assets or are affected by critical business processes should then be selected as the area of the organization which is under control of the ISMS. The following need to be considered when choosing this path:

- The parties which are participating in the Security Forum of the ISMS Management will be impacted
- The management in charge or responsible for the ISMS must be the one who is ultimately responsible for all the areas of responsibility affected (e.g. the upper nodes of an organization's structure)

6.2 Define Information Communication Technology Boundaries

Activity objective: To define the boundaries of the Information and Communication Technology aspects that should be covered by the ISMS.

The definition of the ICT Boundaries can be identified through an information system (not an IT-System) approach. All information systems which process or transports critical business information, assets, or are critical to the information system should included into the ISMS scope. The following should be considered:

- Information systems may cross organizational borders which should be integrated and communicated.
- When information systems cross the organizational borders or national borders the following must be considered:
  - Culture
  - Local regulations
  - Accountability for key responsibilities
  - Technical constraints (e.g. available bandwidth, availability of service etc.)

6.3 Define Physical Boundaries

Activity objective: To define the Physical boundaries aspects that the ISMS.

The definition of physical boundaries consists of identifying premises, locations or facilities within an organization which should be part of the ISMS. It is more complex to deal with information systems which cross physical borders that need:

- Mobile access
- Remote facilities
- Subscribed third party service
- Wireless networks

These issues should be addressed by defining proper interfaces and service levels.

6.4 Complete Boundaries for ISMS Scope

Activity objective: To determine the boundaries the ISMS.

When defining the scope of an ISMS this can be combined in many ways, e.g. a physical location like a premise, datacenter or office is selected and selected critical processes which extend this physical location should be taken into the scope. This could for example be a mobile access to an information system.

6.5 Define ISMS Policy

Activity Objective: To define the ISMS policy.

The ISMS policy is required in addition to the security policy as ISMS policy provides the basic concepts for information security management in an organization. The policy document provides also a declaration of intent, stating that the organization is liable for information security requirements.

Approach

To define an ISMS Policy, the organization should determine the following:

a. General orientations and principles related to information security
b. Organizational environment and items to consider for risk management
c. Criteria for assessing risk structure of risk management
d. Business requirements
e. Legal or regulatory requirements
f. Contractual security obligations

An organization should set the objectives, framework of the ISMS, principals of the activities related to information security. In addition, it is also important to define the meaning of risk management (employment, Business Continuity, safety, Internal Control etc.) in the ISMS phases.

The process to define the ISMS policy is as follows.

a. Establish the general focus and guide to action related to information security
b. Consider the business requirements, legal or regulatory requirements, and contractual security obligations
c. Prepare the environment for the organization and risk management
d. Establish the criteria for evaluating risks and defining a risk assessment structure
e. Obtain endorsement from management

In conclusion, to perform this phase, the following key steps should be addressed through the three steps, collection of an organization's information, definition of the ISMS scope, and ISMS policy:

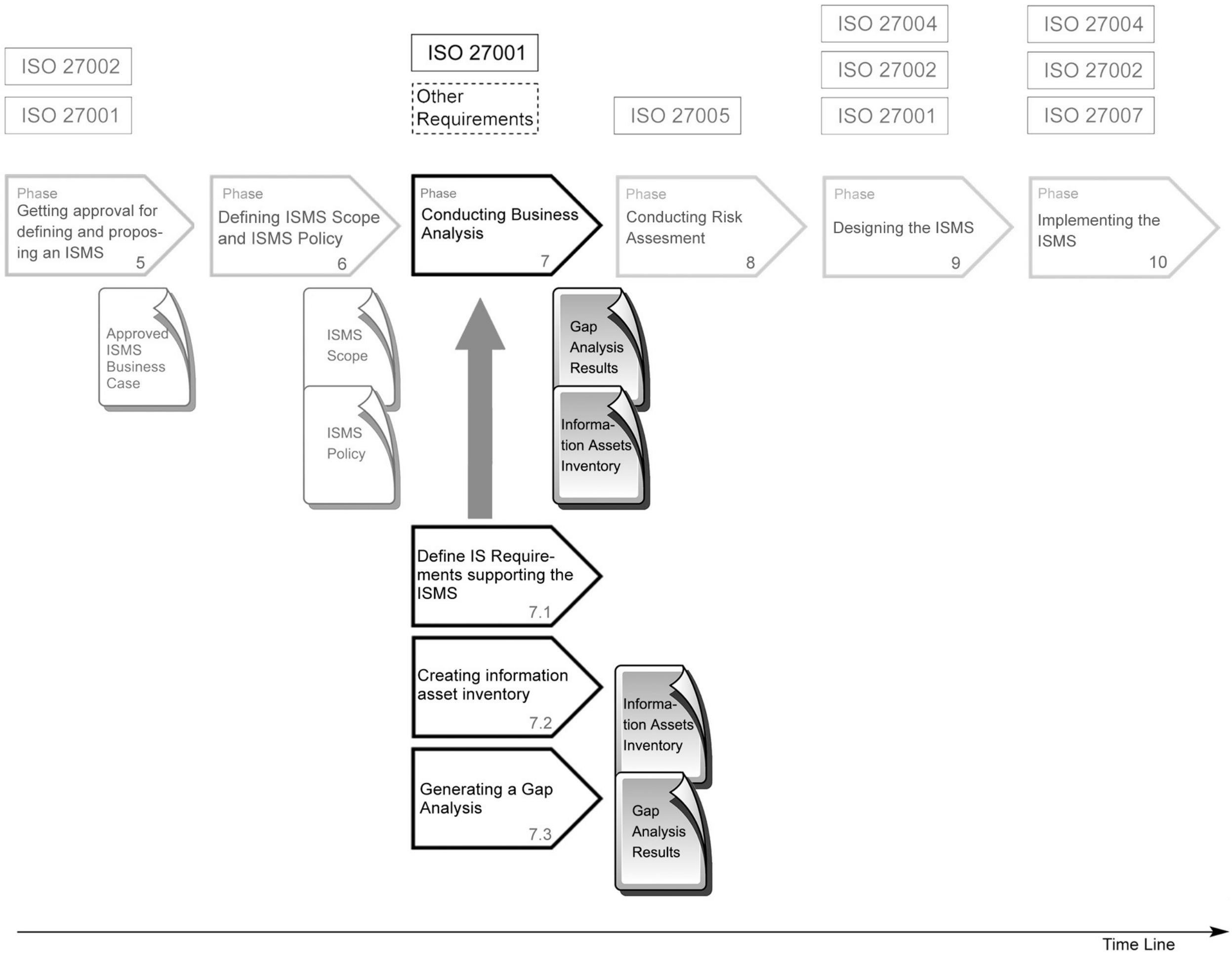
a. Identification of all essential requirements (e.g. laws, ordinances, industry standards, customer and supplier agreements, sector specific industry requirements, insurance conditions etc.) should be undertaken
b. Mapping of regulations, standards etc. in order to set the requirements for the ISMS
c. Organization structure of the ISMS scope and boundaries should be identified.
d. Main processes and functions of the organization should be identified and illustrated from a "executive view"
e. Essential information assets are identified
f. Significance of the information assets are expressed both in economical and human capital terms, (For further information about Information Asset valuation see ISO/IEC 27005.)
g. Visions of the organization are identified
h. Determine the effect of identified visions on future information processing requirements
i. Understand and develop the current forms of information processing, system applications, communication networks, location of activities and IT resources, etc.,
j. Records are maintained
k. Complete comprehensive level of cross-checking between all participants
l. Results

7 Conducting Business Analysis

At this point, the ISMS business case has been approved as well as the ISMS scope and ISMS policy has been defined.

The objectives of the “Conducting Business Analysis” phase are:

- Obtain a mapping of relevant requirements to be supported by the ISMS
- Create an information asset inventory
- Determine the current information security status for the defined scope (gap analysis)



ISO 27002
ISO 27001
ISO 27001
Other Requirements
ISO 27005
ISO 27004
ISO 27002
ISO 27001
ISO 27004
ISO 27002
ISO 27007
Phase Getting approval for defining and proposing an ISMS 5
Phase Defining ISMS Scope and ISMS Policy 6
Phase Conducting Business Analysis 7
Phase Conducting Risk Assesment 8
Phase Designing the ISMS 9
Phase Implementing the ISMS 10
Approved ISMS Business Case
ISMS Scope
ISMS Policy
Gap Analysis Results
Information Assets Inventory
Define IS Requirements supporting the ISMS 7.1
Creating information asset inventory 7.2
Generating a Gap Analysis 7.3
Information Assets Inventory
Gap Analysis Results
Time Line

Figure 7.1. Overview of the Business Analysis phase

The information collected through the business analysis should:

a. Provide management with a starting point (i.e. correct basic data)

b. Identify and document conditions for the implementation

c. Provide a clear and well-established understanding of the organization’s facilities

d. Consider the particular circumstances and situation of the organization

e. Identify an optimum level of protection for the information

f. Determine the compilation of information needed to be to be supported for all or part of an enterprise within the proposed scope of the implementation.

The business analysis can be conducted for the scope chosen for an enterprise, but should at least address the proposed scope defined for the information security management system.

7.1 Defining Information Security Requirements Supporting the ISMS

Activity Objective: To establish the information security requirements for the ISMS

Approach

Analyze the situation of the organization's business and collect the supporting information from the business points of view to establish the ISMS.

The supporting information of the ISMS should be collected in the first step of the business analysis. For each business process and specialist task, a decision needs to be made in terms of how critical the information is, i.e. the level of protection required. A variety of internal conditions may affect information security, and these should be determined. At this early stage it is not important to describe the information technology in detail. There should be a basic summary of the information analyzed for a business process and the associated IT applications and systems.

The analysis of business processes provides statements about the effects of information security incidents on the business activity. In many cases it is adequate to work with a very basic description of the business processes.

The following questions should be answered:

a. Which business processes depend on functional information technology, i.e. Information Technology that meets the requirements and operates properly? Identification of all essential requirements (e.g. laws, ordinances, industry standards, customer and supplier agreements, insurance conditions etc.) should be undertaken.
b. Mapping of regulations, standards etc. in order to set the requirements for the ISMS.
c. Which information is processed for these business processes?
d. Which information is particularly important and therefore worthy of protection in terms of confidentiality, integrity and availability (e.g. board minutes, physical contracts, personal data, customer data, strategic information, secrets such as development plans, patents, procedural descriptions)?
e. What external conditions can affect the information security (e.g. statutory provisions, environmental influences, customer, supplier and partner requirements, and industry-specific security standards)?
m. Organization structure of the ISMS scope and boundaries should be identified.
n. Main processes and functions of the organization should be identified and illustrated from a "executive view"
o. Essential information assets are identified
p. Significance the information assets are expressed both in economical and human capital terms, (For further information about Information Asset valuation see of ISO/IEC 27005.)
q. Visions of the organization are identified
r. Determine the effect of identified visions on future information processing requirements
s. Understand and develop the current forms of information processing, system applications, communication networks, location of activities and IT resources, etc.,
t. Records are maintained
u. Complete comprehensive level of cross-checking between all participants
v. Results

Some of the intermediate material produced in this process should include:

a. Identification of the main processes, functions, location, information systems, communication networks,
b. Information assets (identified elements) of the organization
c. Critical processes/assets classified
d. Non-critical prioritized areas (non critical areas are not considered further as they are deemed to be an acceptable risk to the organization)
e. Organization's requirements addressing confidentiality, availability, and integrity
f. Documenting any known vulnerabilities

7.2 Creating Information Assets Inventory

Activity Objective: To establish an inventory of assets to be supported by information security management system.

To create an asset inventory several paths can be followed. One approach is to follow the information classification scheme. Using this approach, assets that process, operate or transport classified information with a certain classification level can be inserted into the asset list.
Another option is to break down relevant business processes into components and assets critical to them and generate an asset list out of the relevant components. Breaking down business processes can be a difficult task especially, if the business processes have a certain complexity.

7.3 Generating a Gap Analysis

Activity Objective: To establish the status of information security of the organization compared to desired business objectives. This results in a gap analysis.

Approach:
The next step in this Phase is known as the Gap analysis which identifies the existing level of information security (i.e. the organization current procedures of handling protection of information) in order to secure the continuity of the organization from an overall perspective. Figure 7.3 shows the flow diagram for the Gap Analysis.

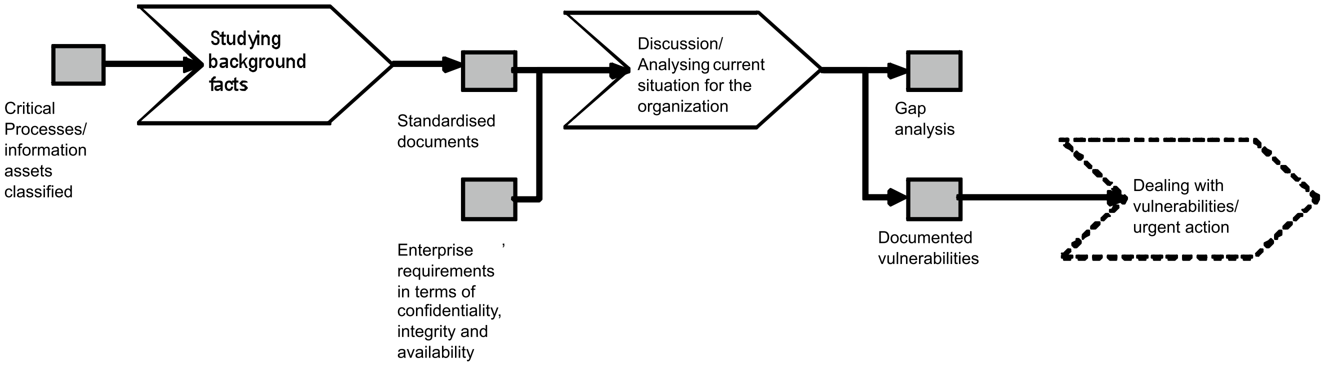

Critical Processes/ information assets classified
Studying background facts
Standardised documents
Enterprise requirements in terms of confidentiality, integrity and availability
Discussion/ Analysing current situation for the organization
Gap analysis
Documented vulnerabilities
Dealing with vulnerabilities/ urgent action

Figure 7.3 Overview of the flow and outcome of a Gap Analysis

In order to continue the work of describing the management system, information security should have the correct orientation and support. The results of the Gap Analysis together with the objectives of the organization are often an important part of the incentive for future work on information security.

The fundamental purpose of the gap analysis is to provide information supporting the description required for the management system in the form of policy and guidelines. It is of course necessary to make sure that the identified deficiencies are dealt with in parallel via a prioritized action plan. All parties involved should be familiar with the results of the business analysis, standards documents, and have access to suitable management personnel.

The Gap Analysis should be performed by an internal or external resource with an independent status in relation to the organization.

Participation in the Gap Analysis should include individuals who possess a strong knowledge of what is the current environment, conditions, and what is relevant in terms of information security. These individuals should be selected to represent a broad spectrum across the organization and include:

a) line managers (e.g. business unit heads)

b) process owners (i.e. representing important business areas)

c) Other individuals who possess the strong knowledge of what is the current environment, conditions, and what is relevant in terms of information security.

To successfully execute the Gap Analysis, it is important to:

a) Identify and list the relevant standards and standardized documents to the organization
b) Use these as reference documents and a rough estimation can be made of the organization's current requirements concerning its level of information security.

The prioritization made in connection with the business analysis constitutes the foundation for which security precautions and checks should be considered.

A method for conducting the Gap Analysis is as follows:

a) Select the important processes and process steps concerning the pattern of requirements (availability, integrity and confidentiality).

b) Create a comprehensive flow chart covering the organization’s main processes including infrastructure (logical and technical), if this is not already present or performed during the business analysis.

c) Analyze with suitable key personal in the organization in workshop form

d) Discuss and analyze the organization’s current situation in relation to the pattern of requirements. Which processes are critical, how well do they currently work with regard to availability, integrity and confidentiality? (The results are used in later work with risk assessment.)

e) Deficiencies identified during the business analysis together with available results from the risk and vulnerability analysis provide guidance for the orientation of policy and guidelines.

f) Complete and documenting the current status.

The results of this analysis are ideally presented to the organization’s management. Deficiencies of a more urgent nature are passed over to the organization for prioritization and the necessary remedial action

The results of the Gap Analysis produce a description of the organization’s actual information security status.

8 Conducting Risk Assessment

At this point, the ISMS business case has been approved, the ISMS scope and ISMS policy has been defined and information assets are known as well as the gap analysis results.

The objectives of the "Conducting Risk Assessment" phase are:

- Establish and document the information security risks
- Create a risk treatment plan
- Create the Selection of controls

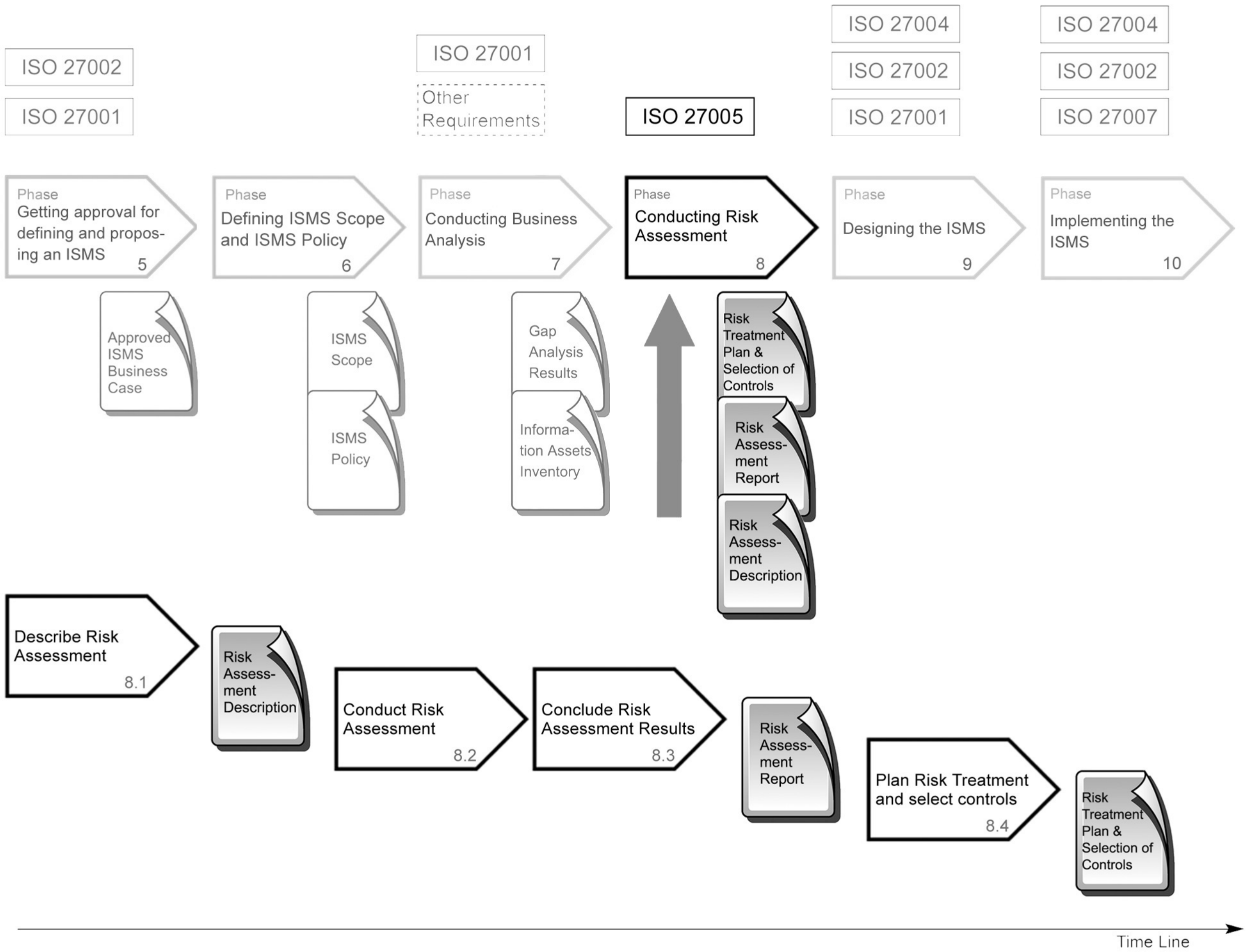

ISO 27002
ISO 27001
ISO 27001
Other Requirements
ISO 27005
ISO 27004
ISO 27002
ISO 27001
ISO 27004
ISO 27002
ISO 27007
Phase
Getting approval for defining and proposing an ISMS
5
Phase
Defining ISMS Scope and ISMS Policy
6
Phase
Conducting Business Analysis
7
Phase
Conducting Risk Assessment
8
Phase
Designing the ISMS
9
Phase
Implementing the ISMS
10
Approved ISMS Business Case
ISMS Scope
ISMS Policy
Gap Analysis Results
Information Assets Inventory
Risk Treatment Plan & Selection of Controls
Risk Assessment Report
Risk Assessment Description
Describe Risk Assessment
8.1
Risk Assessment Description
Conduct Risk Assessment
8.2
Conclude Risk Assessment Results
8.3
Risk Assessment Report
Plan Risk Treatment and select controls
8.4
Risk Treatment Plan & Selection of Controls
Time Line

Figure 8.1. Overview of the Risk Assessment Phase

8.1 Risk Assessment Description

Activity Objective: To determine risks, document the risk treatment plan, and create a selection of controls.

The Risk Assessment defines the step where all operational business risks within the scope are identified. An estimate on the likelihood of an incident and its impact will be made. The risk then often is a cross product of the likelihood and impact (e.g. Risk = Likelihood * Impact) based on management decision on risk tolerance, the level of risks are noted in the risk assessment description.

8.2 Conduct Risk Assessment

Activity Objective: To define the information security risks.

Approach

The next step of this Phase is known as the Risk Assessment. Knowing the risks of implementing the ISMS based on the business vs. gap analysis results is critical to the success of ISMS implementation. A detailed approach on how to assess risks is given in ISO/IEC 27005 and ISO/IEC 31000.

Risk assessment makes it possible to understand the critical issues related to the information assets that an organization possesses especially as it relates to the current situation vs. the desired operations view. Possible damage to the business activities and tasks of an institution due to information security incidents should be analyzed and assessed.

To fulfill the information security objectives and achieve the aspired level of information security, an understanding should first be developed on how information security risks can threaten the fulfillment of tasks and business processes.

In particular, some key questions are:

a. What are the critical gaps/vulnerabilities from business and gap analysis?
b. What are the potential threats?
c. What is the likelihood of these threats?
d. How much the assets are affected when the threats occur?
e. What is management's minimum acceptance level?

It is important that the Business Analysis and Gap Analysis have been performed in order to form the basis for the risk assessment. The analysis should provide guidance towards formulating the required security level in the security policy by means of an overall risk assessment.

Information security risk assessment procedures should be in place. These procedures may cover matters such as:

a. description of risk assessment methodologies
b. risk assessment (Risk identification, Risk estimation)
c. risk evaluation
d. risk treatment option decision
e. risk acceptance decisions,
f. Risk recording and reporting.

The overall analysis can be conducted effectively in workshop form with representatives for different sections of the organization who have the capacity to observe the business impact without too much detail and specialization. One experienced individual, external or internal, should be appointed to maintain the workshop and make sure that the work is advanced.

A method for risk assessment is an integral part of every information security management system. In order to be able to identify a risk, the key threats scenarios should be ascertained from a potential of impact to the system as well as the probability of occurring.

Risk assessment methods that come into question are depending on the application, organizational boundary conditions, type of industry and level of information security that is aspired to. The information security management should select a method that is appropriate for the type and size of the organization. For further guidance on risk as it relates to the ISMS, refer to ISO/IEC 27005 or ISO/IEC 31000.

Participation in the risk assessment should include individuals who possess a strong knowledge of the organization's objectives, and security understanding (e.g. good insight into what is currently relevant in terms of threats to the organization's objectives. These individuals should be selected to represent a broad spectrum across the organization and include:

a. senior management (e.g. COO, CEO, CSO and CFO)
b. line managers (e.g. business unit heads)
c. business process owners (i.e. representing important business areas) and
d. Other individuals who possess a strong knowledge of the organization objectives and share security understanding (e.g. good insight into what is currently relevant in terms of threats to the organization's objectives).

The in-depth risk assessment takes place with representatives who have competence in the area in question. However, it is important that both business and technical competencies are represented. The fundamental objectives and tasks of an organization are the basis for all business processes, specialist procedures and activities, including information security. Information and communications technology should provide meaningful support to an organization's objectives and business processes. Therefore, in order to establish an appropriate information security management system, each organization should consider its most important business processes and specialist tasks as well as its dependence on information. It is important to have the resources to provide guidance towards formulating the acceptable tolerance level in the information security management policy by means of an overall risk assessment. Overall threats and risks for the entire organization are identified in this risk assessment.

An in-depth risk assessment can help identify the acceptable tolerance including understanding the set of regulations, which forms the objective of the work in terms of guidelines and instructions. The management may require an in-depth risk assessment, if it is noted that the overall risk assessment does not cover the entire organization or if one or more processes have not been satisfactorily highlighted, or those obvious risks have not been documented.
The following issues should be reviewed and the associated risk considered when developing the ISMS:

a. Business objectives of the organization
b. Security objectives of the organization
c. Legal requirements and regulations
d. Customer requirements and existing contracts
e. Internal prevailing conditions (e.g. organization-wide risk management or IT infrastructure)
f. (IT-assisted) business processes and tasks
g. Global threats to the business activities through information security risks (e.g. damage to the image, violation of laws, infringement of contractual obligations and theft of research results).

The results of the Risk assessment include the following:

a. Documented overall risk assessment.

b. Requirement for in-depth risk assessment for critical areas.

c. Documented in-depth risk assessment.

It is important to obtain management approval of the proposed residual risks and authorization to implement and operate an ISMS. Management should check and approve the risk retention appropriately, when residual risks are (or are planned to be) below the acceptance risk level. Prior to this management has approved the goal of implementing and operating the ISMS.

8.3 Conclude Risk Assessment results

Activity Objective: Is To complete the information and findings from risk assessment so risks can be evaluated.

For guidance on a Risk Assessment report refer to ISO/IEC 27005 or ISO/IEC 31000.

8.4 Plan Risk Treatment and Select Controls

Activity Objective: To plan how risks should be treated and select appropriate controls for information security.

Among the risks identified are those risks which need to be treated. According to ISO/IEC 27005 and ISO/IEC 31000 there are four ways to treat risks. Within the ISMS the focus lies on the effort to reduce the likelihood of the risks. In certain rare cases efforts are taken to reduce the impact as well. The focus should be on the reduction of the likelihood of an event to happen. This takes place within the risk treatment plan where appropriate controls are selected e.g. from ISO/IEC 27002 to counter a certain risk. The selection of controls is documented. (Note that if an organization is aiming for certification against ISO/IEC 27001 this should be documented within the Statement of Applicability (SOA). The SOA is a mandatory document if a certification is aimed at.)

Approach

This step of the Phase is known as the selection of controls (if certification this refers to as the Statement of Applicability). The selection of controls is based on risk treatment documenting i the applicability of the appropriate controls for the implementation of the ISMS. Figure 8.2 gives an overview of the selection of controls.

The activity supports the control objectives and controls which are relevant and applicable to the organization’s information security management based on the results and conclusions of business, gap analysis, and risk assessment processes. (If the organization is considering certifying itself according to the standard ISO/IEC 27001 this is a mandatory activity in the form of Statement of Applicability). Formulating a risk treatment plan supports the identification of the appropriate countermeasures and management actions needed to achieve the control objectives and controls selected and determined by risk treatment options. For further guidance on risk, refer to ISO/IEC 27005 or ISO/IEC 31000.

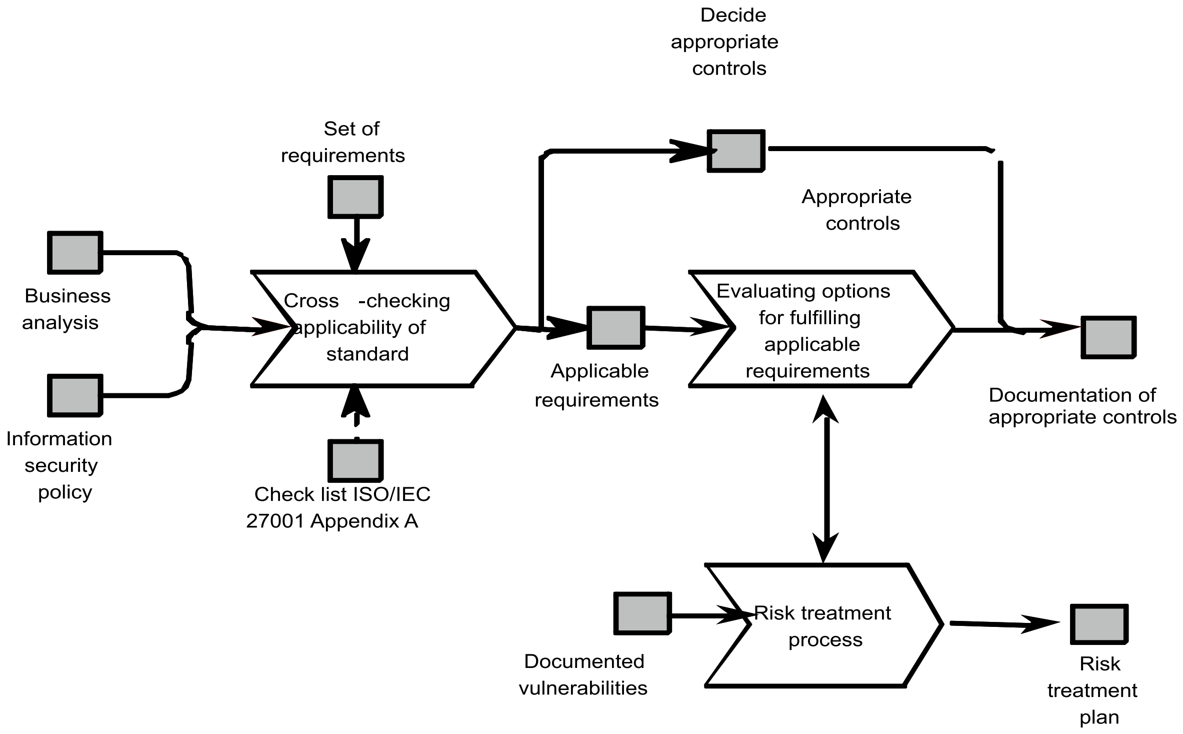

Decide appropriate controls
Set of requirements
Appropriate controls
Business analysis
Cross -checking applicability of standard
Evaluating options for fulfilling applicable requirements
Applicable requirements
Documentation of appropriate controls
Information security policy
Check list ISO/IEC 27001 Appendix A
Risk treatment process
Documented vulnerabilities
Risk treatment plan

Figure 8.2 Selection of Appropriate Controls and Risk Treatment Plan

Approach

Annex A of ISO/IEC 27001 is used as supporting information. The scope specified ISO/IEC 27001 Annex A is not meant to be exhaustive which is why further areas can also be selected. Sector-specific controls may be identified to support the specific needs of the business as well as ISMS. Conducted business, situation and risk assessment are used as supporting information.

The preparations for the declaration of applicability should be included as a part of the work in formulating the policy and overall guidelines, and consequently be carried out by the same working group.

Participation should include individuals who possess a strong knowledge of the organization's objectives, and security understanding (e.g. good insight into what is currently relevant in terms of threats to the organization's objectives. The members should be selected to represent a broad spectrum across the organization. The analysis takes place with representatives who have competence in the area in question. However, it is important that both operational and technical competencies are represented.

For example, the following roles should be included:

a. senior management (e.g. COO, CEO, CSO and CFO)
b. line managers (e.g. business unit heads)
c. process owners (i.e. representing important operational areas)

d. Other individuals who possess a strong knowledge of the organization objectives, and security understanding (e.g. good insight into what is currently relevant in terms of threats to the organization's objectives).

Identify Risk treatment options

Risk treatment options deal with risks, identified by the risk assessment as follows, and decided by management. (For further guidance, refer to ISO/IEC 27005.)

a. Applying the appropriate controls to reduce risk
b. Accepting risks, providing they clearly satisfy the organization's polices and the criteria for accepting risks
c. Avoiding risks
d. Transferring the risks to other parties

Transferring the risks to other parties Formulate a Risk treatment plan

Risk treatment plan is formulated to achieve the control objectives by implementing risk treatment options. (For further guidance, refer to ISO/IEC 27005.)

a. Documented risk treatment plan developed and managed by management
b. Documented selection of appropriate controls prescribed by management

Select the control objectives and controls

From the "Annex A (normative) Control objectives and controls" in ISO/IEC 27001, select control objectives and controls to use for risk treatment. If there are no appropriate control objectives or controls in "Annex A" additional control objectives and controls may be created. It is important to prove that this selection is valid, using the results of the risk assessment and risk treatment process. Annex A and B of this document show some examples of defining new controls as part of implementing an ISMS.

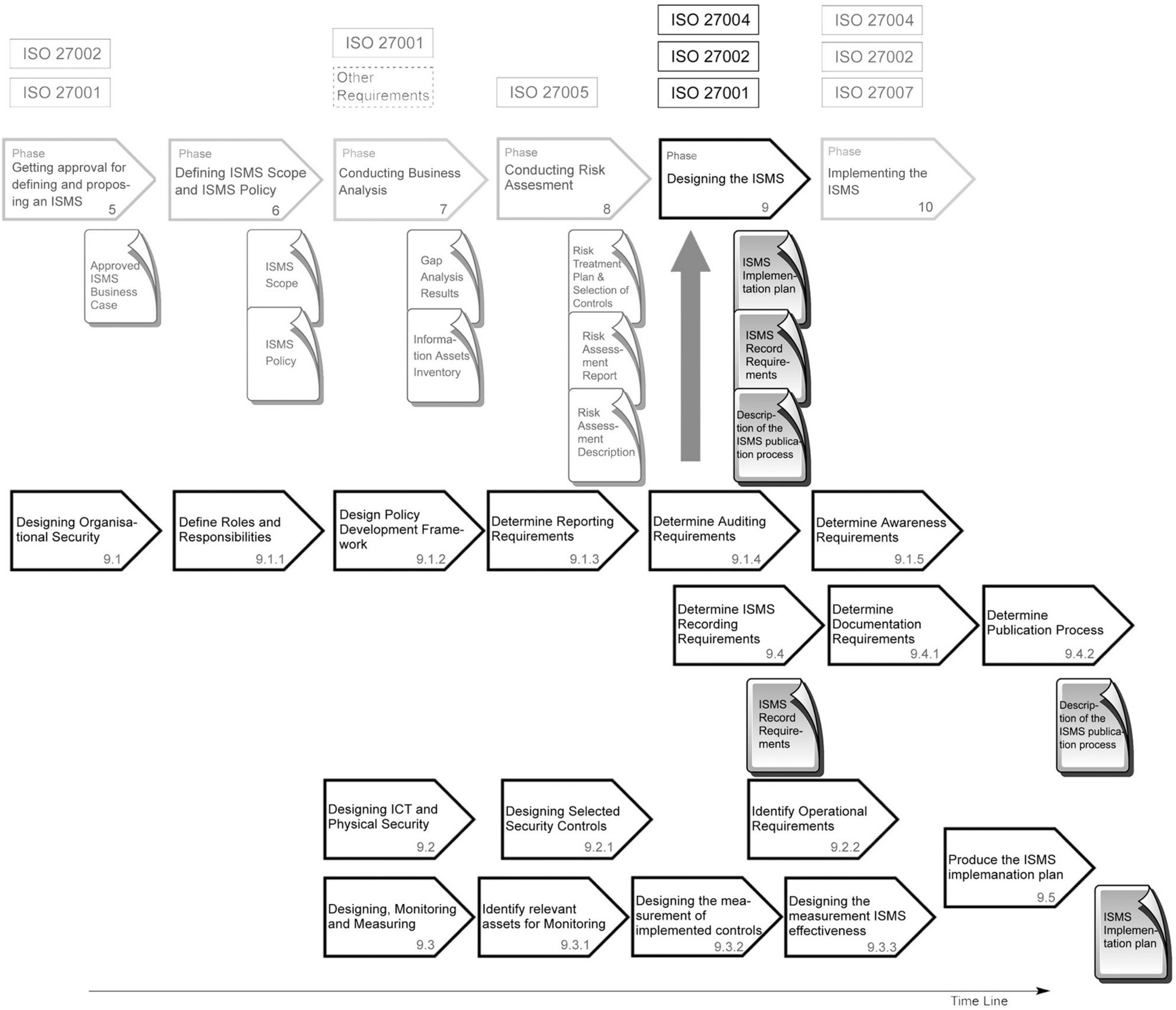
Prepare the documentation of the selection of appropriate controls

The control objectives, controls selected, and the reasons for choosing them should be documented. (If certification is the aim the statement of applicability is prepared. It is then also necessary to record reasons why any control objectives and controls in "Annex A (normative) Control objectives and controls in ISO/IEC 27001:2005" has been excluded.) In connection with the development of the policy or the initial proposals produced for the set of regulations cross-checking should be performed against ISO/ IEC 27001 Annex A.

Whether or not the controls described in ISO/IEC 27001:2005 Annex A are applicable should be checked section by section. If the control is applicable, refer to the regulations. If the control on the other hand is not considered applicable, state the reason why this is the case (e.g. requirements on outsourcing are not applicable if there is no outsourcing). If specific controls are needed that is beyond what is specified in Annex A, then note why this control is needed and how it is being used with the ISMS. If the requirement is applicable, but fulfillment is not considered possible, state how and when this should be rectified in an action plan. Use the table in Annex A and add a column with applicability as well as reference to the regulations. An example of this is shared in Annex A and B of this document.

9 Designing the ISMS

At this point, the ISMS business case has been approved, the ISMS scope and ISMS policy have been defined and information assets and the results of the gap analysis are known. In addition, risk assessment plan, description and assessment report are available.



ISO 27002
ISO 27001
ISO 27001
Other Requirements
ISO 27005
ISO 27004
ISO 27002
ISO 27001
ISO 27004
ISO 27002
ISO 27007
Phase
Getting approval for defining and proposing an ISMS
5
Phase
Defining ISMS Scope and ISMS Policy
6
Phase
Conducting Business Analysis
7
Phase
Conducting Risk Assesment
8
Phase
Designing the ISMS
9
Phase
Implementing the ISMS
10
Approved ISMS Business Case
ISMS Scope
ISMS Policy
Gap Analysis Results
Information Assets Inventory
Risk Treatment Plan & Selection of Controls
Risk Assessment Report
Risk Assessment Description
ISMS Implementation plan
ISMS Record Requirements
Description of the ISMS publication process
Designing Organisational Security
9.1
Define Roles and Responsibilities
9.1.1
Design Policy Development Framework
9.1.2
Determine Reporting Requirements
9.1.3
Determine Auditing Requirements
9.1.4
Determine Awareness Requirements
9.1.5
Determine ISMS Recording Requirements
9.4
Determine Documentation Requirements
9.4.1
Determine Publication Process
9.4.2
ISMS Record Requirements
Description of the ISMS publication process
Designing ICT and Physical Security
9.2
Designing Selected Security Controls
9.2.1
Identify Operational Requirements
9.2.2
Produce the ISMS implemanation plan
9.5
Designing, Monitoring and Measuring
9.3
Identify relevant assets for Monitoring
9.3.1
Designing the measurement of implemented controls
9.3.2
Designing the measurement ISMS effectiveness
9.3.3
ISMS Implementation plan
Time Line

Figure 9.1. Overview of the Designing the ISMS Phase

The objectives of the "Designing the ISMS" are:

- Create a Implementation plan
- Establish the formal and practical requirements for the ISMS documentation

In order to create the implementation plan as well as the formal requirements for the next phase many activities needs to be performed. In order to have a structure for the designing it is advisable to divide it into four main areas:

a. Organizational security – to cover of the administrative aspects of information security related to the responsibility of the business operation. This should be formed into the set of activities resulting in the policies, objectives, processes and procedures to handle and improve information security in relation to the business needs and risks.

b. ICT security – to cover aspects of information security specifically related to the responsibility of the ICT operations. This is to fulfil the requirements set by the business and the technical implementation of controls to reduce risks.

c. Physical Security - to cover aspects of information security specifically related to the responsibility of the handling of the physical environment such as buildings and their infrastructure. This is to fulfil the requirements set by the business and the technical implementation of controls to reduce risks.

d. ISMS specific – to cover the aspects of the different specific requirements for an ISMS according to ISO27001 apart from what is covered in the other three areas. The focus is on certain activities that should be conducted in the implementation to achieve a proper ISMS in operation. These are in particular:
    - Resource allocation
    - Monitoring
    - Internal ISMS Auditing
    - Measuring
    - Training and Awareness
    - Incident Management
    - Management Review

Designing the implementation of the different controls means interaction with people who have responsibilities in all four areas above. The fourth area of the ISMS requires dialogue with the management for reviewing the (a) handling the specific requirements (b) owner of the designed of information security system, or the project manager.

9.1 Designing Organizational Security

Activity Objective: To establish the organizational functions and responsibility for the information security within the organization.

9.1.1 Roles and Responsibilities

Approach

The business analysis is the first process to establish the ISMS in an organization. Therefore, the organizational structures that should be maintained throughout the whole ISMS implementation phase should be planned. The members of the group for establishing the ISMS should be chosen from a range that is wide enough to cover the issues from every department related to the businesses and operations of the ISMS scope. In addition, to this group, there should be discussions on how the organization deals with information security.

The information security to be handled in the ISMS should consider the "information risks". In addition to daily management, it is also required to address the damage after the risks occur. To implement such all-inclusive "management," cross-functional assignments of human resources are needed, not only from the direct units included in the ISMS scope, but also from the indirect divisions, such as legal and administrative departments.

Figure 9.2 shows an example of the organizational structure for establishing the ISMS. The main roles and responsibilities of the organization given below are based on this example.

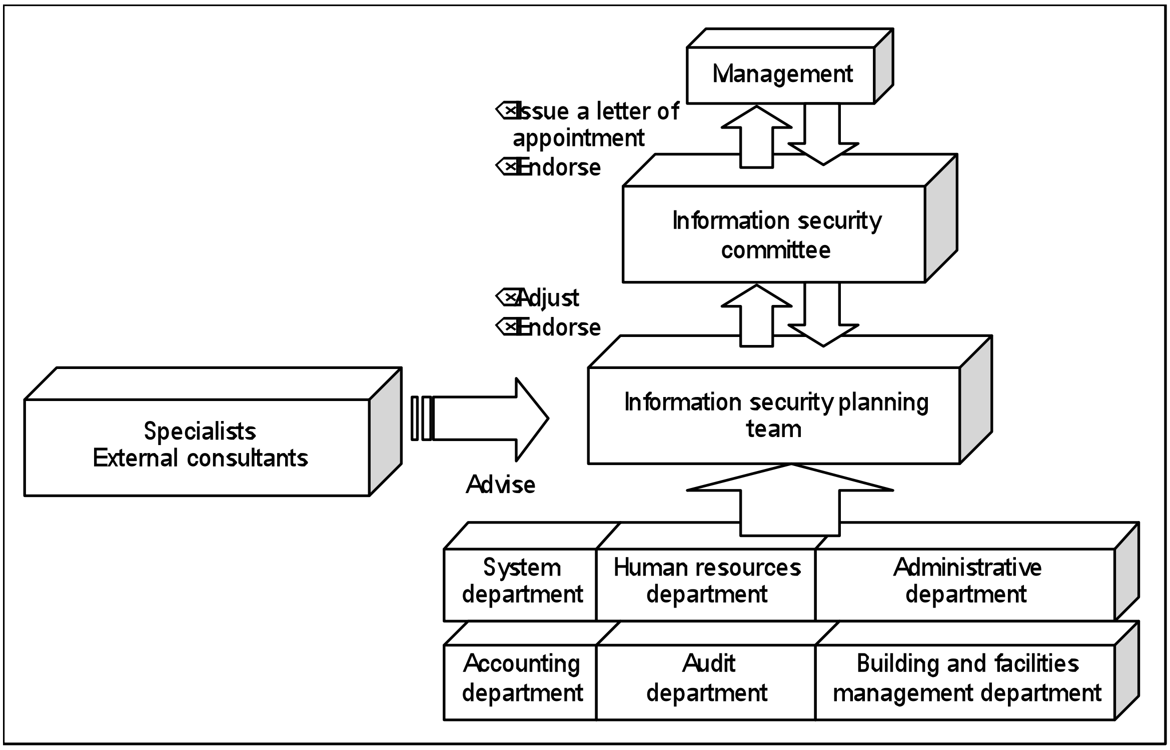

Management
⌫Issue a letter of appointment
⌫Endorse
Information security committee
⌫Adjust
⌫Endorse
Specialists
External consultants
Advise
Information security planning team
System department
Human resources department
Administrative department
Accounting department
Audit department
Building and facilities management department

Figure 9.2 Example Organizational Structure for Establishing the ISMS

9.1.1.1 Designing the Information Security Forum

The design of such forum may vary depending on the organization. The design should be based on knowledge gained during the previous phases and activities and be concluded as:

- Who are the members/participants
- How will the forum interact with the rest of the organization
- When should the meetings be held
- What is the main tasks
- What are the expected results
- The forums formal acceptance by the management (Issue a letter of appointment as in figure 9.2)

Who are the members?

1. Roles of the Information Security Committee

   The Information Security committee should be responsible for handling the information assets which are possessed by an organization, and should have a sufficient understanding of information security for directing tasks and being able to get things done.

   The information security committee should have a leading role for the ISMS in an organization. The following shows examples of the roles that the information security committee should play.

   - Consider the preparation of the environment for risk management
   - Establish the plan for the ISMS documents, being responsible for determining the contents of these documents and acquiring acceptance from the management.
   - Plan the purchase of new equipment and/or to reuse the equipment that the organization already possesses.
   - Handle the problems that may happen while establishing the ISMS
   - Consider the improvement based on the results to implement and to measure the ISMS.

2. Roles for the Information Security project

The project team when planning the project, which is responsible for the ISMS being established, should be assisted by members who have a broad understanding of the important information assets within the ISMS scope, and have enough knowledge to consider how to handle this information. For example, when determining how to handle information assets, there might be different opinions among departments within the ISMS scope so there might be a need to adjust the positive and negative effects of the plan. The project team is required to work as a coordinator of conflicts across the boundaries of departments. To do this, they need communication skills, founded on their experiences and coordination abilities, as well as high levels of knowledge about security.

3. Specialists and External Consultants

   An organization should select members (if possible, members with one exclusive role) at its own cost before establishing the ISMS. However, the members need to have broad knowledge and experience in the field of "information security" such as "IT," "managerial decisions" and "an understanding of the business,”

   The people who are responsible for some operations in an organization may know this best. The many specialists, the experts in specific fields in their organization, should be referred to in terms of their intention about the ISMS matters as it relates to use in their specific fields. It is important to also have a balance of this expertise with the broad knowledge needed to meet the business objectives.

   External consultants can give decisions based on their macroscopic points of view of an organization and experience from other similar occasions, even though they generally do not necessarily have in depth knowledge about the businesses specifics and operational details of an organization.

   The terms that are used in the above examples, such as the Information Security Committee and the Information Security Planning Team, are not important. Only the function of each structure should be understood. Ideally there should be internal structures to coordinate the organization’s information security communicating and working closely with each technical department.

4. Contact Person

   A contact person should be appointed for each business process and specialist application; this person acts as the so-called "process owner" for all information security issues relating to processing data within this business process. The contact person or process owner is responsible, for example, for delegating tasks and handling information within the business processes to which they have been assigned.

In order to determine the relevant information security conditions for each key business process as quickly and in as much detail as possible, it is advisable to hold a short security meeting (brainstorming) for each business process.

The Business analysis should be performed within a defined period with important starting points identified at the very early stages of the analysis. Some important starting points to include in a brainstorming session for each business process form a concise picture of the organization including the identification of existing:

a. Documents (e.g. operational objectives defined within annual reports and policies)
b. Requirements for identifying and protecting the organization assets
c. Infrastructure (e.g. physical locations and information systems)
d. Organization (e.g. department)
e. Personnel (e.g. corporate management, department management and operational individuals)
f. Description of operations environment
g. "Role" with the macro-environment Including the impact of organizations culture
h. Core information processing activities that must be protected

i. Information processed for a business process and the associated IT applications and systems.

Interaction with the organization

All parties involved should review and become very familiar with the current requirements for protecting the organization's assets, ISMS scope and ISMS policy. Participation in business analysis should include individuals who possess a strong knowledge of the organization and the environment in which it operates. These individuals should be selected to represent a broad spectrum across the organization and include:

a. senior management (e.g. COO and CFO)
b. members of the Information Security Committee
c. members of the Information Security Planning Team
d. line managers (e.g. business unit heads)
e. process owners (i.e. representing important operational areas)
f. specialists and external consultants

9.1.2 Policy Development Framework

9.1.2.1 Designing the Information Security Policy

The information security policy documents the strategic position taken by management and administration to achieve the information security objectives throughout the organization.

The policy should reflect the organization's requirement for information security and function as guidance and motivation. In the policy, the management outlines its ambition, roles and responsibility or responsibility allocation within the organization.

The information security policy describes in general terms how information security is to be established in the organization, the purposes, resources and structures. It contains the information security objectives desired by the institution and the information security strategy to be followed. The information security policy should describe the acceptable risk tolerance which translates to the desired security level of the public agency or company beyond the information security objectives. It is therefore both a requirement and a statement that this level of security should be obtained at all levels within the organization.

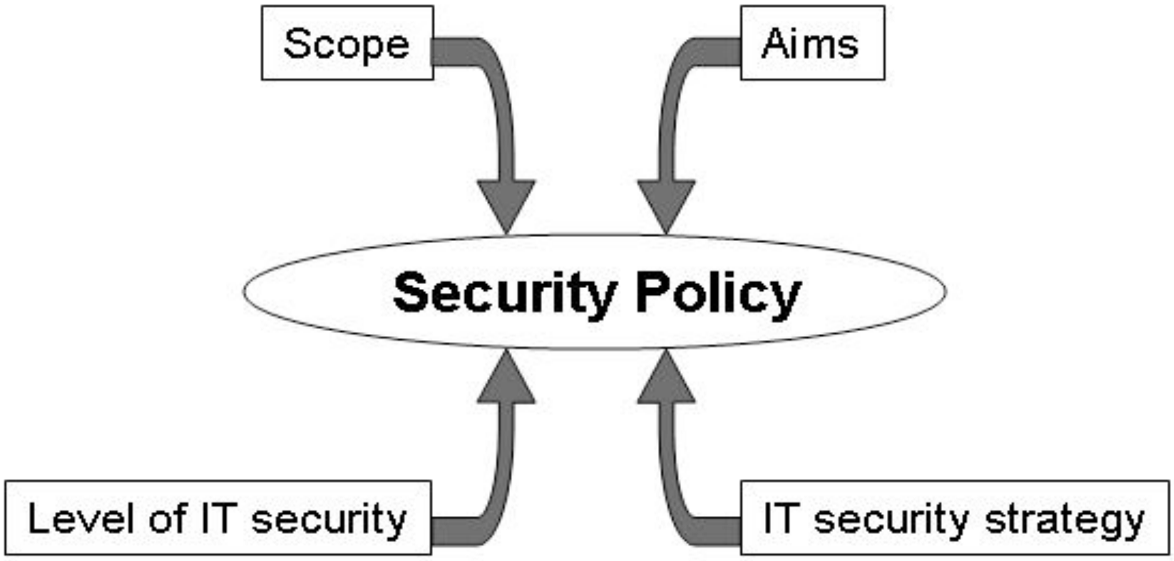


Figure 9.3: Content of the information security policy

Input data for the policy is based on the results from the following processes:

a. General organization management and governance principles and policies
b. Management understanding of and commitment to systematic management of information security
c. Business analysis
d. Gap analysis
e. Overall risk assessment and
f. How the existing organization and other management systems are composed.

If the policy is drawn up with this input data being incomplete or incorrect there is a great risk that the policy is not reflecting the requirements of the organization in terms of security.

The Information Security Policy is often a rewrite of the ISMS policy in order for it to be easily communicated internally and externally (or identical to the ISMS policy if it is regarded as fulfilling the purpose). The Information Security Policy is the formal document signed by management.

In order to define the objectives of the information security expressed in the information security policy, it may be appropriate to involve an external information security expert. To determine the desired level of information security, the institution's objectives should be viewed with reference to the information security requirements, taking into account that there are limited resources available for implementing information security controls. It is particularly important to identify the actual requirements for availability, integrity and confidentiality because a high level of information security is usually related to a high cost of implementation. At this point it is also advisable to prioritize the requirements. This is forming a basis on which decisions are made for resource planning at a later stage in the security process.

The members should be selected to represent a broad spectrum across the organization; for example, the following roles should be included:

a. senior management (e.g. COO, CEO, CSO and CFO)
b. line managers (e.g. business unit heads)
c. process owners (i.e. representing important business areas) and
d. other individuals who possess a strong knowledge of what is the current environment, conditions, existing management system, and what is relevant in terms of information security.

The policy is drawn up based on the above information and knowledge. What is identified by the management as important in the previously conducted analysis should be made evident and emphasized in the policy in order to provide incentive and motivation in the organization. It is also important to point out what happens if the policy is not followed. Laws and regulatory impacts that affect the organization in question should also be emphasized. Examples can be drawn from reference literature, the Internet, interest associations and industry associations. Formulations and overtones can be drawn from annual reports, other policy documents or other documents that management supports.

There may be different interpretations and requirements regarding the actual size of a policy. It should be sufficiently summarized that the staff are able to comprehend. In addition, it should sufficiently distinguish what objectives are needed to address the set of regulations and business objectives. A guideline for its size could be 2-4 pages. If a very brief policy is chosen, a more comprehensive template document should be appended that could be used in the next stage in the process for introducing an information security management system.

The policy should be comprehensive and periodically reviewed. Whoever has responsibility for the policy and its maintenance should be listed in the policy and/or the set of regulations, e.g. under the clause Follow-up and Compliance.

For large and complex organizations (e.g. with widely differing operational areas) it may be necessary to draw up an overall policy and a number of underlying operationally adapted policies.

The policy should comprise the following:

a. definition of information security, its general objectives and scope, and the importance of security that facilitates the sharing of information with others in a secure manner

b. declaration of management's ambitions that supports the objectives and principles of information security;

c. Short presentation of general security policies, principles, guidelines and compliance requirements of particular significance for the organization. Examples include:

    - compliance with laws, ordinances, agreements and other external security requirements;
    - security training requirements;
    - continuity plan for the organization;
    - consequences of neglect of the security policy;
    - risk assessment
    - definition of general and specific responsibility for information security including the reporting of incidents;
    - References to other governing documentation and routines for individual information systems or other security regulations that should be followed.

The policy should be communicated to all individuals affected within the entire organization.

The proposed policy (with the version number and date) should be cross-checked and established within the organization by the operational manager. Following establishment within the management group or equivalent, the operational manager approves the information security policy. It is then communicated to everyone in the organization in such a way that it is relevant, accessible and understandable for its readers.

9.1.2.2 Operational plans and procedures

Approach

For the information security process, standards and procedures covering either the entire organization or particular jobs should be developed. Procedural rules or procedures on actions to be taken should be written, and these should be available to every employee as the basis for their actions or omissions at the workplace. These rules should be compiled and made available in a suitable form to each target group. The standards and procedures should apply to the entire organization or define the demarcations.

The results should provide a foundation for the information security work within the organization. The set of the legal and regulatory requirements should include formulated objectives on WHAT should be achieved, and also procedures at an overall level on HOW the objectives are to be achieved. For example, the sub-processes that should be implemented and the security precautions that should exist need to be defined.

The work covers both standards and procedures in order to provide adequate support to the organization for the introduction and formulation of more detailed procedures. (At the next level, procedures are formulated that are adapted to HOW the work should be carried out).

Standards and procedures should be developed by representatives from the organization assigned by the management.

Security standards and procedures should be available to any individuals in the organization, and may be used as supporting information when developing further detailed application procedures.
The results should be available to use for checking that the organization is following the standards.

The following results from are required to draw up the information security standards and procedures:

a. ISMS scope and boundaries
b. ISMS policy
c. Results from the risk assessment (Overall risk assessment, In-depth risk assessment)
d. Statement of applicability including the control objectives and the selected controls
e. Risk treatment plan
f. Information security policy,

Representatives of different sections of the organization, covered by the scope of the ISMS, should participate in the process of developing standards and procedures. The sections of the organization that participate should cover all the areas that also comprise the regulation and procedures. The representatives should primarily work with sections that fall within their occupational area in order to create as good an operational adaptation as possible. This then facilitates later refinement in the form of procedures and routines at operational level.

Participation from the organization should be perceptible so that the organization recognizes its participation and has been able to raise its questions. Those participating should have authority and be representative of the organization. Good relationship with the management for each respective area is important. It is important to create an editorial group, as small as possible, with the option to appoint special competency.

A first version should be produced quickly. An evaluation of the old regulations, e.g. if they can be refined and further developed in a new version should be made especially if the old version should be replaced with a completely new one.

The establishment process should be clarified at an early stage. Continuous establishment is often required. A strategy should be drawn up for how information on results should be distributed.

The members should be selected from different sections of the organization to develop well adapted information security standards and procedures. For example, the following roles should be included:

a. Information security managers,
b. Representatives for physical security,
c. Information Systems owners and
d. Process owners of strategic and operational areas

For information security standards, it is important to reflect what the general and common requirements are for the entire organization. The results from the applicability section govern which standards and procedures should be drawn up. The results from the risk analysis govern the level of security that should be addressed by the different standards.

Drawing up and establishing regulations are done within the organization. Each member of any working group can be responsible for the establishment within their own allocated regulation section. Drawing up standards and proceeding with more detailed procedures can be done for each sub-section within the chapter.

Establishment in the organization is essential through consultation. This may take time, depending on the size of the organization, management motivation and maturity.

The following are the results of the information security standards and procedures.

a. Information security standards including the baseline of the organization
b. Information security procedures achieving the information security standards

9.1.3 Reporting and Management Review

Approach
A management review is a series of processes in which the management finds out the effectiveness of the ISMS and makes decisions on improving it. An ISMS management review should be performed at specified intervals at least once a year.
As there is no ISMS implemented yet the only activity regarding the management review is at this stage to inform the management and establish when and how it preliminary should be conducted as well as determine what to report to the reviews.
Preconditions of Management reviews are the information collected based on the constructed and the operated ISMS. This information is used by management to determine the improvement of the ISMS. Detailed information about preconditions is written as the requirements of the Management review's inputs in sub clause 7.2 of ISO/IEC 27001. IT should also be noted that this should include Risk management reviews, reviewing the methodology and results of risk assessment at planned intervals in consideration of the changes in the environment, such as organization, and technology. Ensuring the risk management reviews is written as a requirement in ISO/IEC 27001 4.2.3 d).

To plan the review an assumption of who to involve and at this early stage inform them about the necessity and purpose of the review, this could involve roles such as:

(1) Risk assessment reviews

The members who are able to identify and evaluate risks of each asset and who are able to judge the change of environment should be selected. For example, the following roles should be included:
- Senior management (e.g. COO, CEO, CSO and CFO),
- Line managers (e.g. business unit heads)
- Information security staff,
- Information system owners, and- Process owners of strategic and operational areas

(2) Management reviews
Management, and the members who are able to collect the information needed as inputs of the management review, should be selected. For example, the following roles should be included:
- Senior management (e.g. COO, CEO, CSO and CFO),
- Line managers (e.g. business unit heads)
- Information security staff,

It could be useful to define types of information can be input into the management review, such as:

a. Results from the monitoring

b. Results from the ISMS measurements

c. Changes in the environment which may affect the ISMS (e.g., All changes inside and outside of an organization such as changes in the business environment and changes to the organization the social and technical environment, legal regulations)

d. recommendations

e. Feedback from stakeholders, including patients, business partners, and office staff, and from administrative agencies

f. The results of internal or external audits (for example, nonconformities pointed out by a certification or registration body and issues observed)

g. Information on new technology that has become available, new products and services announced by vendors, and the like

h. The practical status and effects of the preventive and corrective action that has been taken

i. Decisions on the need for review of risk assessment of vulnerabilities or threats, which has not been considered by financial, environmental or legal regulations.

j. Reports on follow-ups about whether the results of management reviews in the past have been appropriately addressed.

9.1.4 Planning Auditing

Approach
The implementation of ISMS should be evaluated at regular intervals by means of internal and independent audits. These also serve the purpose of collating and evaluating the experiences made in day-to-day practice. In order to implement an ISMS the forms for auditing have to be planned at this stage.

In the ISMS audits, auditing results should be determined based on the evidences. Therefore, some period for the ISMS operations should be needed to collect suitable evidences.

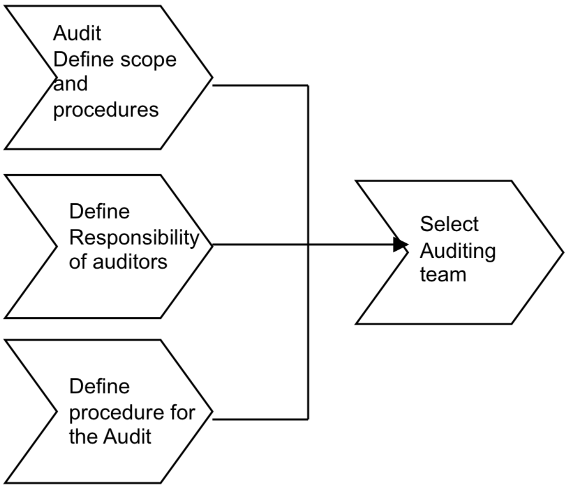

Audit
Define scope and procedures
Define Responsibility of auditors
Define procedure for the Audit
Select Auditing team

Figure 9.4 Overview of the Audit Planning

Note: Prior to carry out auditing, the PDCA cycle of an ISMS must be implemented in full.

Organization units or individuals that are independent from the scopes of internal ISMS audits should be selected as the auditors by management. These auditors should plan, carry out and make reports and follow-up of the internal ISMS audits to acquire the commitment of management.

An internal ISMS audit should be implemented and executed regularly to evaluate whether the control objectives, controls, processes and procedures of the ISMS conform to the requirements of ISO/IEC 27001 and relevant legislation or regulations, conform to the identified information security requirements, and are effectively implemented and maintained.

However, selecting the internal ISMS auditors may be difficult for small companies. If not enough resources are available to have these kinds of audits performed by experienced internal members of staff, external experts should instead be charged with carrying out auditing activities. It might be useful to call in external auditors to avoid the situation in which staff members become blinkered to their own work. When organizations use external auditors, the following should be considered: external auditors are familiar with the internal ISMS audits themselves; however they do not have enough knowledge about the business environments of an organization. Sufficient information should be reinforced from internal staffs. On the contrary, internal auditors tend to be able to perform minute audits by considering an organization's business environment, though they may not have enough knowledge about the ISMS audits. Organizations should recognize the characteristics of internal and external auditors to carry out the internal ISMS audits.

The effectiveness and efficiency of the implemented controls (see ISO/IEC 27004) should be examined within the scope of internal audits. If not enough resources are available to have these kinds of audits performed by experienced internal members of staff, external experts should instead be charged with carrying out auditing activities.

If not enough resources are available to have these kinds of audits performed by experienced internal members of staff, external experts should instead be charged with carrying out auditing activities.

It is important that none of the audits are carried out by those individuals who were involved in the planning and design of the security objectives, because it is difficult to find one's own mistakes. Depending on the size of the institution, it might be useful to call in external auditors to avoid the situation in which staff members become blinkered to their own work.

The members of this step are composed of the persons who carry out the audits, namely internal ISMS auditors, and the persons who are being audited. Management has both aspects that are as the persons who are being audited and as the person responsible for carrying out the audits.

- Senior management (e.g. COO, CEO, CSO and CFO)
- Internal ISMS auditors (internal staffs or external experts)
- All members besides management involved in the ISMS scopes are members who are being audited, such as,
    - The users of the security products,
    - The persons in charge of information systems
    - The persons in charge of information security
    - All operators and responsible of security controls

In an internal ISMS audit, it should be checked that the ISMS is being carried out effectively, maintained and carried out as expected. Since internal ISMS audits should be carried out as planned, auditors take the status and importance of management goals, controls, processes and procedures to be audited into account when planning an audit program, as well as the results of the audit.

In carrying out an audit, the criteria, applicable scope, frequency and method of the audit should be documented.

The objectivity and fairness of the audit process should be ensured when auditors are selected. When auditors are selected, it is important that they have different competences from the security operators or managers. For example, an auditor is required to have the following competences when carrying out the series of processes in the audit:

a. Planning and carrying out the audit

b. Reporting the results

c. Proposing corrective and preventive action, etc.

In addition, the organization is required to define the responsibilities of auditors and the series of processes for the audit in the procedure documentation.

If it is difficult to find an auditor with the required competences inside an organization, it is possible to ask an external auditor. Note that auditors cannot audit their own operations, to ensure objectivity. A manager who is responsible for a process being audited should ensure that action is taken to remove the nonconformity found and its cause without delay. This does not mean that the nonconformity should be corrected immediately. In addition, the corrective actions performed should include a verification of the action that has been taken and a report of the results of verification.

From the viewpoint of governance, the internal ISMS audit for the ISMS can be performed effectively as a part of, or in collaboration with, the internal ISMS audit of a business audit of the whole organization. When performing the audit, it is a good idea to refer to "Requirements for bodies providing audit and certification of ISMS ISO/IEC 27006”, as well as “ISMS ISO/IEC27007” about auditing.

The information security audit system or system audit system may also be used, to ask external specialists to perform an internal ISMS audit.

One of the important pieces of input to a management review is the result of an internal ISMS audit. The ISMS certification criteria define internal ISMS audits in detail.

9.1.5 Awareness

Approach
Information security concerns all staff members without exception. By acting responsibly with security awareness, every individual can avoid damages and contribute to the success of the organization. Increasing the awareness for information security, providing appropriate training to staff members as well as all management personnel are fundamental prerequisites for the organization. In order to be able to implement security controls as planned, staff members should have the necessary basic and practical implementation skills. In addition knowledge about how security management mechanisms should be designed and operated is important. It involves an understanding on the targets and objectives of security controls.

If staff employees are hired or existing ones are transferred to new tasks, they should be provided with thorough training so that they can understand and contribute quickly to the new situation. This should also involve teaching them about the security-related aspects of their job. If staff employees leave the organization or change their roles and responsibilities, this process should be accompanied by appropriate security controls (e.g. withdrawal of authorisation, returning keys and identity cards).

The following results from should be included in the education and training materials:

a. ISMS scope and boundaries
b. ISMS policy
c. Results from the risk assessment
d. Statement of applicability including the control objectives and the selected controls
e. Risk treatment plan
f. Information security policy, standards and procedures

In large organizations, a single set of training material is generally not sufficient. Therefore, it is necessary to have different sets of training material addressing the scope and content based on the importance and complexity of information security as appropriate for each target group of the scope. For example, an IT administrator or software developer needs to have other skills and knowledge of information security than a clerical work person or an administrative assistant. The first stage in drafting information security training materials is to assign the organizational staff to target groups so that the dedicated training materials can be customized for them. It is important to ensure here that every employee either directly or indirectly is allocated to one of these groups, the training material is available and the training takes place.

All members who are responsible for the jobs that are included in the ISMS scope should be provided training and awareness program. The members who are responsible for planning, providing training and awareness program should be included. For example, the following roles should be included:

a. The responsible manager of the training (e.g. Personnel department manager),
b. The supporting manager of the training (e.g. Information security staff, information systems staff),
c. The manager of the employee who is responsible for performing training and
d. The employee who is responsible for performing training

The information security training materials should be prepared with the close co-ordination of other training materials of the organization, especially with the training courses for IT users. It should be considered that the training topics on information security should be integrated into the courses for IT users. It is essential that the lecturers have the expertise and demonstrate the appropriate skills. The training course should be designed with sufficient coverage of information security for the users.

Information security training material should contain the following points as a minimum:

a. Risks and threats regarding information security
b. Basic terms and basic parameters of information security
c. Clear definition what a security incident for the organization is how it is identified and how it should be dealt with by the appropriate target group.
d. Information Security Policy, Standards, Procedures of the organization
e. Responsibilities and reporting channels in the organization
f. How can one contribute to information security?
g. How can one tell if a security-relevant incident has occurred and what should one do?
h. How can one educate themselves and get information regarding information security?

Depending on the type and depth of IT use, additional topics should be included for particular target groups, for example:

a. secure telecommunication,
b. security requirements of particular IT systems and applications,
c. secure software development and
d. drawing up and audit of information security procedures.

In each case, it is necessary to check which subjects can be handled by internal organization's staff and which ones would be better dealt with through external courses.
Due to the speed at which technology changes, knowledge previously acquired becomes rapidly out of date. New systems, new threats, vulnerabilities and mitigating controls, make it mandatory that knowledge regarding information security is continually refreshed and extended. Therefore, training on these points should be provided to the new staff and experienced employee. The supplementary courses should be provided at regular intervals for experienced users as well.

It is important that the training materials are updated regularly and modified to new circumstances as necessary as well as to new target audiences.

Management is responsible for carrying out education and training to ensure that all personnel who are allocated a clearly defined role have the competence to perform the operations required. Ideally, the content of the education and training performed should help all personnel understand the meaning and importance of the information security activities they are involved in, and how they can contribute to achieving the goals of the ISMS.

It is important that the effectiveness of the education and training that has been performed is evaluated, and that the results are used to secure personnel who are competent. The required competence depends on the operation. Possible categories of competences required for establishing, implementing, operating and maintaining the ISMS are shown in below in Table 1.

Competences associated with information security management	General information security management theory, And leadership etc.
Competences associated with information security auditing	General information security audit theory and audit practices
Competences associated with security technology	The theory and practice of network security, server application security, operating systems security, firewalls, penetration detection systems, viruses, secure programming and encryption.

Table 1 **Categories of Competencies**

The following results should be provided from the information security education and training process:

a. Information security education and training materials
b. Formation of information security education and training including their roles and responsibilities
c. Plans for information security education and training
d. Actual records showing the results of the employee's information security education and training

9.2 Designing ICT and Physical Security

Activity Objective: To design necessary activities within ICT and Physical area to implement information security according to the ISMS policy and the selection of controls.

When designing information security, it is crucial that security controls designed are not compromised by the lack of security at other places. Physical security deals with all aspects of access control, physical protection of information assets and what they are stored / kept in as well as a means of protection for security controls itself.

9.2.1 Designing selected security controls

Approach

There are two typical kinds of controls for physical security. They are the (1) ones preventing or slowing down a physical attempt, disaster (fire, water, etc) and the (2) ones which provide an alarm to trigger appropriate action.

When designing a physical security system, these aspects are need to be considered carefully and must be integrated with organizational and ICT security.

9.2.2 Identification of operational requirements

Approach

This step in the Plan Phase provides an overview of implementing ISMS controls based on the organization's information security standards and procedures. Figure 8.3 flow diagram for shows implementing the ISMS controls.

The selected controls described in 7.6 should be implemented based on the Information security standards and procedures according to an implementation plan that addresses the control objectives. A structured implementation plan is essential if the controls identified are to be properly implemented. The information security management is responsible for drawing up the implementation plan.

The following results from are required to draw up the structured implementation plan:

a. ISMS scope and boundaries

b. ISMS policy

c. Results from the risk assessment

d. Statement of applicability including the control objectives and the selected controls

e. Risk treatment plan

f. Information security policy, standards and procedures

The members of the group for implementing the controls in the organization should be selected from the scope that is wide enough for implementing the controls related to handling different types of information, and from the related departments who are performing the actual ISMS operations.

ISMS should implement not only the total management system to meet ISMS policy and objectives, but also the controls to meet the control objectives. To implement such comprehensive total ISMS and controls, the cross-functional formation of human resources is needed not only from the direct departments related to the scope of ISMS implementation, but also from the indirect departments such as general and personnel affairs.

The members should be selected for their role in the implementation of each control. For example, the following roles should be included:

a. Information security staff,

b. Representatives for information systems,

c. Representatives for physical security,

d. Personnel affairs,

e. General affairs and

f. Process owners of strategic and operational areas.

A structured implementation plan is essential if the controls identified are to be properly implemented.
The following should be documented in an implementation plan:

a. name of the person responsible for implementation of a control,

b. priority of the control to be implemented,

c. statement of the time by which the control should have been implemented,

d. tasks or activities to implement controls

e. person to whom implementation of the control should be reported, once complete,

f. resources for implementation (manpower, resource requirements, space requirements, costs).

The implementation plan should also define not only the initial responsibilities, but also the actual implementation responsibilities for the control, which have any distinction between a conceptual design process and the actual implementation process in order to achieve and implement the best practice for the organization. Initial responsibilities generally include:

a. specification of control objectives together with a description of the expected planned state

b. allocation of resources (workload, financial resources) and

c. realistic time target for implementation of the control.

d. Integration options with ICT and organizational security

Responsibility for the actual implementation process can be achieved by the following roles. The roles at the actual implementation process include:

a. design for technical or organizational areas at operational level of the workplace,

b. development for the detail tasks from the implementation main tasks,

c. provision of procedures and information for security awareness promotion controls and training courses, and

d. provision of aids and implementation of the controls at the workplace.

Depending on the type of controls (technical or organizational), it may not always be possible to draw a clear-cut definition between the initial process and the actual process implementation. The implementation of controls frequently requires cooperation between several different organizations. Thus, for example, persons with system responsibility are needed to procure, install and maintain technical facilities. On the other hand, for example, persons with organizational responsibility are needed to create and document the appropriate rules regarding their use.

Information security should be integrated in organization-wide procedures and processes. If it is difficult to implement them, the related organizations should communicate this immediately so that a resolution can be agreed upon. For example, typical solutions are modifying the procedures and processes, allocating roles and responsibilities and adapting technical procedures.

The following are the results of implementing ISMS controls.

a. Implementation plan which specifies details of the implementation of controls, such as schedule, structure of implementing team and so on
b. Records and documentation of the results on implementation

9.3 Designing the Monitoring and Measuring

Activity Objective: To design the future security monitoring and measurement program for the ISMS that supports management review.

9.3.1 Designing Monitoring

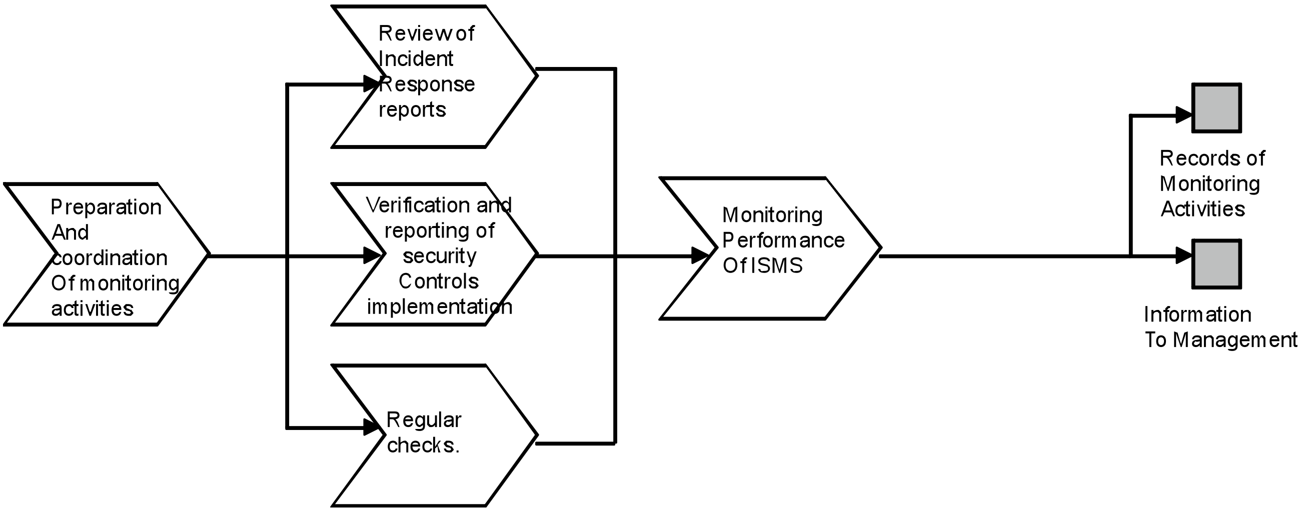

Preparation And coordination Of monitoring activities
Review of Incident Response reports
Verification and reporting of security Controls implementation
Regular checks.
Monitoring Performance Of ISMS
Records of Monitoring Activities
Information To Management

Figure 9.3.1 The Monitoring Process flow

9.3.1.1 Preparation and coordination: Identification relevant assets for monitoring

It should be noted that monitoring process is a continues process and as such the design must take into consideration the set up of the monitoring process as well as designing the actual monitoring needs and activities. These activities need to be coordinated which is part of the design.

Based on previous information set by the scope and the assets defined in combination with the results from the risk analysis and the selection of controls, the objectives of Monitoring can be defined. These objectives should include:

- What to Detect
- When
- Against what,

In practical terms the previous set business activities/processes and linked assets is the basic scope for monitoring (bullet “Against what” above). For designing the monitoring a selection may be needed to cover the important assets from an information security point of view. Consideration should also be made for the risk treatment that the selection of controls in order to find what should be monitored on the assets and linked business activities/processes. (This will set both What to Detect and When.)

As monitoring may have legal aspects is essential that the design of the monitoring is checked so that it will not have any legal implications.

It is then from a design point of view important to coordinate and make the final design of activities for monitoring.

9.3.1.2 Monitoring activities

In order to maintain the level of information security, the information security controls that have been identified as being appropriate should be applied correctly; security incidents should be detected and responded to in a timely manner, the performance of the information security management system should be monitored regularly. Regular checks must be performed to see whether all controls are being applied and implemented as planned in the information security concept. This must involve checking that the technical controls (e.g. as regards the configuration) and the organizational controls (e.g. processes, procedures and operations) are complied with. Checks should be primarily geared towards remedying defects. If checks are to be accepted, it is important that this is recognised by all those involved as the objective of the checks. It is important to discuss possible solutions to problems with participants during a check and to pre-prepare appropriate remedies.

Checks should be carefully prepared so to ensure that they can achieve their goals as efficiently as possible while at the same time causing as little disruption as possible to the work routine. The general implementation of checks should be coordinated in advance with Management. The design activities may be concluded in three different basic forms:

- Incident reports
- Verification or non-conformity of control functionality
- Other Regular Checks

Further how the results from the activities should be designed in terms of how records are made and information to management.

Formal documentation should be made to describe the design and covering principle activities and their purpose as well as different responsibilities.

9.3.1.3 Requirements for Monitoring outcome

The results are:

a. Records of the monitoring activities on required level of detail
   As a result of the monitoring activities, a management report should be provided. All the information that management requires in order to fulfill its management and supervisory duties must be recorded therein with the required level of detail.

b. Information to management for decisions making when required for prompt actions
   Management reports should always end with a list of recommended actions, clearly prioritized, together with a realistic assessment of the expected cost of implementation of each of these actions. This ensures that the needed decisions can be obtained from Management without undue delay.

9.3.2 Designing the information security measurement program

9.3.2.1 Overview for designing an information security measurement programme

The measurement process should be seamlessly integrated into the ISMS cycle of the project or organization and used to effect the continual improvement of security-related processes and outcomes within that project or organization. This is referred to as an information security information program (ISO/IEC27004). The design of the program needs to be viewed in the perspective if the ISMS cycle. The following figure depicts how the measurement process fits within the ISMS cycle.

The following functions are required of the management systems to ensure the satisfaction of require things and expectations, such as structuring the necessary PDCA; measuring the validation of outputs and its effectiveness; and providing feedback of the results of measurement to the manager of the processes.
In order to have the right measurements in place, previous generated information is essential, especially:

a. The ISMS policy, including scope and boundaries
b. The result from the risk assessment
c. The Selection of controls
d. The Control objectives
e. The specific information security objectives
f. Specified Processes and resources and their classification

Management should establish and sustain a commitment to the overall measurement process. In implementing a measurement process Management should:

a. Accept the requirements for measurement see ISO 27004. for further details

b. The information needs, see ISO 27004. for further details

c. Obtain staff commitment by the following:

- The organization should demonstrate its commitment through, for example, a measurement policy for the organization, allocation of responsibility and duties, training, and the allocation of budget and other resources.

- A responsible person or organizational unit for the measurement program should be assigned.

- The person or organizational unit is responsible for communicating the ISMS measurement importance and results throughout the organization to ensure its acceptance and use and should have the management support

- Ensure that ISMS measures data is collected, analyzed, and reported to the CIO and other stakeholders.

- Educate program line managers about using results of ISMS measurement for policy, resource allocation, and budget decisions

The information security measurement program and the design should involve the following roles:

a. Senior Management

b. The users of the security products

c. The persons in charge of information systems

d. The persons in charge of information security

An Information Security Measurement Program is established in order to get indicators of the effectiveness of the ISMS, control objectives and controls. The program is described in ISO/IEC27004.
The result of the Plan Phase suitable measurements should be conducted to fulfill these objectives.
A suitable Information Security Measurement Programme could be different depending on the organization's:

a. Size

b. Complexity

c. Overall risk profile/need of information security

Generally the larger and more complex an organization is the more extensive measurement program is needed. But the level of overall risk is affecting the extent of measurement program as well. A by comparison smaller organization may need more comprehensive measurement program in order to cover the risk if the impact of poor information security is severe, than a larger organization that does not face the same impact. The extent of the measuring program can be evaluated based on the selection of controls that needs to be covered and the results from the risk analyze.

9.3.2.2 Designing the information security measurement program

The responsible for the information security measurement program has to consider the following:

a. Scope
b. Measurement Points?
c. Carry out the measurements
d. Periods of measurements
e. Reporting

The scope of the measuring program should at least cover the scope, control objectives and controls of the ISMS. In particular, should the objectives and boundaries of the ISMS Measurement be set in terms of the characteristics of the business, the organization, its location, assets, technology, and including details of and justification for any exclusion from the ISMS scope. This may be a single security control, a process, a system, a functional area, the whole enterprise, a single site, or a multi-site organization.

When selecting measurement "points" ISO/IEC27004 Information Security Measurement Process stipulates that the starting point is the object of measure. In order to establish a measurement program these objects must be identified. These objects could be a process or a resource. (See ISO/IEC27004 for further details). When defining the program the objects defined by ISMS scope is often broken down find the actual objects that should be measured. This defining process could be exemplified by the following example: The Organization is the overall object – Business Process A/or IT system X is a part of that object and constitutes an object in itself– Objects within that process that are affecting information security (People, Rules, Network, Applications, Facilities etc.) are generally the objects of measure in order to see the effectiveness of protecting information.

When implementing an Information Security Measurement Program care should be taken to the objects of measure could be serving many business processes within the ISMS scope and subsequently have a larger impact on the Effectiveness of the ISMS and Control objectives. Such

Objects should generally be prioritized with the scope of the program, such as the Security Organization and linked process, Computer Hall, Co-workers regarding information security etc.

The periodic of the measurement may vary but is preferable that the measurement is done or summarized with certain intervals in order to fit into the management review and the continual improvement process of the ISMS in order to be integrated. The design of the program must state this.

The reporting of the results should be designed so that communication is assured according to ISO27004.

The design of the Information Security Measurement program should be concluded in a document stipulating the procedure which should be approved by management. This document should cover the following:

a. Responsibilities for the Information Security Measurement Program
b. Responsibilities for communication
c. The scope of measurements
d. How it is going to be performed (basic method used, external, internal execution etc.)
e. When it should be performed
f. How it is reported

If the organization develops own measuring points, these have to be documented as part of the design phase, for further reference see ISO/IEC 27004. This document may be quite comprehensive and is not necessary needed to be signed by the management. This also due to that the details may change when implemented.

9.3.3 Measuring the effectiveness of the ISMS

When setting the scope for Information Security Measurement Program that should be implemented care should be taken so that the objects are not too many. If so there could be wise to divide the program into different parts. The scope of these parts may be seen as separate measurements for comparison. But the main purpose prevails that a combination of the measurements provides an indication to evaluate the ISMS effectiveness. These sub scopes are normally an organizational unit that could be defined with clear boundaries. A combination of objects that serves many business processes and the measurements of objects within the sub scopes may together form a proper scope for the Information Security Measurement Program. This could also be seen as a series of ISMS activities that can be regarded as constructed with two or more processes/objects. Therefore, the effectiveness of the entire ISMS can be measured based on measuring the results of these two or more processes/objects.

As the objectives are to measure the effectiveness of the ISMS, it is important to measure the control objectives and controls. A sufficient number of controls are one aspect and that these controls are sufficient for evaluating the effectiveness of the ISMS is the other aspect. (There may be other reasons for limiting the scope of the Information Security Measurement Program, which is mentioned in ISO/IEC 27004).

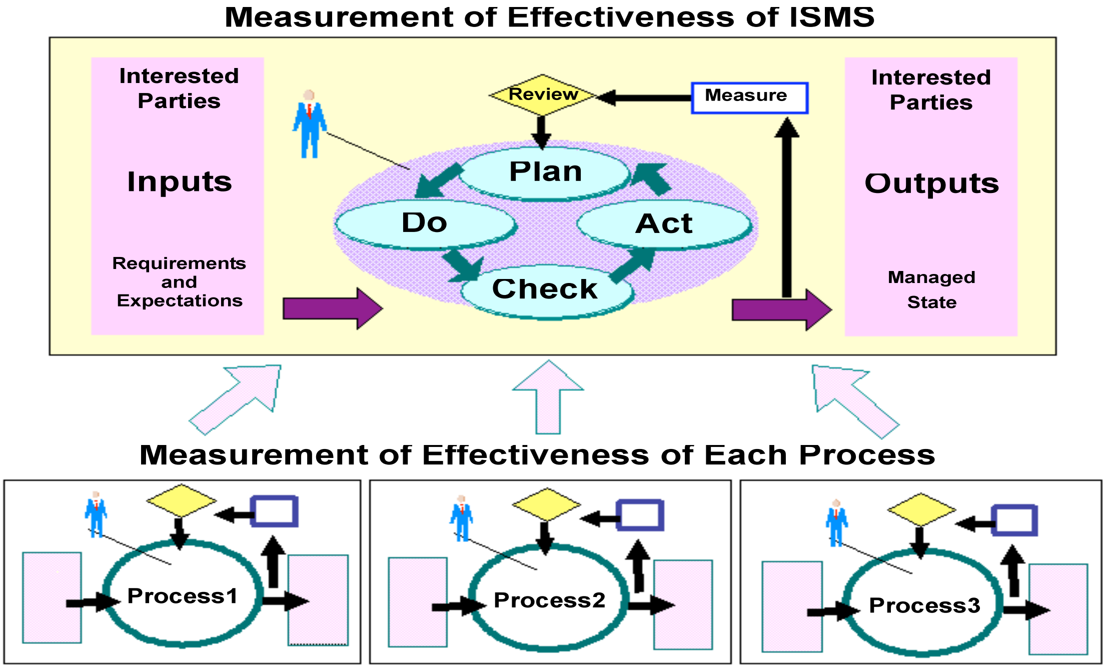


Figure 9.3.3 two aspects of measurement effectiveness with the PDCA process of ISMS and the examples of process within the organization.

When using measurement results for evaluating the effectiveness of ISMS, Control objectives and controls it is essential that the management is aware of the scope of the Information Security Measurement Program. The responsible for the measuring program should have the management approval for the scope of the information Security Measurement Program prior to launch.

Note 1:
The requirement related to the measurement of effectiveness in ISO/IEC 27001 is "the measurement of controls or series of controls." (see 4.2.2 d) in ISO/IEC 27001)
Note 2:
The requirement related to the effectiveness of the entire ISMS in ISO/IEC 27001 is only a "review of the effectiveness of the entire ISMS", and "the measurement of the entire ISMS" is not required. (See 0.2.2 in ISO/IEC 27001).

The actual carrying out of measurements could be done using internal personnel or external or a combination. The size, structure and culture of the organization are factors to consider when evaluating internal or external resources. Small and medium size companies have more to benefit from using external support than larger organizations. The result from using external resources could also provide a more valid result depending on the culture. If the organization is used to internal audits internal resources may be as valid.

9.4 Requirements for ISMS recording

Activity Objective: To establish necessary formats for recording and publishing formal information of the ISMS.

9.4.1 Documentation Requirements

9.4.1.1 Controlling documentation and records

It is required that the documentation for ISMS should include records of management decisions, ensure that actions are traceable to management decisions, policies, the recorded results are reproducible.

It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives. In ISMS activities, the risk assessment and treatment processes are implemented along with the ISMS policy and objectives indicated by management, and based on the results, controls are selected.

The documents indicate the evidences that controls are selected based on the results of risk assessment and risk treatment, and such processes are implemented along with the ISMS policy and objectives. Procedures of risk assessment and measurement of effectiveness tend to have different interpretations by each person. However in such cases, it is difficult to compare the results by different people and it makes it difficult to manage the information security effectively.

Documentation is essential for the reproducibility of these results and procedures. As for selected controls, the establishment and documentation of the procedures are required for a person who executes it.

The ISMS documentation is required to include documented statements of the ISMS policy and objectives, the scope of the ISMS, procedures and controls in support of the ISMS, a description of the risk assessment methodology, the risk assessment report, the risk treatment plan, and the Statement of Applicability.

9.4.1.2 Controlling of documents

As for ISMS documents, it is necessary for the version and to be managed and made available whenever necessary for a person who needs it. It is necessary to establish the administrative procedure of the ISMS document management and to manage the document which includes the approval of documents for adequacy prior to issue, updated documents, ensuring that changes and the current revision status of documents are identified.

It is important that relevant versions of applicable documents are available at points of use, ensuring that documents remain legible, readily identifiable, transferred, stored and ultimately, disposed of in accordance with the procedures applicable to their classification. In addition ensuring that documents of external origin are identified, that the distribution of documents is controlled, preventing the unintended use of obsolete documents, and applying suitable identification to them if they are retained for any purpose.

9.4.1.3 Controlling of Records

Records should be created, maintained and controlled as evidence that the ISMS of the organization conforms to ISO/IEC 27001 and to show the effects of operations.

It is also required to keep records of implementation status in the entire PDCA Phase, and records of all the security-related troubles and accidents concerning ISMS such as incident and event records, records of education, training, skills, experience and qualifications, internal ISMS audits, corrective and preventive actions, and organizational records.

The following tasks should be performed to control records.

a. Documenting the controls required to identify data, store it, protect it, search it, and discard it, and documenting its storage duration
b. Defining what should be record, and in what scope, in the operation management process
c. When any period of retention is specified by the Commercial Code or any other legislation, the period of retentions should be set pursuant to such legal requirement.

9.5 Produce the ISMS Implementation Plan

Activity Objective: To complete the project plan for the implementation phase of the ISMS project with necessary activities for implementing the selected controls within organizational, ICT and Physical security as well as formal activities related to the ISMS as described in ISO/IEC 27001

The conclusion of the selection of the controls, as well as other ISMS related activities planned for, and how to implement them should be formalized in a project plan. The project plan should follow general criteria for handling a project properly and could be supported by general tools and methods. As an ISMS project involves many different roles in the organization it is important that the activities is clearly designated to responsible and that the plan and the responsible are communicated early in the project and widely throughout the organization.

As with all projects it is of course essential that the project responsible ensure that enough resources have been planned and allocated for the project.

10 Implementing the ISMS

At this point, the ISMS business case has been approved, the ISMS scope and ISMS policy has been defined and information assets and the results of the gap analysis are known. The risk assessment plan, description, and assessment report are also available. Now the ISMS implementation plan, recording and publication process are also available.

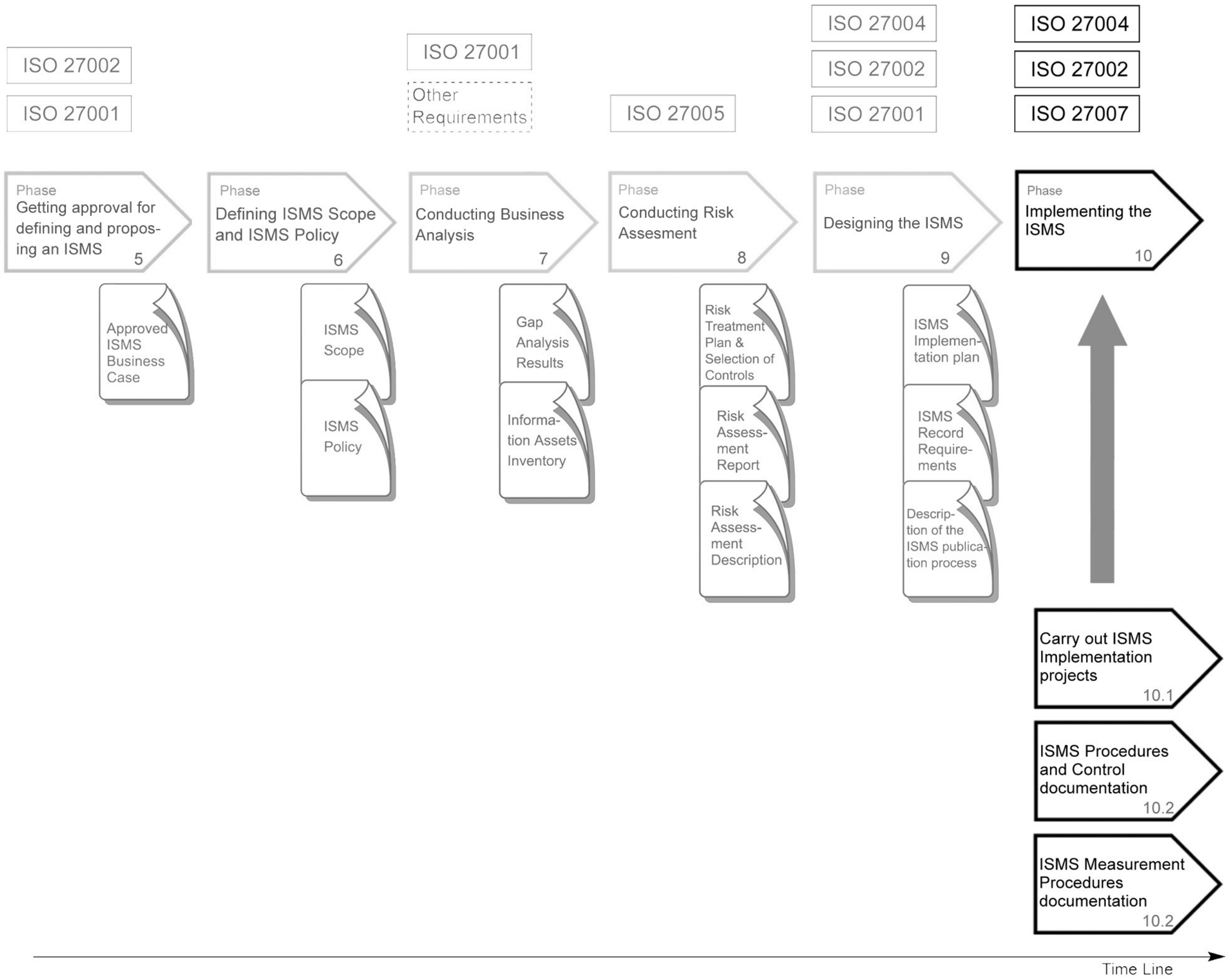

ISO 27002
ISO 27001
ISO 27001
Other Requirements
ISO 27005
ISO 27004
ISO 27002
ISO 27001
ISO 27004
ISO 27002
ISO 27007
Phase
Getting approval for defining and proposing an ISMS
5
Phase
Defining ISMS Scope and ISMS Policy
6
Phase
Conducting Business Analysis
7
Phase
Conducting Risk Assesment
8
Phase
Designing the ISMS
9
Phase
Implementing the ISMS
10
Approved ISMS Business Case
ISMS Scope
ISMS Policy
Gap Analysis Results
Information Assets Inventory
Risk Treatment Plan & Selection of Controls
Risk Assessment Report
Risk Assessment Description
ISMS Implementation plan
ISMS Record Requirements
Description of the ISMS publication process
Carry out ISMS Implementation projects
10.1
ISMS Procedures and Control documentation
10.2
ISMS Measurement Procedures documentation
10.2
Time Line

Figure 10.1. Overview of the implementation phase and its main activities

The objectives of the "Implementing the ISMS" phase are:

- Implement selected controls according to plan
- Set up of Measurement procedure
- Set up of audit procedure
- Create awareness
- Set up of monitoring and review

The different activities that form the overall project have their own objectives primary related to the controls in 27002 as well as additional controls selected (for an example of implementation of controls see Appendix B). Also activities related to 27001 are included as described above.

The phase includes basically to carry out the activities designed in the implementation plan and if proper done the objectives is reached.

10.1 Carry out ISMS Implementation Projects

Activity Objective: To implement the sub projects for the selected controls and ISMS related subjects

10.1.1 Responsibilities and roles

When designing the ISMS a number of projects have been defined. These projects will be assigned to different responsibilities within the organization (please see Appendix X for example of roles). Preconditions for the project are that the management as stipulated in ISO/IEC 27001 clause 5.2.1 allocates the sufficient resources.

10.1.2 Communication

Apart from handling the project in a proper manner it is also advisable that the project responsible keep a regular dialogue with opinion influencers on the implementation within the organization even if they are not active as part of the project.
It is also a beneficial for the implementation if the management can communicate the importance of the project especially in the internal communications.

10.1.3 Coordination

It is essential that the responsible for the complete implementation project keep track of the different activities so that the logical flow of events can be obtained. This especially linked to the particular activities mentioned in the bullet list above. For example there is no point in carrying out a broad training activity if not the proper instructions are in place or that the technical solutions are missing.

10.1.4 Changes

Implementing an ISMS will involve basically the whole organization within the scope it will take some time and it is likely that there will be changes. It is essential for a successful implementation of an ISMS that the overall project are aware of and can handle these changes, make proper adjustments and report back to management if there is major implications. Typical changes are:

a. Changes in the organization such as:
   - Change in top management (new commitment must be assured)
   - Reorganization of departments etc.
   - Mergers
   - Outsourcing

b. Changes in technical environment such as:
   - New systems
   - New Platforms
   - New communication
   - New buildings

c. Legal or contractual changes such as:
   - New client obligations
   - New legislation

The importance is not make dramatic changes in the implementation project but aware that changes may have an impact on the initial decided scope and objectives as well as selected controls.

It may be the case that the implementation cannot consider some of these changes without risking the success of the whole implementation, and if so it should be clearly stated by the management.

10.2 Implementation of monitoring

Activity objective: To implement routine checking as monitoring.

As a part of monitoring is routine checking which is the routine performance of the implemented controls as described in other subprojects in the ISMS implementation this needs to be noted especially. This could involve some checking that employees do is not described as a control (e.g. checking on old invoices when chasing debts, confirming the analysis of numbers in management reports, following up customer queries, investigating IDS anomalies or system crashes etc). In the course of these checks errors or security incidents may be detected and these should be reported and corrected in a consistent manner.

The objective with the monitoring is to maintain the consistency with the objectives and the results, change the expressions like below.

Monitoring activities should be pre-defined in organizational standards and procedures during the Do phase. In this step, monitoring should be performed continuously and accumulate the monitoring results along the pre-defined rules above. Throughout these continuous monitoring activities, prompt detection of errors in the processing results should be achieved, and prompt identification of security breaches and incidents attempted should also be achieved whether they succeeded or not.

It should be recognized that monitoring activities do not perform as expected when they are performed independently. These activities should be performed considering the relationships of other activities, especially other Check phase's activities, reviews, measurements and audits. If security breaches or incidents happen, or if errors in the processing results are found, prompt and effective reactions should be ensured to the monitoring activities. Accumulated monitoring results should be reviewed or should be used in audits for improvements.

On the other hand, it should also be recognized that continuous monitoring is performed to check the ISMS, however these activities are performed in daily ISMS operations which are distributed in the Do phase.

To implement the monitoring work correctly, the following should be done:

a. Make the organization standards and procedures about monitoring, and operate along these rules, and
b. Make these rules known to everyone who are responsible for monitoring, and if necessary plan and do the trainings.

Of course, the continuous operation of monitoring along the rules should be maintained throughout the ISMS operations. In addition, it is also important that monitoring work is performed by all staff, particularly supervisory staff. Supervisory duties include determining that the procedures in place are being performed satisfactorily.

10.3 ISMS Procedures and Control Documentation

Activity Objective: To create and update necessary ISMS procedures and control documentation

The implementation of documentation needed depends on controls selected and the record requirements and publication process set forth in the design of the ISMS.

Generally the necessary documentation for procedures and controls should be documented to such an extent that information security can be achieved even if the personnel are changed.
They should have a logical structure and should be possible to easy update.

The documentation should among other cover implementation plans for the following activities in particular:

a. Documentation of audit procedure of the ISMS
b. Documentation of training procedure of the ISMS
c. Documentation of monitoring procedure of the ISMS
d. Documentation of review procedure of the ISMS

Apart from the regulatory framework documentation for information security within the organization there may be subsets of other documentation that is essential for a successful implementation. To which extent these are included in the ISMS implementation project may vary depending on the implementation plan. As this type of documentation also is mostly only possible to create after the implementation of the ISMS is done, it is not likely that it is included in the actual implementation phase. However it is important that the implementation phase is aware of the need for these types of documentation. The following documentation types are samples only that should be considered:

1. Technical documentation and documentation of work procedures (target group: experts)
When malfunctions or information security incidents occur, it must be possible to restore the desired nominal conditions of the business processes. Technical details and work procedures must therefore be documented such that this can be achieved within a reasonable amount of time.
Examples of this are instructions for installing IT applications, backing up data, restoring data backups, restarting an application server after a power failure as well as the documentation for testing and approval procedures and instructions on what to do when malfunctions and information security incidents occur.

2. Instructions for users (target group: users)
Work procedures, organizational stipulations and technical information security measures must be documented such that information security incidents caused by a lack of knowledge or mistakes can be avoided. Examples of this are security guidelines for the usage of e-mail and the Internet, information on how to prevent infection by viruses or on how to recognise social engineering as well as rules of conduct for users if they suspect an information security incident has occurred.

3. Reports for management tasks (target group: management level)
All the information that the management requires in order to fulfil its management and supervisory duties must be recorded with the required level of detail (e.g. results of audits, measurements of effectiveness, reports on information security incidents).
The problems, successes and opportunities for improvements should be pointed out. The management reports must contain all the information regarding the management of the information security process that is necessary for the management level.
This information includes, for example:

a. An overview of the current status in the information security process
b. A report on the follow-up action taken after previous management appraisals
c. Feedback from customers and staff members
d. An overview of new threats and security vulnerabilities that have emerged

The management level takes note of the management reports and makes the necessary decisions pertaining to, for example, improvements to the security process, the demand for resources as well as to the results of security analyses (e.g. minimisation, absorption or acceptance of risks).

4. Recording management decisions (target group: management level)
The management level must record and account for the selected information security strategy. Furthermore, decisions affecting aspects relevant to security that are taken on all the other levels must also be recorded to ensure they can be comprehended and repeated at any time.

The monitoring is performed in the usual way for supervision of work. Where staff is experiencing problems the following should be addressed:

a. problems are reported appropriately
b. solution is found
c. better way of doing things is found

These problems may be real or potential information security issues or they may be normal business

10.4 ISMS Measurement Procedure Documentation

Activity Objective: To document necessary procedures etc. within the information security measurement program

It is essential that during implementation phase that consideration is taken to how measurement of the effectiveness should be addressed. Further information about an information security measurement program can be found in ISO/IEC 27004.

11 Bibliography

ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC 31000

Annex A: Example Templates

1. *Contributions for Templates supporting the deliverables noted in the document*

2. *Example of Selection of Controls*

Table 1: Sample Mapping Examples

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.5	**Security Policy**		
A.5.1	Information Security Policy		
A.5.1.1	Information Security policy document	An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.	**PARTIAL**[2]
A.5.1.2	Review of the information security policy	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	N/A
A.6	**Organizational of Information Security**		
A.6.1	Internal Organization		
A.6.1.1	Management commitment to information security	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.	N/A
A.6.1.2	Information security coordination	Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions.	N/A
A.6.1.3	Allocation of information security responsibilities	All information security responsibilities shall be clearly defined.	N/A
A.6.1.4	Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be defined and implemented.	N/A

[1] Each applicable (partial, full, ECS) item in this table have a separate rationale.

[2] Please refer to the rationale for A5.1.1 described in the section called Mapping examples

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.6.1.5	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.	**Partial**
A.6.1.6	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	N/A
A.6.1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	N/A
A.6.1.8	Independent review of information security	The organization's 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 to the security implementation occur.	**Partial**
A.6.2	External Parties		
A.6.2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.	**Partial**
A.6.2.2	Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.	**Full**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.6.2.3	Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.	**Full**
A.7	**Asset Management**		
A.7.1	Responsibility for assets		
A.7.1.1	Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.	**Full**
A.7.1.2	Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designated part of the organization.	**Partial**
A.7.1.3	Acceptable use of assets	Rules for acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.	**Partial**
A.7.2	Information classification		
A.7.2.1	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.	**Partial**
A.7.2.2	Information labeling and handling	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.	N/A
A.8	**Human Resources Security**		
A.8.1	Prior to employment		
A.8.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information	N/A

ISO/IEC 27001 Number	**Control Objective/Control Name**	**Control Description**	**Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]**
		security policy.	
A.8.1.2	Screening	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy. <Note: This doesn't seem to have anything to do w/ screening.>	N/A
A.8.1.3	Terms and conditions of employment	As part of the contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract which shall state their and the organization's responsibilities for information security.	N/A
A.8.2	During employment		
A.8.2.1	Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	N/A
A.8.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training regular updates in organizational policies and procedures, as relevant for their job description.	**Partial**
A.8.2.3	Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.	N/A
A.8.3	Termination of change of employment		

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.8.3.1	Termination responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	N/A
A.8.3.2	Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.	N/A
A.8.3.3	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	N/A
A.9	**Physical and Environment Security**		
A.9.1	Secure Areas		
A.9.1.1	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.	**Partial**
A.9.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	**Partial**
A.9.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied.	**Partial**
A.9.1.4	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster shall be designed and applied.	**Partial**
A.9.1.5	Working in secure areas	Physical protection and guidelines for working in secure areas shall be designed and applied.	**Partial**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.9.1.6	Public access, delivery and loading areas.	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	**Partial**
A.9.2	Equipment security		
A.9.2.1	Equipment sitting and protection	Equipment shall be sited or protested to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	**Partial**
A.9.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	**Partial**
A.9.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	**Partial**
A.9.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	**Partial**
A.9.2.5	Security of equipment off-premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.	**Partial**
A.9.2.6	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	**Partial**
A.9.2.7	Removal of property	Equipment, information or software shall not be taken off-site without prior authorization.	**Partial**
A.10	**Communications and Operations Management**		
A.10.1	Operational procedures and responsibilities		

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.10.1.1	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.	**Partial**
A.10.1.2	Change management	Changes to information processing facilities and systems shall be controlled.	N/A
A.10.1.3	Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	**Partial**
A.10.1.4	Separation of development, test and operational facilities	Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.	N/A
A.10.2	Third party service delivery management		
A.10.2.1	Service delivery	It shall be ensured that security options, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	**Partial**
A.10.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.	**Partial**
A.10.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking into account of the criticality of business systems and processes involved and re-assessment of risks.	**Partial**
A.10.3	System planning and acceptance		

ISO/IEC 27001 Number	**Control Objective/Control Name**	**Control Description**	**Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]**
A.10.3.1	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	N/A
A.10.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.	**Partial**
A.10.4	Protection against malicious and mobile code		
A.10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	**Full**
A.10.4.2	Controls against mobile code	Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.	**Full**
A.10.5	Back-up		
A.10.5.1	Information Back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	**Partial**
A.10.6	Network Security Management		
A.10.6.1	Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	**Full**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.10.6.2	Security of network services	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	**Partial**
A.10.7	Media handling		
A.10.7.1	Management of removal media	There shall be procedures in place for the management of removable media.	**Partial**
A.10.7.2	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.	**Partial**
A.10.7.3	Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.	**Partial**
A.10.7.4	Security of system documentation	System documentation shall be protected against unauthorized access.	**Partial**
A.10.8	Exchange of information		
A.10.8.1	Information exchange policies and procedures	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.	**Partial**
A.10.8.2	Exchange agreements	Agreements shall be established for the exchange of information and software between the organization and external parties.	N/A
A.10.8.3	Physical media in transit	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	**Partial**
A.10.8.4	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	**Full**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.10.8.5	Business information systems	Polices and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.	**Partial**
A.10.9	Electronic commerce services		
A.10.9.1	Electronic commerce	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	**Full**
A.10.9.2	On-line transactions	Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	**Full**
A.10.9.3	Publicly available information	The integrity of information being made available of publicly available system shall be protected to prevent unauthorized modification.	**Full**
A.10.10	Monitoring		
A.10.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	**Full**
A.10.10.2	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	**Partial**
A.10.10.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	**Full**
A.10.10.4	Administrator and operator logs	System administrator and system operator activities shall be logged.	**Full**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.10.10.5	Fault logging	Faults shall be logged, analyzed, and appropriate action taken.	N/A
A.10.10.6	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	N/A
A.11	**Access Control**		
A.11.1	Business requirement for access control		
A.11.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.	**Partial**
A.11.2	User access management		
A.11.2.1	User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	N/A
A.11.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.	**Full**
A.11.2.3	Use password management	The allocation of passwords shall be controlled through a formal management process.	**Partial**
A.11.2.4	Review of user access rights	Management shall review user's access rights at regular intervals using a formal process.	**Partial**
A.11.3	User responsibilities		
A.11.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	**Full**
A.11.3.2	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	**Partial**
A.11.3.3	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.	**Partial**

ISO/IEC 27001 Number	**Control Objective/Control Name**	**Control Description**	**Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1**[1]
A.11.4	Network access control		
A.11.4.1	Policy on use of network services	Users shall only be provided with access to the services that they have been specifically authorized to use.	**Full**
A.11.4.2	User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.	**Full**
A.11.4.3	Equipment identification in networks	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.	**Full**
A.11.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports shall be controlled.	**Full**
A.11.4.5	Segregation in networks	Groups of information services, users, and information systems shall be segregated on networks.	**Full**
A.11.4.6	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.	**Full**
A.11.4.7	Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	**Full**
A.11.5	Operating system access control		
A.11.5.1	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.	**Full**
A.11.5.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	**Full**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.11.5.3	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.	**Full**
A.11.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	**Full**
A.11.5.5	Session time-out	Inactive sessions shall shut down after a defined period of inactivity.	**Full**
A.11.5.6	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.	**Full**
A.11.6	Application and information access restriction		
A.11.6.1	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	**Full**
A.11.6.2	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.	**Partial**
A.11.7	Mobile computing and teleworking		
A.11.7.1	Mobile computing and communications	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communications facilities.	**Partial**
A.11.7.2	Teleworking	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.	**Partial**
A.12	**Information Systems Acquisition, Development and Maintenance**		
A.12.1	Security requirements of information systems		

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.12.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.	**Full**
A.12.2	Correct processing in applications		
A.12.2.1	Input data validation	Data input to applications shall be validated to ensure that this data is correct and appropriate.	**Partial**
A.12.2.2	Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	**Partial**
A.12.2.3	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.	**Full**
A.12.2.4	Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	**Partial**
A.12.3	Cryptographic controls		
A.12.3.1	Policy on use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	**Partial**
A.12.3.2	Key management	Key management shall be in place to support the organization's use or cryptographic techniques.	**Partial**
A.12.4	Security of systems files		
A.12.4.1	Control of operational software	There shall be procedures in place to control the installation of software on operational systems	**Partial**
A.12.4.2	Protection of system test data	Test data shall be selected carefully, and protected and controlled.	**Partial**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.12.4.3	Access control to program source code	Access to program source code shall be restricted.	**Partial**
A.12.5	Security in development and support process		
A.12.5.1	Change control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.	**Partial**
A.12.5.2	Technical review of applications after operating system changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	**Partial**
A.12.5.3	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	**Partial**
A.12.5.4	Information leakage	Opportunities for information leakage shall be prevented.	**Partial**
A.12.5.5	Outsourced software development	Outsourced software development shall be supervised and monitored by the organization.	**Partial**
A.12.6	Technical Vulnerability Management		
A.12.6.1	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	**Full**
A.13	**Information Security Incident Management**		
A.13.1	Reporting information security events and weaknesses		
A.13.1.1	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	N/A

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.13.1.2	Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	**Partial**
A.13.2	Management of information security incidents and improvements		
A.13.2.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	**Partial**
A.13.2.2	Learning from information security incidents	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	**Full**
A.13.2.3	Collection of evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	N/A
A.14	**Business Continuity Management**		
A.14.1	Information security aspects of business continuity management		
A.14.1.1	Including information security in the business continuity management process	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	**Partial**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.14.1.2	Business continuity and risk assessment	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	**Full**
A.14.1.3	Developing and implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	**Partial**
A.14.1.4	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	**Partial**
A.14.1.5	Testing, maintaining and reassessing business continuity plans	Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.	N/A
A.15	**Compliance**		
A.15.1	Compliance with legal requirements		
A.15.1.1	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.	**Partial**
A.15.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	**Partial**

ISO/IEC 27001 Number	Control Objective/Control Name	Control Description	Applicability of ISO/IEC 27001 to Network Security Guidelines per Figure A.1[1]
A.15.1.3	Protection of organizational records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	**Partial**
A.15.1.4	Data protection and privacy of personal information	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and if applicable, contractual clauses.	**Partial**
A.15.1.5	Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorized purposes.	**Partial**
A.15.1.6	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.	**Partial**
A.15.2	Compliance with security policies and standards, and technical compliance		
A.15.2.1	Compliance with security policies and standards	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security practices and standards.	**Partial**
A.15.2.2	Technical compliance checking	Information systems shall be regularly checked for compliance with security policies and standards.	**Full**
A.15.3	Information systems audit considerations		
A.15.3.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to businesses processes.	**Partial**
A.15.3.2	Protection of information systems audit tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	**Full**

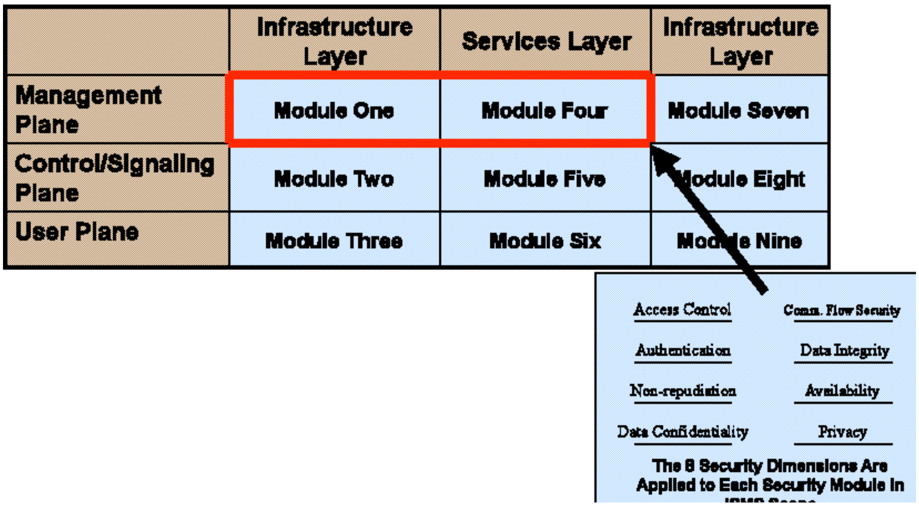
Example 1: Supporting the Plan Phase of Implementing an ISMS ISO/IEC 27001

The purpose of this case study is to demonstrate an industry example using in conjunction with ISO/IEC 27001/2 to establish, implement and operate an Information Security Management System (ISMS). This example shows a sector-specific viable framework used in conjunction with ISO/IEC 27001/2 controls that need to be applied in an end-to-end network.

ISO/IEC 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS within the context of an organization's overall business activities and the risks that it faces. Although ISO/IEC 27001 provides a list of steps that must be performed to accomplish each of the above phases, additional technical guidance on the specific actions that need to be performed for each step is needed for network guidance. This technical guidance is provided via Figure A.1.

As shown in Figure A.1 for a given ISMS scope, decomposes an IT product, service or solution into a layered hierarchy of equipment and facilities groupings and examines the types of activities that occur at each layer in a standardized manner. This consists of: (1) the infrastructure security, (2) the services security, and (3) the applications security. In addition, the three types of activities that can occur are: (1) management or known as operations security, (2) signaling security, and (3) end-user security.

ISO/IEC 27001/2 control objectives and controls are identified to mitigate threats and vulnerabilities. The eight security mechanisms shown in Figure A.1 provide further guidance required to implement and operate the ISO/IEC 27001/2 controls and provide the basis for additional control objectives not listed in ISO/IEC 27001 Annex A.



	Infrastructure Layer	Services Layer	Infrastructure Layer
Management Plane	Module One	Module Four	Module Seven
Control/Signaling Plane	Module Two	Module Five	Module Eight
User Plane	Module Three	Module Six	Module Nine

Figure A.1: Tabular Form of Network Security Requirements Applied to ISMS Scope

The intersection of a security plane and layer represents a security module that can be included or excluded depending on the scope of the ISMS being established. From the figure, one can see that if the ISMS is being established for the management of information infrastructure and information services. Modules one and two are in scope.

For the purposes of this case study, consider establishing, implementing and operating an ISMS for the management of the information infrastructure and services of a large enterprise that stores its employee information in a data center.

The scope is therefore as depicted in Figure A.2. This scope does not represent everything that is required for the implementation of an enterprise-wide ISMS, but is broad enough to demonstrate how is used in conjunction with ISO/IEC 27001/2 to establish, implement and operate an Information Security Management System (ISMS). The same types of activities are performed if the applications, control plane, and end-user are also included in the ISMS scope.

The employee information stored in the data center also includes personal information that should be restricted to authorized users only. Protecting this employee information is defined to be within the scope and boundaries of this ISMS and has been identified through the ISMS asset identification and valuation process as an essential asset that needs protection. The employee information is accessed by several support organizations employed by the enterprise, one of which is the help desk; in addition, the data centre and systems contained therein are maintained by the corporate IT organization.

As seen in Figure A.2, the Help Desk accesses the employee information for handling complaints, supporting orders for new IT services, resolving problems employees are having with IT services (e.g., remote access), etc. In addition, the Corporate IT organization accesses the employee information as part of its maintenance activities of file system maintenance, system updates, patch management, etc.

Figure A.2: Access Scenario for Enterprise Asset

As part of establishing, implementing and operating an ISMS for the management of the information infrastructure and services, the technical management, infrastructure, and services of the employee information are analyzed as part of a risk assessment. This analysis reveals that the employee information is accessed by the enterprise's help desk as part of service management (e.g., managing employee remote access service) as well as by the enterprise's corporate IT organization as part of infrastructure management (e.g., performing backups). At this point, the analysis is performed in concert with the ISMS risk assessment to identify threats and vulnerabilities in the technical management or operations activity of the employee information's infrastructure and services. In this example, the analysis reveals that members of the corporate IT organization can view and modify the employee information thereby making it vulnerable to disclosure and corruption in the infrastructure layer. In addition, as part of performing problem resolution, employee information is transmitted in the clear between the data center and the help desk; thereby making it vulnerable to disclosure, corruption and interception in the services layer as depicted in Figure A.3

Figure A.3 : Threat and Vulnerability Analysis for Enterprise Asset

Continuing with the process used to establish an ISMS, at this point a risk analysis is performed that assesses the business impacts upon the organization that might result from security failures in the employee information as well as the realistic likelihood that these security failures would occur in light of the prevailing threats, vulnerabilities, and the controls currently implemented by the enterprise. This analysis culminates in a decision by the organization to apply controls, accept the risk, avoid the risk, or transfer the risk.

For the purposes of this case study, a conclusion of the risk analysis is that controls need to be applied to protect employee information from the previously identified threats and vulnerabilities. Hence, as part of establishing the ISMS, control objectives and controls must be identified and selected to protect employee information against threats and vulnerabilities in the management plane of its infrastructure and services layers.

Continuing with the example, ISO/IEC 27001 Control A.10.9.2 is identified and selected as being required to protect the management of employee information in the services and infrastructure layers due to the vulnerabilities and threats identified there by the risk analysis. This is depicted in Figure A.4.

ISO/IEC 27001 Control A.10.9.2 states that *information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.*

Management approval of the residual risks and management authorization to implement and operate the ISMS is then obtained and a statement of applicability is prepared to provide a summary of decisions concerning risk treatment as the remaining steps of establishing an ISMS.

Figure A.4: Using Sector Specific Guidelines to Determine where Apply ISO/IEC 27001 Controls

As part of implementing and operating the enterprise's ISMS, the sector specific information from Figure A.1 provide explicit implementation and operation guidance for Control A.10.9.2 in the services and infrastructure layers for the employee information asset. Figure A.6 depicts how the implementation and operation of control A.10.9.2 is needed to protect the employee information asset.

In the services, Communications Flow Security ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points) and therefore provides for the use of VPNs to prevent misrouting.

Data Integrity ensures the correctness or accuracy (i.e., data are only processed by authorized processes or actions of authorized people or devices) of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities. Data Integrity provides for the use of IPSec AH[3] in the services layer to prevent incomplete transmission, unauthorized message alteration and duplication as well as prevent message replay. In the infrastructure, the Data Integrity dimension provides for the use of file checksums to detect unauthorized alteration.

Data Confidentiality protects data from unauthorized disclosure and provides for the use of IPSec ESP[4] in the services layer to prevent unauthorized disclosure. In the infrastructure layer, the Data Confidentiality dimension provides for the use of file encryption.

In the infrastructure, Access Control provides authorization for the use of the network resources. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. Access Control provides the use of file system access control lists (ACLs) to prevent unauthorized duplication.

Therefore, as a result of using sector specific information to establish, implement and operate an ISMS, the enterprise decides to deploy IPSec VPNs with authentication headers (IPSec AH) and encapsulated security protocol (IPSec ESP) enabled to protect the transmission of employee information between the data centre and help desk. The enterprise also decides to protect the employee identification database with ACLs as well as to encrypt and include checksums in the database to protect the employee information from unauthorized access by the corporate IT organization.

[3] For information on IPSec AH see http://www.ietf.org/rfc/rfc1825.txt.

[4] For information on IPSec ESP see http://www.ietf.org/rfc/rfc1825.txt.

Figure A.5: Industry specific Implementation and Operation Details for ISO/IEC 27001 Controls

Finally, to complete the implementation and begin operation of the ISMS, the enterprise performs the following activities contained in ISO/IEC 27001:

- Formulates and implements a risk treatment plan,
- Defines how to measure the effectiveness of controls and how these measurements are to be used to assess control effectiveness,
- Implements training and awareness programs,
- Manages the operation of and resources for the ISMS,
- Implements procedures and other controls capable of enabling prompt detection of security events in response to security incidents.

In conclusion, this case study demonstrates how industry specific network security standards enhance ISO/IEC 27001.

The necessary ISO/IEC 27001 controls and incorporates granularity in terms of which assets and activities they should be applied to. Additional granularity is provided for the guidance of the implementation and operation of ISO/IEC 27001 controls to different layers and planes. This provides comprehensive end-to-end security by applying, implementing and operating security controls in a holistic, standardized manner.

X.4.1.1 Industry example in concert with ISO/IEC 27001

Figure A.1 shows the partitioning of a telecommunications network into a three-layered hierarchy of equipment and facilities groupings: (1) the infrastructure security layer, (2) the services security layer, and (3) the applications security layer. This defines the three types of activities that can occur at every layer as security planes. The three security planes or activities present at every layer are: (1) management security plane, (2) control/signalling security plane, and (3) end-user security plane. Further granularity is achieved by looking at security mechanisms or dimensions to secure each security layer/plane combination.

This example defines guidelines that support the application of the ISO/IEC 18028-2 security layers, planes and dimensions to the ISO/IEC 27001 model for the establishment, implementation and operation of an ISMS.

x.4.1.2 Mapping example

The following provides two examples of the nature of the analysis and structure of the control sections.

[A.]5.1.1 Information security policy document

Control

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Network Security : Applicable __X__ Not Applicable ______.

Layer(s) or Asset(s): All

Planes(s) or Activities: All

Dimensions(s) or Mechanisms: All

Rationale: The implementation guidance for the information security policy document states that the policy must set out the organization's approach to managing information security. The information security policy identifies the priority the organization places on each technical security dimension and provides the organization's approach to managing information security in each asset and activity.

[A.]10.9.2 On-Line Transactions

Control

Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Network Security: Applicable __X__ Not Applicable ______.

Layers(s) or Asset(s): Services, Infrastructure, Applications

Planes(s) or Activities: Management or Operations , End-User

Dimensions(s) or Mechanisms: Data Integrity, Data Confidentiality, Communications Security, and Access Control

Rationale: In order to protect information involved in on-line transactions, the assets and activities are used to determine the necessary controls (in this case control 10.9.2), and where they need to be applied, for on-line transactions. The dimensions specify measures required to implement and operate the control. For example: implementing IPSec AH of the data integrity dimension to prevent unauthorized message alteration in the services layer and IPSec ESP of the data confidentiality dimension to prevent unauthorized disclosure in the services layer.[5]

The following table addresses how the ISMS RCL applies to the requirements of network security

x.4.1.3 Example Results in creating ECS using Network Security

The following table identifies the applicability of network security guidelines to each ISO/IEC 27001/2 control. With respect to a given ISO/IEC 27001/2 control may be one of the following:

Not Applicable (N/A). The ISMS control covers an area not required by the reference source.

[5] Refer to the case study (Creation of Extended Control Set Using network security standards in earlier section)

Partially Applicable (Partial). ISO/IEC 27001/2 provides guidance for a portion of the establishment, implementation, operation, monitoring, reviewing, maintaining and improving the control.

Fully Applicable (Full). ISO/IEC 27001/2 provides guidance for the complete establishment, implementation, operation, monitoring, reviewing, maintaining and improving the control.

Separately an additional aspect that is discussed and incorporated in a separate contribution shows how extended control sets (ECS) can be created. The definition of ECS used in this context is the following:

Extended Control Set (ECS)[6]. Network Security guidance how to extend the establishment, implementation, operation, monitoring, reviewing, maintaining and improving the control in order to make it more effective.

Per the stages noted earlier, extended control set should also be identified from what is not contained in the current ISO/IEC 27001. For sake of simplicity, the following table shows example results in using Network security guidelines itemizing Partial, Fully Applicable and Not Applicable.

[6] Extended Control Set can be derived from the process described earlier. Extended Controls expect to come from looking at the reference source and noting what is not in ISO/IEC 27001 as well as noting what is the current controls in the ISO 27001 and how it meets reference source requirements.

Annex B Conformity mapping example

Both ISO/IEC 27001and ISO/IEC 27002 recognize the potential need to add additional controls, and encourage implementers to do so when their circumstances require it. This section gives guidance on how to identify and use extended controls in concert with ISO 27001 to implement a robust ISMS that meets the business objectives of the organization, and supports this guidance with examples of how to map the ISMS controls with those from real global industry examples. This section addresses those issues in three parts: it first describes, at a high level of abstraction, a Conformity mapping model which takes into account specific legal, regulatory, technical, and policy requirements, and other chosen standards[7], against which an organization may have to, or may wish to, show their compliance / conformity. This may introduce the need to define and implement additional controls, beyond those defined in Reference Control List (RCL) of ISO/IEC 27001 Annex A. It then describes a detail mapping process for performing a mapping exercise between a selected reference source and the RCL. This offers additional guidance when implementing the ISMS process.

The final part gives industry examples of the results of the mapping process.

Conformity mapping model

The model has four components which map, or channel, the organization's goal conformity-requirements into the overall ISMS model. These components are referred to as 'layers' – the represent the layering within the model, rather than imply any hierarchical relationship which might imply greater importance. Compliance with a piece of legislation may be the most important thing to an organization, but in this model, if the organization is trying to show its compliance through the implementation of an ISMS then comparison with the ISMS requirements is the point of reference when performing the mapping.

By mapping their conformity-requirements into the overall ISMS model the owner organization can build into their ISMS the specific controls and review processes necessary to achieve and to be able to demonstrate their required observance. The final specific controls would be expressed in the organization's **Statement of Applicability** which would refer to the controls set out in Annex A of ISO/IEC 27001and include such additional controls as necessary to provide a holistic ISMS.

The four layers are defined thus:

Layer 1: ISO/IEC 27001, normative ISMS requirements (ISMS-L1):

Formal requirements for the implementation, operation and management of the ISMS, including the risk management process and the provision of a **Statement of Applicability** which relates to the **RCL**.

Layer 2: ISO/IEC 27002, informative ISMS code of practice (ISMS-L2):

Generic (business, technical, functional) controls with implementation guidance, having a one-one relationship with the **RCL**.

Layer 3: Reference documents to which conformity is required (ISMS-L3):

Existing policies, legislation, regulation, contracts, international agreements, management and technical standards, &c. to which compliance/conformity is required, either by direct imposition (e.g. as laws, corporate policies) or through agreement (e.g. contract, choice of

[7] Such 'standards and specific legislation and regulation' are hereafter referred-to collectively as 'reference sources', a term intended also to cover any other specified requirements which a business aims to include within the scope of its ISMS as a definition of how some process is performed, defined, etc. This may extend to include other guidelines, although demonstration of conformity to them may prove difficult because of their informative nature.

standards). Privacy and Corporate Governance laws, ISO/IEC 18028-2, Basel II and PCI Data Security Standard are examples of reference sources which would fit into this component of the model.

Layer 4: baseline operational security controls (ISMS-L4):

Controls which are either implemented in order to conform to a standard requiring them or are determined to be required through the organization's own risk analysis or requirements. Baseline controls may also be those directly required by a specific standard. An example would be implementing some specific technical controls to meet the needs specific reference sources, such as ISO/IEC 18028-2 and the PCI DSS.

The focus of this process is therefore on the relationship between the implied controls determined by the conformity requirements of the reference sources which populate the ISMS-L3, and the specific controls implemented in ISMS-L4 and their relationship to the **RCL** of ISMS-L1 (i.e. to the **SoA** required by ISO/IEC 27001).

Mapping approach

Based upon ISO/IEC 27001, an organization implementing an ISMS must prepare a **Statement of Applicability** (**SoA** – ref. ISO/IEC 27001 §4.2.1.j), §4.3.1.i)). The **SoA** must, as a minimum, show how all of the controls listed in the **RCL** have either been implemented or justifiably excluded from implementation, based upon the scoping of the ISMS and the outcome of the risk analysis performed in conformity to ISO/IEC 27001.

It is therefore appropriate that the controls identified in and/or required by other policies, legislation, regulation and other standards etc. should be identified for completeness and sufficiency (where the implementer has any discretion in their application) before the risk analysis draws from them to establish the required **SoA**. This process involves collating controls from all applicable sources into an interim list which is known as the **Extended Control List (ECL)**. This serves two purposes: firstly, to provide the basis of a conformity mapping which can be used to demonstrate conformity against these other references and secondly, to provide a check that the ISMS controls identified through following ISO/IEC 27001 and defined in ISO/IEC 27002 (the latter providing interpretive guidance on their intended scope) are indeed sufficient in their defined scope or whether additional controls need to be stated and/or if additional implementation guidance need be given.

The approach to generating the **ECL** performs an analysis through a number of stages.

The first step in this process is to identify the reference sources which forms the basis for the **ECL**. These references should be those against which the organization wishes to be able to show conformity through their ISMS. However, it may be that in practice certain references are simply taken at face value and associated controls are identified as appropriate for inclusion within the ISMS, such as may be the case with adherence to an overall corporate policy or to a standard that mandates certain controls.

The control objectives and controls derived from those references should be used to extend the **RCL**, thus creating the initial **ECL**. This should include all controls, including those required to meet the industry and regulatory reference sources. Figure 1 illustrates how, based on the core ISMS standards, the initial Extended Control List can be created

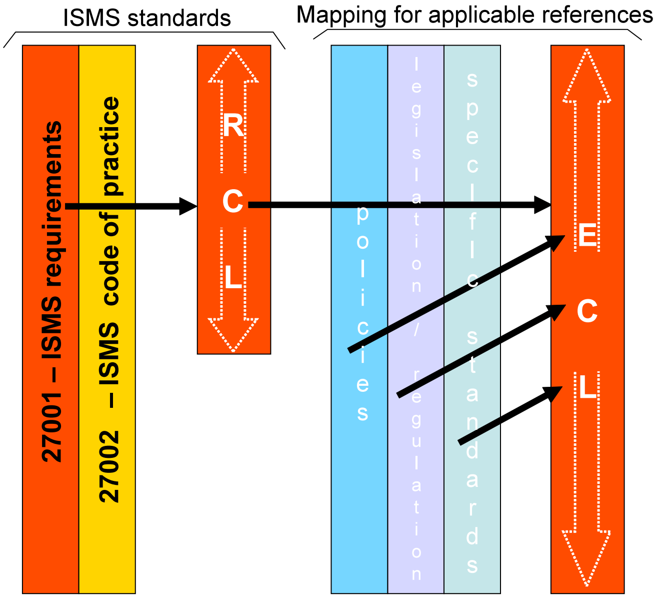

ISMS standards
Mapping for applicable references
27001 – ISMS requirements
27002 – ISMS code of practice
RCL
policies
legislation / regulation
specific standards
ECL

Figure 1. Creating the initial Extended Control List

In order to eliminate unwarranted duplication it is then necessary to assess each of the requirements, for each identified reference, against each of the ISMS controls defined in ISMS-1.

In preparing such a mapping, the analysis should give consideration to the extent to which a particular control from the **RCL** satisfies the requirements of the referenced source. In doing this, interpretive guidance from ISMS-L2 should be taken into account, as should be any guidance provided in the reference source.

If in the conduct of the analysis there are instances where the defined ISO/IEC 27002 implementation guidance does not adequately provide for the specific requirements of the referenced documents it is necessary to define a specific control for the express purposes of being able to show clearly conformity to the requirements of that referenced source.

At the end of this process the **ECL** contains a full set of optimized controls which, according to their origins and how the contents have been collated, could possess varying degrees of duplicated control objectives and controls. Figure 2 illustrates how the Extended Control List is created.

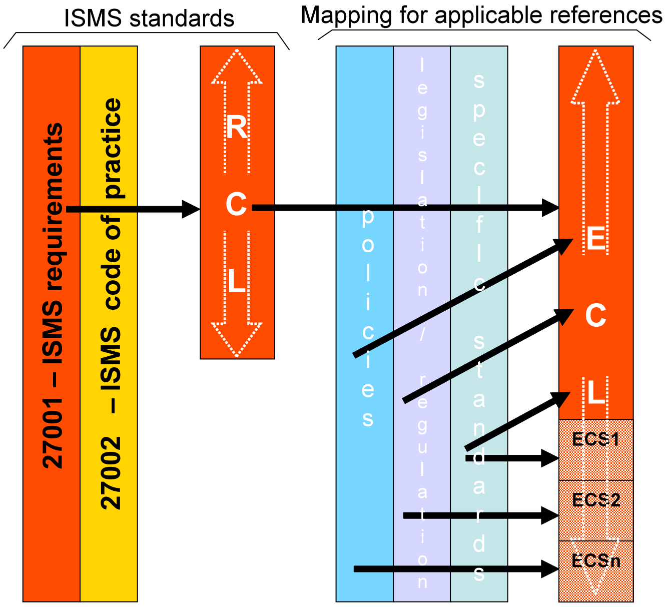

ISMS standards
Mapping for applicable references
27001 – ISMS requirements
27002 – ISMS code of practice
RCL
policies
legislation / regulation
specific standards
ECL
ECS1
ECS2
ECSn

Figure 2: Incorporating Extended Control Sets into the ECL

Note that it is not the intention to propose that a formalized process be necessarily undertaken in each case; rather that, where an organization needs to explicitly demonstrate its conformity to any specific reference, there be suitable analysis undertaken to identify the applicable controls and thus provide the needed traceability.

It is unlikely that the analysis of each reference source reveals a neat one-one mapping, for a variety of reasons. The preparation of this analysis requires thought and consideration. For example, comparing a piece of legislation and its associated regulations with a standard: the analysis must recognize that the documents are written for different purposes and from different viewpoints. Thus, the level of focus may vary, and the legislative text may not be provided with any guidance as to its implementation. It is also quite likely that an ISMS control may be an effective measure for more than one requirement within a reference source and, conversely, that a reference requirement may find more than one ISMS control which can fulfill it. In practice a single implemented instance of a control may satisfy more than one need for both the reference and the ISMS standards. Practitioners should not, therefore, be disappointed to find that a simple one-to-one mapping cannot be achieved. As a consequence of this implementers may develop an **Extended Control Set (ECS)** which relates explicitly to a specific reference source and has the potential for re-use, or may use an **ECS** from other sources. Each **ECS** should be used to supplement their **ECL**. In practice, the requirements of the implementing organization may also require extended controls to be defined.

As a final step in this analytic process, the specific controls implemented by the ISMS-owning organization require selection according to a risk analysis which takes into account the needs of the referenced sources and of course of the organization within the scope). These controls can then be mapped to the referenced sources and the final **SoA** identified (now considered also to include the **ECS**).

At this stage justification needs to be made if controls from the **ECL** are to be included within the ISMS or not, or if only one control is selected from a set of similar controls.

It should be kept in mind that this process is focusing on how to use an ISMS to support an organization in fulfilling its required conformity goals. It does not try to resolve how the organization performs its risk assessment and develops risk treatment plans which implement specific measures to fulfill the needs of ISO/IEC 27001 Annex A. The final ISMS needs to relate, through its **SoA**, how the organization's specific measures do indeed fulfill the requirements of both ISO/IEC 27001 and other target references as see Figure 3.

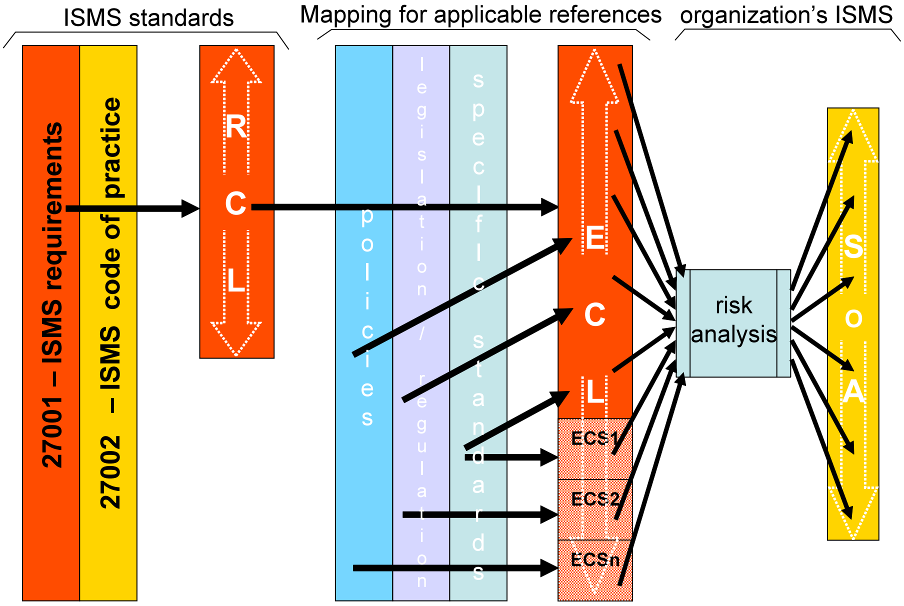


Figure 3. Deriving the organization's SoA

The above method explains at a high level an approach to generating the SoA for an ISMS being used to support conformity to other reference sources. The following part of this section now deals with the steps in that process.

Mapping process

The mapping process is described as number of discrete steps. Implementers should adopt them to their own circumstances in terms of the level of rigour and complexity demanded by their situation.

Mapping goals

The goals of the mapping are to:

i) establish the relationship between the two ISMS standards and the reference source;

ii) determine the extent to which the ISMS processes and controls are able to satisfy the requirements of the referenced source, and;

iii) Determine where additional controls are required to compensate for a lack of a suitable ISMS control or to strengthen existing ISMS controls.

The process to achieve fulfillment of these goals is now described.

Types of documents

In performing a comparative mapping between a specific reference source and the ISMS controls it is important to recognize that the mapping may not be between two documents of a common type, i.e. between documents having the same scope and intent in their usage. For example, the selected reference may be a national regulatory statement as to what organizations in a specific market sector must do in order to remain compliant with those sector-specific regulations; ISO/IEC 27001 is an international standard with required management **processes** supported by a code of practice (ISO/IEC 27002), related to a set of **controls** which have generic application, that application depending upon the scoping and requirements of an over-riding policy and business goals.

Thus, at a simplistic level, the comparison would be between a specific and a generic document; between a regulation (compliance with which is probably a legal obligation if operating in the sector which the legislation covers) and a standard (compliance with which is the exercise of choice). An inspection of the legislative impositions and the RCL shows that the former has a set of clauses which state how that document is to be interpreted, which entities are subject to it and what the subject entities are required to do.

Sometimes actions required for the demonstration of conformity may be given. Frequently they are not –legislation often sets the rules and those subject to it have to work out what they must do to achieve compliance, and possibly to justify their decisions at a later date. Other standards may be more like the ISMS standards, having normative and informative parts and using similar language, yet may still not have a defined process for demonstrating conformity. Other documents include sector specific standards and guidelines.

Thus, the implementer needs to be aware of the possible different purposes and structures of the reference sources being mapped and to keep that in mind when interpreting the respective documents during the mapping.

A consequence of this is that the mapping may need to be done between the reference source and both or either of ISO/IEC 27001 and ISO/IEC 27002, depending on the nature of its requirements and the extent to which they may focus on process (ISO/IEC 27001) and/or specific controls (ISO/IEC 27001 Annex A / 27002).

Mapping the relationships

It is valuable to arrive at the conclusion of the mapping with a bi-directional correspondence between the RCL and the reference source, i.e. for each control/requirement in the reference source, list all of the ISMS controls which relate to it and for each ISMS control list each of the reference source controls/requirements to which it contributes. This bi-directional mapping is valuable whenever a control or the control requirement changes and the corresponding controls need assessment to ensure that the conformity is maintained. The mapping supports management review, internal audit and the production of evidence of effective management control and regulatory compliance when the ISMS is subjected to external assessment or review.

Which of these two mappings is chosen to be the driver for the mapping process does not really matter, technically. However, since the ISMS controls can be the common element when more than one other reference source is mapped, and furthermore the information security management system can be the basis for embracing the other reference source(s), it is strongly recommended that the ISMS controls are taken as the fixed basis for the mapping, i.e. the reference source is mapped *into* the ISMS.

Below are headings related to two tables which may be used as the basis for recording the results of the mapping. In them «RefSrc» refers to the chosen reference source which is being mapped into the ISMS standard(s). These tables provide the basis of a simple cross-mapping: for the sake of these examples mapping against only 27002 is assumed.

Table 1A - headings for mapping against ISMS controls:

ISO/IEC 27002:2005 control	Matching «RefSrc» clause/section	Comparative coverage: 27002 cf. «RefSrc»	Commentary / Observations

Table 2A - headings for mapping against «RefSrc» controls:

«RefSrc» requirement	Matching ISO/IEC 27002:2005 implementation guidance	Commentary / Observations

How the mapping process should proceed is now explained by using an example. Each clause or discrete requirement / criterion in «RefSrc» is compared against the ISMS controls. With 133 controls against which to compare, comprehensive knowledge of the ISMS controls helps focus, often to within a single group of controls. Note that it is usual to find a one-to-many mapping between clauses, so a number of ISMS controls may be relevant.

As an example, the ISMS control (A)14.1.2 "Business continuity and risk assessment" could relate to, e.g., three separate controls in «RefSrc» which relate to having a data back-up plan, having a disaster recovery plan and performing a criticality analysis of applications and data.

Each time that a control mapping is found the «RefSrc» clause identity should be entered into Table 1A against the ISMS control, and similarly in Table 2A the ISMS control identity should be recorded against the «RefSrc» clause. Ideally, these should be hyper-linked to make easier the processes of cross-checking, implementation and audit/assessment.

Following from the example above, as the mapping progresses, the «RefSrc» requirement for having a disaster recovery plan may map into ISMS controls 14.1.1 to 14.1.5 inclusive.

Thus, the tables outlined above might develop the content like that shown below.

In the following Table 1B example, the text in the 'commentary/observations' column is exemplar, indicating the kinds of analysis that might be derived.

Table 1B - content after mapping against ISMS controls:

ISO/IEC 27002:2005 control	Matching «RefSrc» clause/section	Comparative coverage: 27002 cf. «RefSrc»	Commentary / Observations
14 BUSINESS CONTINUITY MANAGEMENT	§ 101(a) *Contingency plan*		27002 devotes a whole section to this subject and provides detailed controls and guidance whereas the «RefSrcs»'s requirements are stated in a series of brief paragraphs. «RefSrcs» also only refers to incidents which 'damage systems', rather than considering the loss of information *per se*.
14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT			See subordinate 27002 clauses.

ISO/IEC 27002:2005 control	Matching «RefSrc» clause/section	Comparative coverage: 27002 cf. «RefSrc»	Commentary / Observations
14.1.1 Including information security in the business continuity management process	§ 101(a)(ii) *Disaster recovery plan*		
	§ 101(a)(iv) *Applications and data criticality analysis*		
14.1.2 Business continuity and risk assessment	§ 101(a)(i) *Data backup plan*		
	§ 101(a)(ii) *Disaster recovery plan*		
	§ 101(a)(iv) *Applications and data criticality analysis*		
Etc.			
14.1.5 Testing, maintaining and re-assessing business continuity	§ 101(a)(i) *Data backup plan*		
	§ 101(a)(ii) *Disaster recovery plan*		

ISO/IEC 27002:2005 control	Matching «RefSrc» clause/section	Comparative coverage: 27002 cf. «RefSrc»	Commentary / Observations
plans	[§ 101(a)(iii)](#) *Emergency mode operation plan*		27002 has no explicit reference to an ‘emergency mode’, although it would be included within the general scope of item (c)(iii). Alternative wording for «RefSrc» recommended to be used in the ‘SoA’: “(iii) fallback procedures which describe the actions to be taken to: move essential business activities or support!services**, and required off-site back-ups,** to alternative temporary locations **from where emergency mode operations can be run, and;** bring business processes back into operation within the required timescales.” (bold indicates new text beyond that presently in 27002).
	[§ 101(a)(iii)](#) *Testing and revision procedures*		
	[§ 101(a)(iii)](#) *Contingency operations*		

In the following Table 2B example, the entries complement those in Table 1A (immediately above). Note that against the second «RefSrc» clause there is an ISMS control outside of the §14 group which has been mapped. Implementers should be aware that it might not be uncommon to find that a clause in the reference source has a relationship across a number of ISMS control groups, simply because of the structure of requirements within the reference source.

Table 2B - content after mapping against «RefSrc» controls:

«RefSrc» requirement	Matching ISO/IEC 27002:2005 implementation guidance	Commentary / Observations
§ 101(a) *Contingency Plan*	[14](#)**BUSINESS CONTINUITY MANAGEMENT**	
§ 101(a)(i) *Data*	*[10.5.1](#) Informatio*	

«RefSrc» requirement	Matching ISO/IEC 27002:2005 implementation guidance	Commentary / Observations
backup plan	*n Back-up* 14.1.2 *Business continuity and risk assessment* 14.1.3 *Developing and implementing continuity plans including information security* 14.1.4 *Business continuity planning framework* 14.1.5 *Testing, maintaining and re-assessing business continuity plans*	
§ 101(a)(iii) *Emergency mode operation plan*	14.1.3 *Developing and implementing continuity plans including information security* 14.1.4 *Business continuity planning framework* 14.1.5 *Testing, maintaining and re-assessing*	

«RefSrc» requirement	Matching ISO/IEC 27002:2005 implementation guidance	Commentary / Observations
	business continuity plans	

Determining ISMS control adequacy

Table 1A includes a column titled “Comparative coverage: 27002 cf. «RefSrc»”. This column should be used to indicate the extent to which the ISMS control can adequately fulfill the requirements of each discrete reference source clause or criterion.

OK	the ISMS control is **sufficient** to address the reference source requirement;
Partial	the ISMS control **does not fully** address the reference source requirement;
No	the ISMS control **does not** address the reference source requirement although headings / titling / etc. used in the respective documents suggest that they are addressing a similar issue;
N/A	the ISMS control covers an area not required by the reference source.

The benefit of this approach is that it is more immediately obvious where additional controls need to be defined.

It should be understood that the mapping has to be conducted with a ‘comparative’ judgment as to how the implementation of an ISMS based upon the control definitions and implementation guidance in 27002, having regard to the language and description of those controls, would enable the implementer to demonstrate that its conformity against the reference source was being adequately accomplished.

The mapping process defined above has so far identified an initial mapping. At the conclusion of this first parse of the reference source there are some requirements of the document which have not been addressed at all (by an ISMS control).

It would be prudent to crosscheck the mapping, and more specifically to verify whether any un-mapped controls (in either document) may in fact be mappable. Using additional resources to do this, which have not been involved in the first parse mapping, is usually beneficial.

In many cases the lack of a mapping against an ISMS control can be justified on the basis of ‘no direct relationship’ (to the reference source’s requirements) and can be marked as ‘not applicable’. This mapping attribute needs to be explicitly stated, so as not to lead to a later uncertainty as to whether the control was checked during the mapping.

‘***n/a***’ should therefore be added to both the above-defined suggestions for recording the comparative mapping results.

Three important points should be made. Firstly, it is unlikely that, and it should not be the goal that, each control within the ISMS is mapped to at least one of the reference source’s requirements and vice-versa. The broad applicability intended for ISO/IEC 27001 and the more likely narrower focus of the reference source (and why not more narrow, otherwise isn’t it just another ISMS under another name?) intuitively suggest that a complete mapping is unlikely to exist. Therefore, un-mapped ISMS controls should be anticipated.

Secondly, the fact that there is no mapping to an ISMS control is not a suggestion that that control would have no place in the overall ISMS being implemented – only that it would have an indirect relationship to the specific reference source clauses.

Lastly, the failure to find an ISMS control which satisfies one or more of the reference source’s requirements (i.e. where the adequacy mapping is determined to be ‘***Partial***’ or ‘***No***’) should not be seen as a weakness in the ISMS model – it actually points to where an obscurely-stated strength of the ISMS model should now be turned to the advantage of the implementer: define additional controls as required and include them within the overall framework of their ISMS

Extended Control Sets

ISO/IEC 27001 §4.2.1 (g) states: “*The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.*” Where the reference source’s requirements have not been satisfied in whole or part it is now appropriate to define additional objectives and controls, which can be placed into an Extended Control Set (ECS). This ensures that the controls implemented within the final ISMS allow the demonstration of full conformity with the reference source's requirements.

The ECS can be constructed in a number of ways –simply built into the operational procedures and processes, listed in a tabular form to record collectively the additional controls or constructed as a more formalized set of control objectives and controls with implementation guidance in a form which mimics that used in ISO/IEC 27001 Annex A. The following table provides a specimen ECS in this format. Note that the individual controls are given discrete clause references so that they may be addressed within the ISMS in the same way that the SoA would address the ISMS RCL.

Table 3A - Specimen Extended Control Set

«RefSrc» clause/ section	Control objective	Control	Implementation guidance	Related «RefSrc»& ISO/IEC 27002:2005 clause(s)
«RefSrc».101 Administrative safeguards				
«RefSrc». 101.1	Emergency mode continuity planning	Within the single framework of business continuity plans there shall be described, with appropriate priority, procedures to ensure protection of electronic personal identifiable information while operating in emergency mode.	Business continuity plans should (ref. 27002 §14) should describe the approach to provide fallback procedures which enable an emergency mode continuity plan to be put into effect, which takes into account the following actions: a) move critical business processes, and required off-site back-ups, to alternative temporary locations from where emergency mode operations can be run, and; b) bring business processes back into operation within the required timescales. Other information These controls should be integrated with the overall access control used by the organization, as covered by 27001 A.14, in particular A.14.1.4.	§ 101(a)(iii) *Emergency mode operation plan* 14.1.4*Business continuity planning framework*
«RefSrc». 101.2	Testing, maintaining and re-assessing emergency	Business continuity plans for operating the business in emergency mode should be tested and updated regularly	Business continuity plan tests should ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for	§ 101(a)(iii) *Emergency mode operation plan* 14.1.5*business continuity plans*

«RefSrc» clause/ section	Control objective	Control	Implementation guidance	Related «RefSrc»& ISO/IEC 27002:2005 clause(s)
	mode plans	to ensure that they are up to date and effective.	business continuity and information security, including transfer to emergency mode, and know their role when a plan is invoked. The test schedule for business continuity plan(s) should indicate how and when each element of the emergency mode plan should be tested. Each element of the plan(s) should be tested frequently. Other information Techniques used in order to provide assurance that the plan(s) for switching to emergency mode will operate in real life should follow, and be integrated with, those described in 27001 A.14.1.5.	

To complete the mapping, the new controls should be mapped into the table based upon the reference source requirements, which is now record both the matching ISMS controls and the specific ECS controls. Within the context of the ISMS-owner's system, there can be a complete mapping for the reference source.

Table 3B - content after creating the ECS:

«RefSrc» requirement	Matching ISO/IEC 27002:2005 implementation guidance	Commentary / Observations
§ 101(a)(iii) *Emergency mode operation plan*	*14.1.3 Developing and implementing continuity plans including information security* *14.1.4 Business continuity planning framework* *14.1.5 Testing, maintaining and re-assessing business continuity plans*	«RefSrc».101.1 «RefSrc».101.2

A potential difficulty which may encountered during the mapping process could be the introduction of control requirements from sources which may have no accommodation for one another, leading to conflict between their respective requirements. This is essentially a matter which must be resolved during the risk analysis process. Some basic observations can be made. Firstly, if it is possible to accommodate both requirements by partitioning them through the introduction of additional controls then those controls should, if not already within the scope of the **ECL**, be added, eventually to become a fixture within the **SoA**. Alternatively, one control could be downgraded to limit the degree of conflict, or might be eliminated altogether. In making such a decision any vulnerability created (including a potential non-conformity against the reference source) should be carefully assessed and management must accept and defend the consequences. It also may be practical to obtain a waiver from any contracting party or authority imposing the requirement, following a reasoned argument as to the nature of the conflict and the consequences of reduction or elimination of the control.

Whatever the outcome in such a situation, the risk analysis and the **SoA** must record the decision and its effect upon policy and the implementation of controls.

Managing the Extended Control List and Extended Control Sets
How extended controls are managed within the context of a specific ISMS and in a wider context depends on a number of issues which may include the following:

Is this a one-off requirement? If so then recording the ECS locally may be sufficient. If not, what might be the other uses of it? The ECS could be 'packaged' and made available to other parties within the same organization, or within the sector or some other community of interest. There is the potential for, e.g., a library of full 'other reference' to ISMS mappings to be established as a kind of library, including the ECS. Issues of commercial confidentiality may come into play, which are not addressed here.

Is the mapping done purely for internal reasons? If so, the ECS could be simply appended to the SoA derived from the RCL, or even integrated within it where the RCL control groups cover the general area of the extended control.

Is there a need to show conformity to an external (or possible a specific internal) party? If so, a separate SoA might be constructed which contains all, and only, the controls required to show that conformity. The complete ISMS may therefore have two (or more if desired) SoAs allowing different specific conformities to be demonstrated. Between multiple SoAs there is most likely be a high degree of commonality: The ISMS must address all controls within its scope; each reference source-specific SoA has its own (sub-) scope. Essentially, this can be accomplished by having a matrix which lists the full set of controls in one axis and the specific reference sources' use of controls in the other (the full ISMS can be excluded from the matrix since it ***is*** the full set).

Where there is a community of interest in having a particular reference source included within the scope of an ISMS, as a basis for mutual assurance between the participants in that community, a commonly-recognized ECS enables greater consistency and rigour in the application of controls which address the requirements of the specific reference source.

<u>ISMS scoping and operation</u>
The ISMS certification process is most directly concerned with determining the conformity of the management system to the normative requirements of ISO/IEC 27001. However, where an organization wishes to use its ISMS to indicate its conformity to other key references it would be wise to include such a claim within the scoping of its ISMS, thus requiring that the assessor looks explicitly for the evidence of that conformity within the ISMS.

Within the PDCA framework of the ISMS each of these ECS would be treated uniformly and consistently in terms of management, review, improvement etc. This provides both informal and formal forms of evidence of best endeavours to attain conformity and support traceability for ongoing maintenance.

Inclusion of evidence of conformity in this manner may eliminate the need for a separate conformity assessment, and in any event make more efficient the provision of evidence and the ongoing conformity oversight (through inclusion within the broader PDCA Phase of the ISMS).

Apart from controls, some frameworks provide certain process requirements. It may be necessary to have an additional document showing how additional management processes or procedures supplement the ISO/IEC 27001 requirements.