INTERNATIONAL STANDARD

ISO/IEC 27003

First edition
2010-02-01

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

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information

Reference number
ISO/IEC 27003:2010(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27003 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

The purpose of this International Standard is to provide practical guidance in developing the implementation plan for an Information Security Management System (ISMS) within an organization in accordance with ISO/IEC 27001:2005. The actual implementation of an ISMS is generally executed as a project.

The process described within this International Standard has been designed to provide support of the implementation of ISO/IEC 27001:2005; (relevant parts from Clauses 4, 5, and 7 inclusive) and document:

a) the preparation of beginning an ISMS implementation plan in an organization, defining the organizational structure for the project, and gaining management approval,

b) the critical activities for the ISMS project and,

c) examples to achieve the requirements in ISO/IEC 27001:2005.

By using this International Standard the organization will be able to develop a process for information security management, giving stakeholders the assurance that risks to information assets are continuously maintained within acceptable information security bounds as defined by the organization.

This International Standard does not cover the operational activities and other ISMS activities, but covers the concepts on how to design the activities which will result after the ISMS operations begin. The concept results in the final ISMS project implementation plan. The actual execution of the organizational specific part of an ISMS project is outside the scope of this International Standard.

The implementation of the ISMS project should be carried out using standard project management methodologies (for more information please see ISO and ISO/IEC Standards addressing project management).

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

1 Scope

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

This International Standard is intended to be used by organizations implementing an ISMS. It is applicable to all types of organization (e.g. commercial enterprises, government agencies, non-profit organizations) of all sizes. Each organization's complexity and risks are unique, and its specific requirements will drive the ISMS implementation. Smaller organizations will find that the activities noted in this International Standard are applicable to them and can be simplified. Large-scale or complex organizations might find that a layered organization or management system is needed to manage the activities in this International Standard effectively. However, in both cases, the relevant activities can be planned by applying this International Standard.

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2009, ISO/IEC 27001:2005 and the following apply.

3.1
ISMS project
structured activities undertaken by an organization to implement an ISMS

4 Structure of this International Standard

4.1 General structure of clauses

The implementation of an ISMS is an important activity and is generally executed as a project in an organization. This document explains the ISMS implementation by focusing on the initiation, planning, and definition of the project. The process of planning the ISMS final implementation contains five phases and each phase is represented by a separate clause. All clauses have a similar structure, as described below. The five phases are:

a) Obtaining management approval for initiating an ISMS project (Clause 5)

b) Defining ISMS Scope and ISMS Policy (Clause 6)

c) Conducting Organization Analysis (Clause 7)

d) Conducting Risk Assessment and Risk Treatment planning (Clause 8)

e) Designing the ISMS (Clause 9)

Figure 1 illustrates the five phases of the planning of the ISMS project referring to ISO/IEC standards and main output documents.

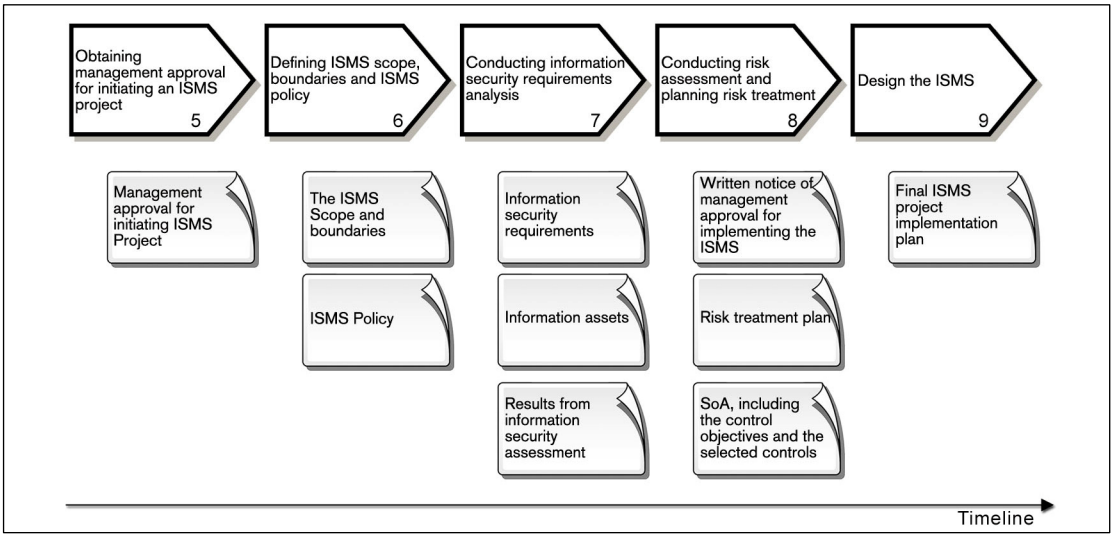


Figure 1 — ISMS project phases

Further information is noted in the annexes. These annexes are:

Annex A. Summary of activities with references according to ISO/IEC 27001:2005

Annex B. Information security roles and responsibilities

Annex C. Information on planning of internal audits

Annex D. Structure of policies

Annex E. Information on planning of monitoring and measuring

4.2 General structure of a clause

Each clause contains:

a) one or more objectives stating what is to be achieved noted in the beginning of each clause in a text box;

and

b) one or more activities necessary to achieve the phase objective or objectives.

Each activity is described in a subclause.

Activity descriptions in each subclause are structured as follows:

Activity

The activity defines what is necessary to satisfy this activity which achieves all or part of the phase objectives.

Input

The input describes the starting point, such as the existence of documented decisions or outputs from other activities described in this International Standard. Inputs could either be referred to as the complete output from an activity just stating the relevant clause or specific information from an activity may be added after the clause reference.

Guidance

The guidance provides detailed information to enable performing this activity. Some of the guidance may not be suitable in all cases and other ways of achieving the results may be more appropriate.

Output

The output describes the result(s) or deliverable(s), upon completion of the activity; e.g. a document. The outputs are the same, independent of the size of the organization or the ISMS scope.

Other information

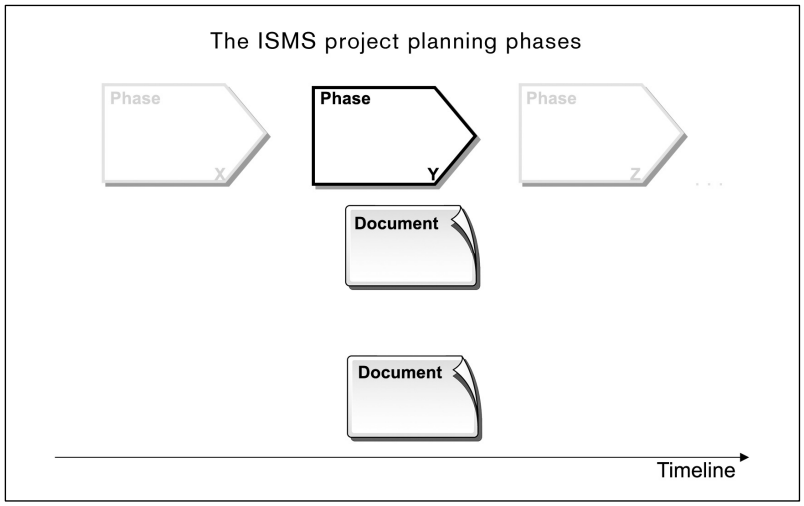
The other information provides any additional information that may assist in performing the activity, for example references to other standards.

NOTE The phases and activities described in this document include a suggested sequence of performing activities based on the dependencies identified through each of the activities' "Input" and "Output" descriptions. However, depending on many different factors (e.g., effectiveness of management system currently in place, understanding with regard to the importance of information security, reasons for implementing an ISMS), an organization may select any activity in any order as necessary to prepare for the establishment and implementation of the ISMS.

4.3 Diagrams

A project is often illustrated in graphical or diagram form showing an overview of activities and outputs.

Figure 2 illustrates the legend of diagrams which are illustrated in an overview subclause of each phase. The diagrams provide a high level overview of the activities included in each phase.



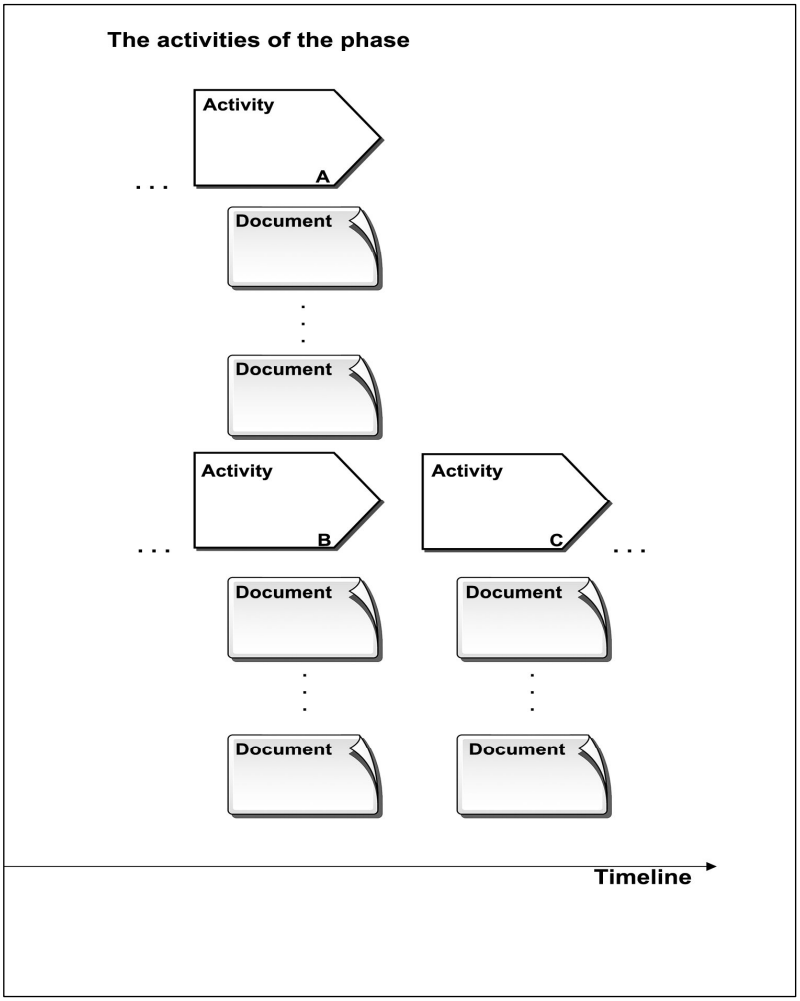


Figure 2 — Flow diagram legend

The upper square illustrates the planning phases of an ISMS project. The phase explained in the specific clause is then emphasized with its key output documents.

The lower diagram (activities of the phase) includes the key activities which are included in the emphasized phase of the upper square, and main output documents of each activity.

The timeline in the lower square is based on the timeline in the upper square.

Activity A and Activity B can be executed at the same time. Activity C should be started after Activity A and B is finished.

5 Obtaining management approval for initiating an ISMS project

5.1 Overview of obtaining management approval for initiating an ISMS project

There are several factors that should be taken into consideration when deciding to implement an ISMS. In order to address these factors, management should understand the business case of an ISMS implementation project and approve it. Therefore the objective of this phase is:

Objective:
To obtain management approval to start the ISMS project by defining a business case and the project plan.

In order to acquire management approval, an organization should create a business case which includes the priorities and objectives to implement an ISMS in addition to the structure of the organization for the ISMS. The initial ISMS project plan should also be created.

The work performed in this phase will enable the organization to understand the relevance of an ISMS, and clarify the information security roles and responsibilities within the organization needed for an ISMS project.

The expected output of this phase will be the preliminary management approval of, and commitment to implement, an ISMS and performing the activities described in this International Standard. The deliverables from this clause include a business case and a draft ISMS project plan with key milestones.

Figure 3 illustrates the process to obtain management approval to initiate the ISMS project.

NOTE The output from Clause 5 (Documented management commitment to plan and implement an ISMS) and one of the outputs of Clause 7 (Document summarization of the information security status) are not requirements of ISO/IEC 27001:2005. However, the outputs from these activities are recommended input to other activities described in this document.

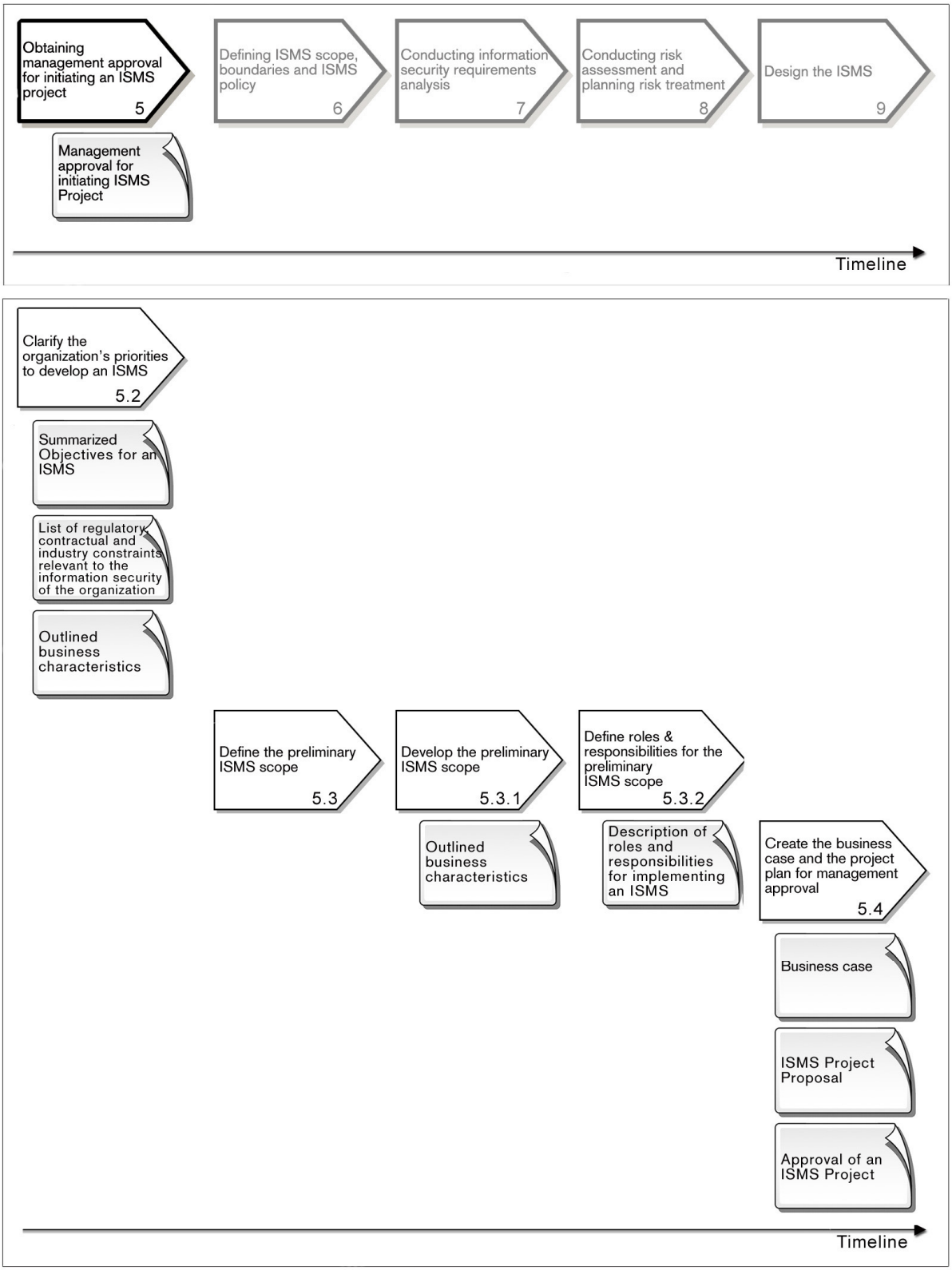


Figure 3 — Overview of obtaining management approval for initiating an ISMS project

5.2 Clarify the organization's priorities to develop an ISMS

Activity

The objectives to implement an ISMS should be included by considering the organization's information security priorities and requirements.

Input

a) the organization's strategic objectives

b) overview of the existing management systems

c) a list of legal, regulatory, and contractual information security requirements applicable to the organization

Guidance

In order to start the ISMS project, management approval is generally needed. Therefore, the first activity that should be performed is to collect the relevant information illustrating the value of an ISMS to the organization. The organization should clarify why an ISMS is needed and decide the objectives of the ISMS implementation and initiate the ISMS Project.

The objectives for implementing an ISMS can be determined by answering the following questions:

a) risk management – How will an ISMS generate better management of information security risks?

b) efficiency – How can an ISMS improve the management of information security?

c) business advantage – How can an ISMS create competitive advantage for the organization?

In order to answer the questions above, the organization's security priorities and requirements are addressed by the following possible factors:

a) critical businesses and organization areas:

   1. What are the critical businesses and organizational areas?
   2. Which organizational areas provide the business and with what focus?
   3. What third party relationships and agreements exist?
   4. Are there any services that have been outsourced?

b) sensitive or valuable information:

   1. What information is critical to the organization?
   2. What would be the likely consequences if certain information were to be disclosed to unauthorized parties (e.g., loss of competitive advantage, damage to brand or reputation, legal action, etc.)?

c) laws which mandate information security measures:

   1. What laws relating to risk treatment or information security apply to the organization?
   2. Is the organization part of a public global organization that is required to have external financial reporting?

d) contractual or organizational agreements relating to information security:

   1. What are the storage requirements (including the retention periods) for data storage?
   2. Are there any contractual requirements relating to privacy or quality (e.g. service level agreement-SLA)?

e) industry requirements which specify particular information security controls or measures:

   1. What sector-specific requirements apply to the organization?

f) The threat environment:

   1. What kind of protection is needed, and against what threats?
   2. What are the distinct categories of information that require protection?
   3. What are the distinct types of information activities that need to be protected?

g) Competitive Drivers:

   1. What are the minimum market requirements for information security?
   2. What additional information security controls should provide a competitive advantage for the organization?

h) Business continuity requirements

   1. What are the critical business processes?
   2. How long can the organization tolerate interruptions to each critical business process?

The preliminary ISMS scope can be determined by responding to the information above. This is also needed in order to create a business case and overall ISMS project plan for management approval. The detailed ISMS scope will be defined during the ISMS project.

The requirements noted in ISO/IEC 27001:2005 reference 4.2.1 a) outline the scope in terms of the characteristics of the business, the organization, its location, assets and technology. The resulting information from the above supports this determination.

Some topics which should be considered when making the initial decisions regarding scope include:

a) What are the mandates for information security management established by organizational management and the obligations imposed externally on the organization?

b) Is the responsibility for the proposed in-scope systems held by more than one management team (e.g. people in different subsidiaries or different departments)?

c) How will the ISMS-related documents be communicated throughout the organization (e.g. on paper or through the corporate intranet)?

d) Can the current management systems support the organization’s needs? Is it fully operational, well maintained, and functioning as intended?

Examples of management objectives that may be used as input to define the preliminary ISMS scope include:

a) facilitating business continuity and disaster recovery

b) improving resilience to incidents

c) addressing legal/contractual compliance/liabilities

d) enabling certification against other ISO/IEC standards

e) enabling organizational evolution and position

f) reducing costs of security controls

g) protecting assets of strategic value

h) establishing a healthy and effective internal control environment

i) providing assurance to stakeholders that information assets are properly protected

Output

The deliverables of this activity are:

a) a document summarizing the objectives, information security priorities, and organizational requirements for an ISMS.

b) a list of regulatory, contractual, and industry requirements related to the information security of the organization.

c) Outlined characteristics of the business, the organization, its location, assets, and technology.

Other information

ISO/IEC 9001:2008, ISO/IEC 14001:2004, ISO/IEC 20000-1:2005.

5.3 Define the preliminary ISMS scope

5.3.1 Develop the preliminary ISMS scope

Activity

The objectives to implement ISMS should include the preliminary ISMS scope definition, which is necessary for the ISMS project.

Input

Output from Activity 5.2 Clarify the organization's priorities to develop an ISMS.

Guidance

In order to execute the ISMS implementation project, the structure of an organization for the ISMS should be defined. The preliminary scope of the ISMS should now be defined to provide management with guidance for implementation decisions, and to support further activities.

The preliminary ISMS scope is needed in order to create the business case and the proposed project plan for management approval.

The output from this stage will be a document defining the preliminary scope of the ISMS, which includes:

a) a summary of the mandates for information security management established by organizational management, and the obligations imposed externally on the organization;

b) a description of how the area(s) in scope interact with other management systems;

c) a list of the business objectives of information security management (as derived in clause 5.2);

d) a list of critical business processes, systems, information assets, organizational structures and geographic locations to which the ISMS will be applied.

e) the relationship of existing management systems, regulatory, compliance, and organization objectives;

f) the characteristics of the business, the organization, its location, assets and technology.

The common elements and the operational differences between the processes of any existing management system(s) and the proposed ISMS should be identified.

Output

The deliverable is a document which describes the preliminary scope of the ISMS.

Other information

No other specific information.

NOTE Special attention should be drawn that in case of certification specific documentation requirements of ISO/IEC 27001:2005 as for the ISMS scope are to be fulfilled regardless of the management systems in place within the organization.

5.3.2 Define roles & responsibilities for the preliminary ISMS scope

Activity

The overall roles and responsibilities for the preliminary ISMS scope should be defined.

Input

a) output from Activity 5.3.1 Develop the preliminary ISMS scope

b) list of stakeholders who will benefit from results of the ISMS project.

Guidance

In order to execute the ISMS project, the role of an organization for the project should be determined. The role generally is different at each organization, because of the number of people dealing with information security. The organizational structure and resources for information security vary with the size, type and structure of the organization. For example, in a smaller organization, several roles may be carried out by the same person. However, management should explicitly identify the role (typically Chief Information Security Officer, Information Security Manager or similar) with overall responsibility for managing information security, and the staff should be assigned roles and responsibilities based on the skill required to perform the job. This is critical to ensure that the tasks are carried out efficiently and effectively.

The most important considerations in the definition of roles in information security management are:

a) overall responsibility for the tasks remains at the management level,

b) one person (usually the Chief Information Security Officer) is appointed to promote and co-ordinate the information security process,

c) each employee is equally responsible for his or her original task and for maintaining information security in the workplace and in the organization.

The roles for managing information security should work together; this may be facilitated by an Information Security Forum, or similar body.

Collaboration with appropriate business specialists should be undertaken (and documented) at all stages of the development, implementation, operation and maintenance of the ISMS.

Representatives from departments within the identified scope (such as risk management) are potential ISMS implementation team members. This team should be maintained at the smallest practical size for speed and effective use of resources. Such areas are not only those directly included in the ISMS scope, but also the indirect divisions, such as legal, risk management and administrative departments.

Output

The deliverable is a document or table describing the roles and responsibilities with the names and organization needed to successfully implement an ISMS.

Other Information

Annex B provides details of roles and responsibilities needed in an organization to successfully implement an ISMS.

5.4 Create the business case and the project plan for management approval

Activity

The management approval and commitment of resources for the ISMS implementation project should be obtained by creating the business case and the ISMS project proposal.

Input

a) output from Activity 5.2 Clarify the organization's priorities to develop an ISMS

b) output from Activity 5.3 Define the preliminary ISMS scope – The documented: preliminary

   1. ISMS scope and

   2. associated roles and responsibilities.

Guidance

The information for the business case and initial ISMS project plan should include estimated timeline, resources, and milestones needed for the main activities noted in Clauses 6 to 9 of this International Standard.

The business case and initial ISMS project plan serve as the base of the project, but also ensures management commitment and approval of resources needed for the ISMS implementation. The manner in which the implemented ISMS will support the business objectives contributes to the effectiveness of the organizational processes and increases the efficiency of the business.

The business case for implementing an ISMS should include short statements linked to the organization's objectives and cover the following subjects:

a) goals and specific objectives

b) benefit to the organization

c) preliminary scope of ISMS including business processes affected

d) critical processes & factors for reaching the ISMS objectives

e) high-level project overview

f) initial implementation plan

g) defined roles and responsibilities

h) required resources (both technology and people)

i) implementation considerations including existing information security

j) timeline with key milestones

k) expected costs

l) critical success factors

m) quantify the benefits to the organization

The project plan should include relevant activities of phases in Clause 6-9 set forth in this International Standard.

Individuals that effect, or are affected by, the ISMS should be identified and allowed adequate time to review and comment on the ISMS business case and ISMS project proposal. The business case and ISMS project proposal should be updated as necessary as input is provided. Once sufficient support is gained, the business case and the ISMS project proposal should be presented to management for approval.

Management should approve the business case and initial project plan in order to achieve full organization commitment and begin execution of the ISMS project.

The expected benefits from management commitment for implementing an ISMS are:

a) knowledge and implementation of relevant laws, regulations, contractual obligations and standards relating to information security, resulting in avoidance of liabilities and penalties of non-compliance,

b) efficient use of multiple processes for information security,

c) stability and increased confidence to grow through better management of information security risks,

d) identification and protection of business-critical information.

Output

The deliverables of this activity are:

a) a documented approval by management to execute the ISMS project with the allocated resources

b) a documented business case

c) an initial ISMS Project Proposal, with milestones, such as performing risk assessment, implementation, internal audits, and management review)

Other Information

ISO/IEC 27000:2009 for examples of critical success factors to support the ISMS business case.

6 Defining ISMS scope, boundaries and ISMS policy

6.1 Overview of defining ISMS scope, boundaries and ISMS policy

Management approval for the implementation of an ISMS is based on the preliminary ISMS scope, ISMS business case and initial project plan. The detailed definition of the scope and boundaries of the ISMS, the definition of the ISMS policy and acceptance and support by management are the key primary factors for successful implementation of the ISMS.

Therefore, the objectives of this phase are:

Objectives:

To define the detailed scope and boundaries of the ISMS and develop the ISMS policy, and obtain endorsement from management

ISO/IEC 27001:2005 reference: 4.2.1 a) and 4.2.1 b)

In order to achieve "Define the detailed scope and boundaries for the ISMS" objective, the following activities are necessary:

a) define the organizational scope and boundaries,

b) Information Communication Technology (ICT) scope and boundaries and

c) physical scope and boundaries.

d) specified characteristics in ISO/IEC 27001:2005 reference 4.2.1 a) and b), i.e. business, organization, location, assets and technology aspects of the scope and boundaries, and policy are determined in the process of defining these scope and boundaries

e) integrate elementary scope and boundaries to obtain the ISMS scope and boundaries

To achieve the definition of the ISMS policy and obtain acceptance from the management, a single activity is necessary.

To build an effective management system for the organization, the detailed scope of the ISMS should be determined by considering critical information assets of the organization. It is important to have a common terminology and systematic approach for identifying information assets and assessing viable security mechanisms. This enables ease of communication and fosters consistent understanding through all phases of the implementation. It is also important to ensure that critical organization areas are included in the scope.

It is possible to define the scope of an ISMS to encompass the entire organization, or a part thereof, such as a division or clearly bounded subsidiary element. For example, in the case of "services" provided to customers, the scope of the ISMS can be a service, or a cross-functional management system (an entire division or part of a division). The requirements of ISO/IEC 27001:2005 shall be fulfilled for certification regardless of the existing management systems in place within the organization.

Organizational scope and boundaries, ICT scope and boundaries (6.3) and physical scope and boundaries (6.4) are not always to be carried out sequentially. However it is useful to reference already obtained scope and boundaries when defining other scope and boundaries.

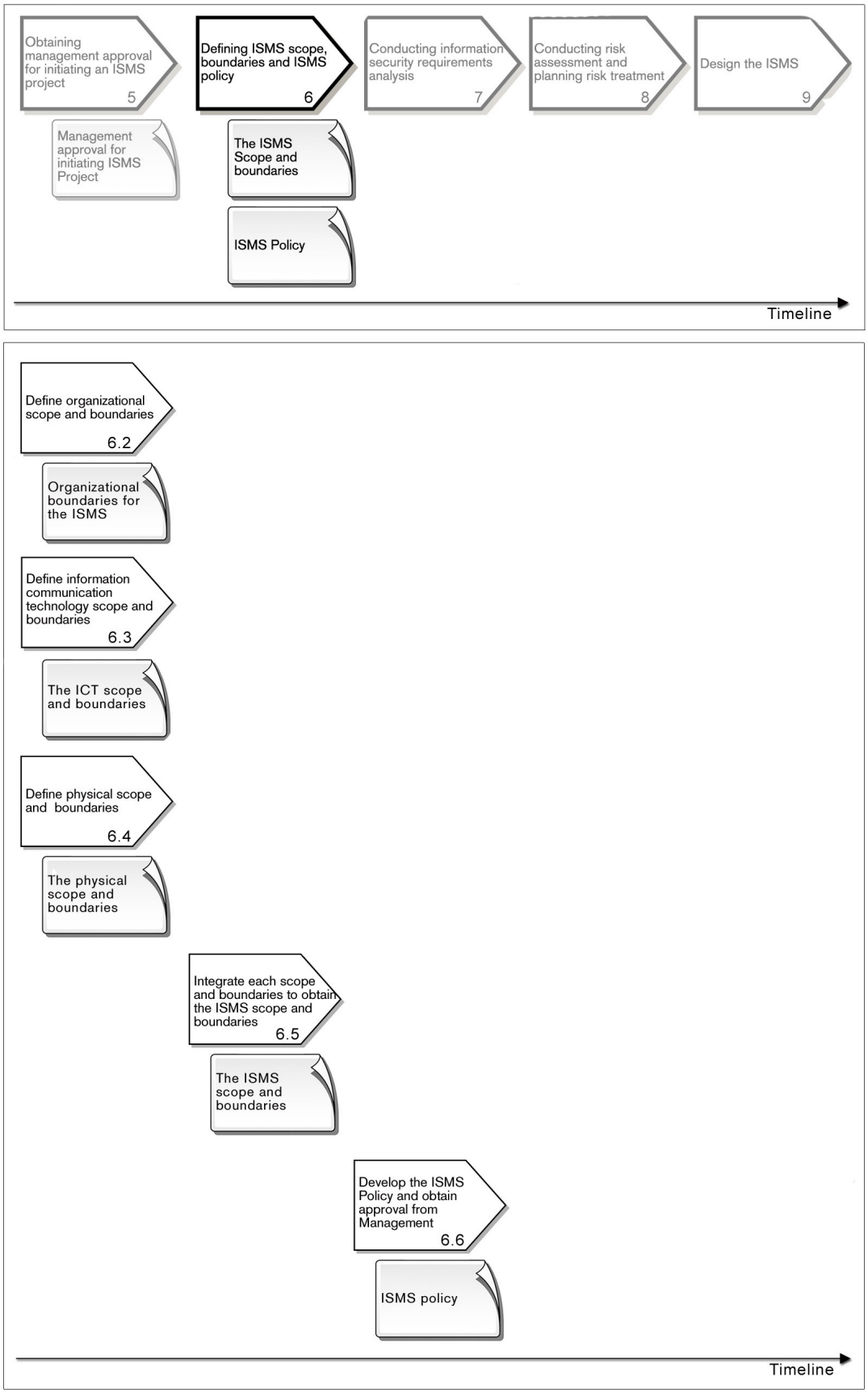


Figure 4 — Overview of defining ISMS scope, boundaries and ISMS policy

6.2 Define organizational scope and boundaries

Activity

The organizational scope and boundaries should be defined.

Input

a) output from Activity 5.3 Define the preliminary ISMS scope - The documented preliminary scope of the ISMS which addresses:

   1. relationship of existing management systems, regulatory, compliance, and organization objectives;

   2. characteristics of the business, the organization, its location, assets and technology.

b) output from Activity 5.2 Clarify the organization's priorities to develop an ISMS - The documented approval by management to implement an ISMS and start the project with necessary resources allocated.

Guidance

The amount of effort required to implement an ISMS is dependent on the magnitude of the scope to which it is to be applied. This can also impact all activities relating to maintenance of information security of in-scope items (such as process, physical locations, IT systems and people), including implementing and maintaining controls,managing operations, and carrying out tasks such as identifying information assets and assessing risk. If management decides to exclude certain parts of the organization from the scope of the ISMS, their reasons for doing so should be documented.

When the scope of the ISMS is defined, it is important that its boundaries are clear enough to be explained to those who were not involved in its definition.

Some controls relating to information security may already be in existence as a result of the deployment of other management systems. These should be taken into account when planning the ISMS, but will not necessarily indicate the boundaries of the scope for the current ISMS.

One method of defining organizational boundaries is to identify those areas of responsibility which are non-overlapping to ease assignment of accountability within an organization.

Responsibilities directly related to information assets or business processes included in the ISMS scope should be selected as a part of organization which is under control of the ISMS. While defining organizational boundaries the following factors should be considered:

a) ISMS management forum should consist of managers directly involved in the scope of the ISMS.

b) the member of management responsible for the ISMS should be the one who is ultimately responsible for all the areas of responsibility affected (i.e. their role will usually be dictated by their span of control and responsibility within an organization).

c) In the case where the role responsible for managing the ISMS is not a member of senior management, a top management sponsor is essential to represent the interests of information security and act as the advocate for the ISMS at the highest levels of the organization.

d) Scope and boundaries need to be defined to ensure that all relevant assets are taken into account in the risk assessment, and to address the risks that might arise through these boundaries.

Based on the approach, the organizational boundaries analyzed should identify all personnel affected by the ISMS, and this should be included in the scope. The identification of personnel may be linked to processes and/or functions depending on the selected approach. If some processes within the scope are outsourced to the third parties those dependencies should be clearly documented. Such dependencies will be subjected to further analysis in the ISMS implementation project.

Output

The deliverables of this activity are:

a) description of organizational boundaries for the ISMS, including any justifications for portions of the organization that have been excluded from the ISMS scope,

b) functions and structure of those parts of the organization within the scope of the ISMS,

c) identification of information exchanged within the scope and information exchanged through boundaries

d) organization processes and the responsibilities for the information assets of the scope and outside scope,

e) process for the hierarchy of decision making as well as structure within the ISMS.

Other information

No other specific information.

6.3 Define information communication technology (ICT) scope and boundaries

Activity

The scope and boundaries of the elements of information communication technology (ICT) and other technology items covered by the ISMS should be defined.

Input

a) output from Activity 5.3 Define the preliminary ISMS scope - The document for the preliminary scope of the ISMS

b) output from Activity 6.2 Define organizational scope and boundaries

Guidance

The definition of the ICT scope and boundaries can be obtained through an information system (rather than IT-based) approach. Once there is a management decision to include the information system business processes into the ISMS scope, all related ICT elements should be considered as well. This includes all parts of the organization which store, process or transport critical information, assets, or which are critical to the parts of the organization in-scope. Information systems may span organizational or national borders. Should this be the case, the following should be considered:

a) socio-cultural environment

b) legal, regulatory and contractual requirements applicable to the organizations

c) accountability for key responsibilities

d) technical constraints (e.g. available bandwidth, availability of service, etc.)

Taking the above into consideration, ICT boundaries should include a description of the following when applicable

a) the communications infrastructure, where responsibility for managing it is held by the organization including various different technologies (e.g. wireless, wireline, or data/voice networks).

b) software within the organizational boundaries, that is used and controlled by the organization

c) ICT hardware required by the network or networks, applications or production systems

d) roles and responsibilities regarding ICT hardware, network and software

If any one or more of the above bullets is not controlled by the organization, third-party dependencies should be documented. See 6.2, Guidance.

Output

The deliverables of this activity are:

a) information exchanged within the scope and information exchanged through boundaries

b) ICT boundaries for the ISMS, including any justifications for the exclusion of ICT under the organization's management that have been excluded from the ISMS scope,

c) the information systems and telecommunication networks, describing what is in scope, along with roles and responsibilities for these systems. Out-of-scope systems should be briefly summarised

Other information

No other specific information

6.4 Define physical scope and boundaries

Activity

The physical scope and boundaries that should be covered by the ISMS should be defined.

Input

a) output from Activity 5.3 Define the preliminary ISMS scope - The document for the preliminary scope of the ISMS

b) output from Activity 6.2 Define organizational scope and boundaries .

c) output from Activity 6.3 Define information communication technology (ICT) scope and boundaries

Guidance

The definition of physical scope and 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:

a) remote facilities

b) interfaces to the customer's information systems and services provided by third party service

c) applicable proper interfaces and service levels.

Taking the above into consideration, physical boundaries should include a description of the following, when applicable:

a) functions or process description taking into account their physical location and extent the organization controls them

b) special facilities used for storing/containing ICT hardware or in-scope data (e.g. on back-up tapes) based upon the coverage of the ICT boundaries

If any one or more of the above bullets is not controlled by the organization, third-party dependencies should be documented. See 6.2, Guidance.

Output

The deliverables of this activity are:

a) description of physical boundaries for the ISMS, including any justifications for the exclusion of physical boundaries under the organization's management that have been excluded from the ISMS scope,

b) description of the organization and their geographical characteristics relevant to the scope.

Other information

No other specific information.

6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries

Activity

The ISMS scope and boundaries should be obtained by integrating each scope and boundaries.

Input

a) output from Activity 5.3 Define the preliminary ISMS scope - The document for the preliminary scope of the ISMS

b) output from Activity 6.2 Define organizational scope and boundaries

c) output from Activity 6.3 Define information communication technology (ICT) scope and boundaries

d) output from Activity 6.4 Define physical scope and boundaries

Guidance

The scope of an ISMS can be described and justified in many ways. For example, a physical location such as a datacenter or office may be selected, and critical processes listed; each of which involve areas outside that datacenter bringing those outside areas into scope. One such critical process could, for example, be mobile access to a central information system.

Output

The deliverable of this activity is a document describing the scope and boundaries of the ISMS, containing the following information:

a) the key characteristics of the organization (its function, structure, services, assets, and the scope and boundaries of the responsibility for each asset)

b) the in-scope organizational processes

c) the configuration of in-scope equipment and networks

d) a preliminary list of in-scope information assets

e) a list of in-scope ICT assets (e.g. servers)

f) maps of in-scope sites, indicating the physical boundaries of the ISMS.

g) roles and responsibilities descriptions within the ISMS and their relationships with the organizational structure

h) details of and justification for any exclusions from the ISMS scope

Other information

No other specific information.

6.6 Develop the ISMS policy and obtain approval from management

Activity

The ISMS policy should be developed and approval from the management should be obtained.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The documented ISMS Scope and Boundaries

b) output from Activity 5.2 Clarify the organization's priorities to develop an ISMS – The documented objectives for implementing the ISMS

c) output from Activity 5.4 Create the business case and the project plan for management approval - The documented:

   1. organization requirements and information security priorities,

   2. the initial project plan for the ISMS implementation, with milestones, such as performing risk assessment, implementation, internal audits, and management review)

Guidance

While defining the ISMS policy, the following aspects should be considered:

a) establish the ISMS objectives based on organizational requirements and information security priorities of the organization

b) establish the general focus and guide to action to achieve the ISMS objectives

c) consider the organization's requirements, legal or regulatory and contractual obligations related to information security

d) risk management context within the organization

e) establish the criteria for evaluating risks (see ISO/IEC 27005:2008) and defining a risk assessment structure

f) clarify high-level management responsibilities with regard to the ISMS

g) obtain management approval.

Output

The deliverable is a document which describes the documented management-approved ISMS policy. This document should be re-confirmed in a later phase of the project as it is dependent on the outcome of the risk assessment.

Other information

ISO/IEC 27005:2008 provides additional information on criteria for evaluating risks.

7 Conducting information security requirements analysis

7.1 Overview of conducting information security requirements analysis

The analysis of the current situation in the organization is important, as there are existing requirements and information assets that should be considered when implementing an ISMS. The activities described in this phase can be undertaken mainly in parallel with those described in Clause 6 for reasons of efficiency and practicality.

Objectives:

To define the relevant requirements to be supported by the ISMS, identify the information assets, and obtain the current information security status within scope

ISO/IEC 27001:2005 reference: 4.2.1.c)1) partially, 4.2.1. d), 4.2.1. e)

The information collected through the information security 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 the desired level of protection for the information

f) determine the compilation of information needed for all or part of an enterprise within the proposed scope of the implementation.

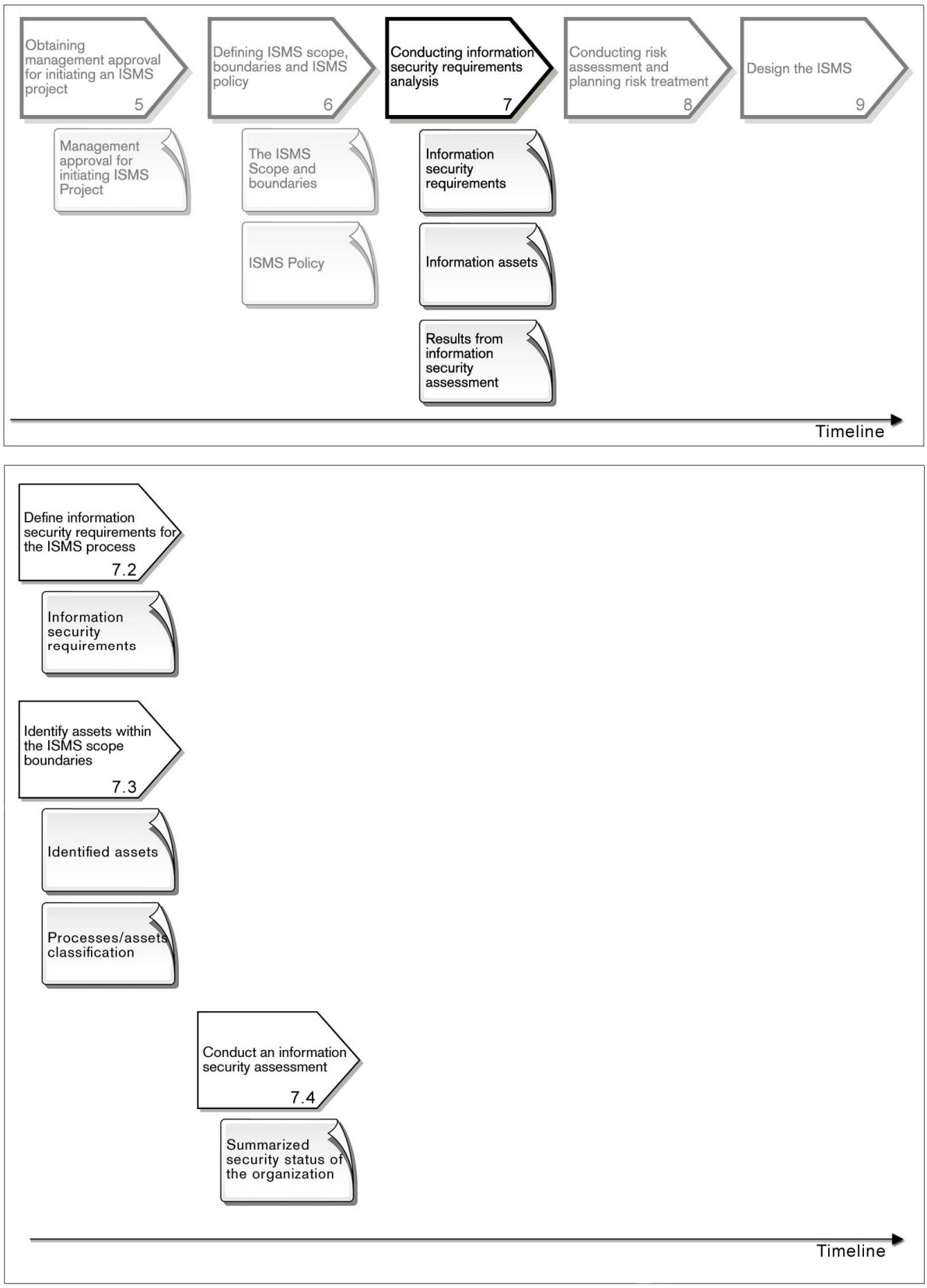


Figure 5 — Overview of conducting information security requirements phase

7.2 Define information security requirements for the ISMS process

Activity

The detailed information security requirements for the ISMS process should be analyzed and defined.

Input

a) output from Activity 5.2 Clarify the organization's priorities to develop an ISMS – The documents:

   1. summarizing the objectives, information security priorities, and organization requirements for ISMS

   2. list of regulatory, contractual, and industry constraints relevant to the information security of the organization

b) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

c) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

Guidance

The first step requires all supporting information for the ISMS to be collected. For each organizational 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 an organization process and the associated ICT applications and systems.

The analysis of the organization's processes provides statements about the effects of information security incidents on the organization's activity. In many cases it is adequate to work with a very basic description of the organization's processes. The processes, functions, locations, information systems and communications networks need to be identified and documented, if they have not already been included as part of the ISMS scope.

The following should be addressed to get the detailed information security requirements for the ISMS:

a) preliminary identification of important information assets and their current information security protection.

b) identify visions of the organization and determine the effect of identified visions on future information processing requirements.

c) analyze the current forms of information processing, system applications, communication networks, location of activities and IT resources, etc.

d) identify all essential requirements (e.g. legal and regulatory requirements, contractual obligations, organization requirements, industry standards, customer and supplier agreements, insurance conditions etc.).

e) identify the level of information security awareness and, from that, derive the training and education requirements, in terms of each operational and administrative unit.

Output

The deliverables of this activity are:

a) identification of the main processes, functions, locations, information systems and communication networks

b) information assets of the organization

c) critical processes/assets classification

d) information security requirements derived from the organization's legal, regulatory, and contractual requirements

e) list of publicly known vulnerabilities that will be addressed as a result of the security requirements

f) organization information security training and education requirements

Other information

No other specific information.

7.3 Identify assets within the ISMS scope

Activity

The assets to be supported by the ISMS should be identified.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

b) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

c) output from Activity 7.2 Define information security requirements for the ISMS process

Guidance

To identify the assets within the ISMS scope the following information should be identified and listed:

a) unique name of the process

b) process description and associated activities (created, stored, transmitted, deleted)

c) criticality of the process to the organization (critical, important, supporting)

d) process owner (organization unit)

e) processes providing input and outputs from this process

f) IT applications supporting the process

g) information classification (confidentiality, integrity, availability, access control, non-repudiation, and/or other important properties for organization, e.g., how long the information may be stored)

Output

The deliverables of this activity are:

a) identified information assets of the main processes of the organization within the ISMS scope

b) Information security classification of critical processes and information assets

Other information

No other specific information.

7.4 Conduct an information security assessment

Activity

The information security assessment should be performed by comparing the current status of information security of the organization compared to the desired organization objectives.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

b) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

c) output from Activity 7.2 Define information security requirements for the ISMS process

d) output from Activity 7.3 Identify assets within the ISMS scope

Guidance

Information security assessment is the activity for identifying the existing level of information security (i.e. the organization current procedures of handling protection of information). The fundamental purpose of the information security assessment 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 organization analysis, standards documents, and have access to suitable management personnel.

Information security assessments analyse current situation for the organization by using the following information and determine current status of information security and document vulnerabilities:

a) studying background facts based upon critical processes

b) information assets classification

c) organizational information security requirement.

The results of the information security assessment together with the objectives of the organization are often an important part of the incentive for future work on information security. The information security assessment should be performed by an internal or external resource with an independent status in relation to the organization.

Participation in the information security assessment should include individuals who possess a strong knowledge of 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. organization unit heads)

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

c) other individuals who possess strong knowledge of the current environment, conditions, and what is relevant in terms of information security. For example, business process users and operational, administrative functions and legal functions.

The following actions are important for successful information security assessment:

a) Identify and list the relevant standards of the organization (e.g. ISO/IEC 27002:2005).

b) identify known control requirements that arise from policies, legal and regulatory requirements, contractual obligations, findings from past audits, or findings from risk assessments done in the past.

c) use these as reference documents in order for a rough estimation to be made of the organization's current requirements concerning its level of information security.

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

The approach for conducting the information security assessment is as follows:

a) select the important organizational business processes and process steps concerning information security requirements,

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 organization analysis.

c) discuss with suitable key personnel and analyze the organization's current situation in relation to the information security requirements. For example which processes are critical, how well do they currently work? (The results are used later in the risk assessment.)

d) determine control deficiencies by comparing existing controls with previously identified control requirements.

e) complete and document the current status.

Output

The deliverable of this activity is:

a) a document summarizing the assessed security status of the organization, and evaluated vulnerabilities.

Other information

The information security assessment conducted at this stage will only deliver preliminary information about the organization's status of information security and vulnerabilities, because the full set of information security policies and standards is developed at a later stage (see Clause 9), and a risk assessment has not yet been conducted.

8 Conducting risk assessment and planning risk treatment

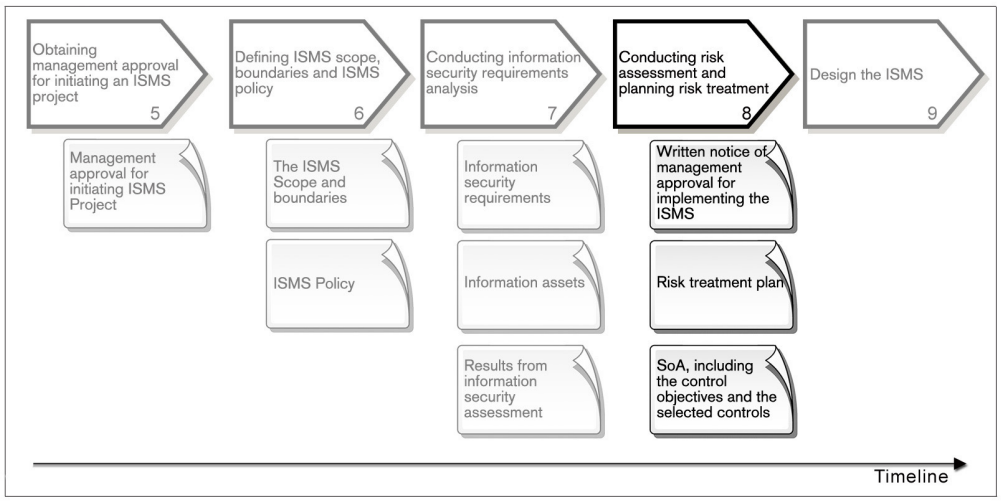
8.1 Overview of conducting risk assessment and planning risk treatment

The implementation of an ISMS should address relevant information security risks. The identification, evaluation and planned treatment of the risks and the selection of control objectives and controls are important steps for an ISMS implementation and should be handled in this phase.

ISO/IEC 27005:2008 provides specific guidelines for Information Security Risk Management and should be referred to throughout Clause 8.

It is assumed that management has committed to the implementation of the ISMS, and that the ISMS scope and ISMS policy have been defined, and that information assets are known as well as the information security assessment results.

Objective: To define the risk assessment methodology, identify, analyze and evaluate the information security risks for selecting risk treatment options and selecting control objectives and controls **ISO/IEC 27001 reference** 4.2.1 c) to 4.2.1 j)



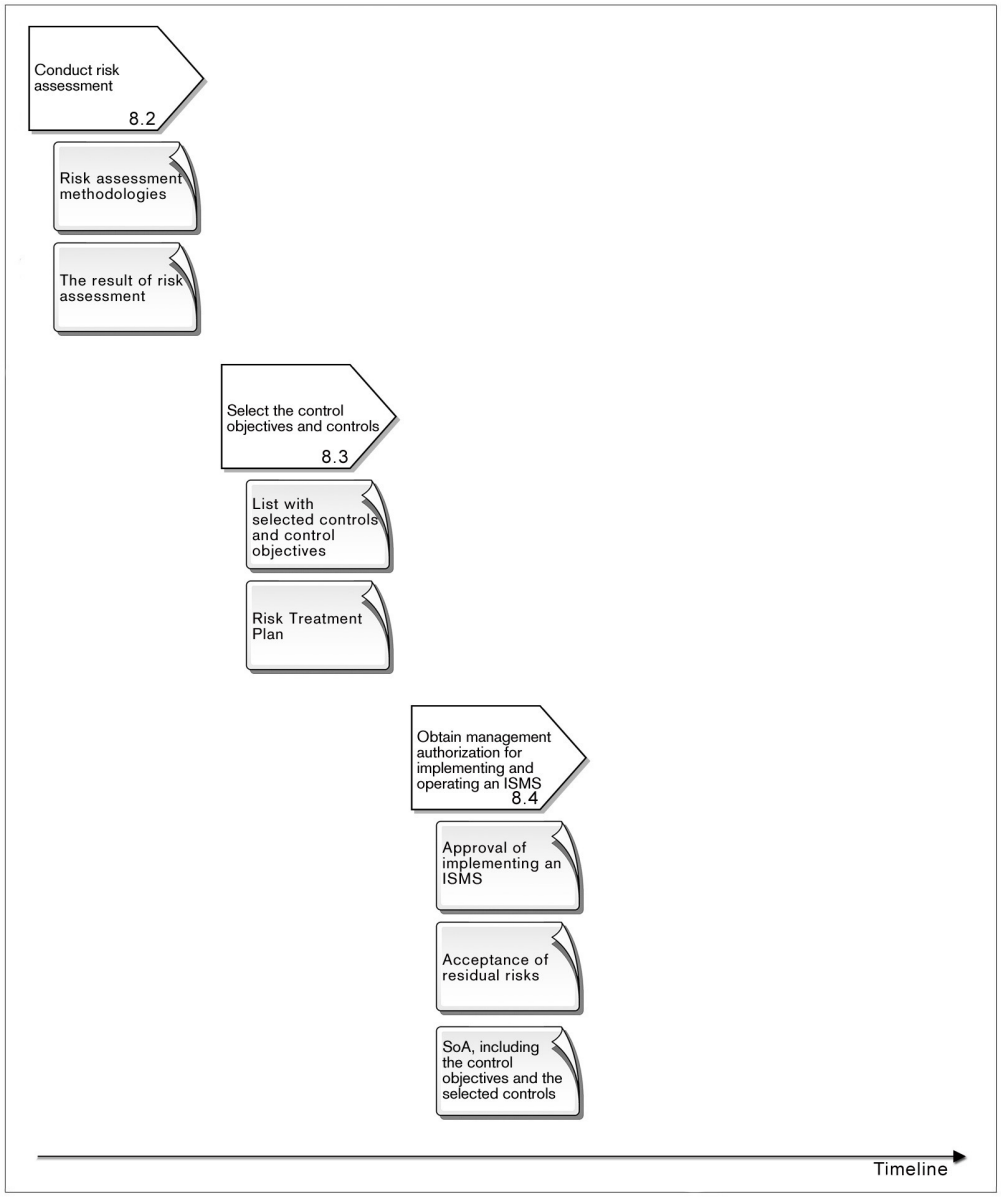


Figure 6 — Overview of the risk assessment phase

8.2 Conduct risk assessment

Activity

The risk assessment should be performed.

Input

a) outputs from Activity in clause 7 Conducting information security requirements analysis - The information concerning:

   1. summarized information security status

   2. identified information assets

b) output from activity in clause 6 Defining ISMS scope, boundaries and ISMS policy – The documented:

   1. ISMS scope

   2. ISMS policy

c) ISO/IEC 27005:2008

Guidance

The performance of a security risk assessment within the business context in support of the ISMS scope is essential for compliance and successful ISMS implementation according to ISO/IEC 27001:2005. The risk assessment should:

a) identify threats and their sources

b) identify existing and planned controls

c) identify vulnerabilities that can be exploited by threats, to cause harm to assets or to the organization

d) identify the consequences that losses of confidentiality, integrity, availability, non-repudiation, and other security requirements may have on the assets

e) assess the business impact that might result from anticipated or actual information security incidents

f) assess the likelihood of the incident scenarios

g) estimate the level of risk

h) compare levels of risk against risk evaluation criteria and risk acceptance criteria

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. For reference, see Annex B, 'Roles and Responsibilities'.

An organization may employ a risk assessment methodology that is project-specific, company-specific or a sector specific standard.

Output

The deliverables of this activity are:

a) the description of risk assessment methodologies

b) the results of the risk assessment

Other information

Annex B – information about Roles and Responsibilities.

NOTE An incident scenario is the description of a threat exploiting a certain vulnerability or set of vulnerabilities in an information security incident. ISO/IEC 27001 describes the occurrence of incident scenarios as “security failures". (see ISO/IEC 27005:2008)

8.3 Select the control objectives and controls

Activity

The options for the treatment of risks should be identified as well as the selection of the appropriate controls should be identified in accordance with the identified risk treatment options.

Input

a) output from Activity 8.2 Conduct risk assessment - The result of risk assessment

b) ISO/IEC 27005:2008

c) ISO/IEC 27002:2005

Guidance

It is important to specify the relation between the risks and the selected options for treating them (e.g. a risk treatment plan), as this will provide a summary of risk treatment. Possible options for the treatment of risks are enumerated in ISO/IEC 27001:2005 reference 4.2.1 f).

The ISO/IEC 27001:2005 Annex A (normative) “Control objectives and controls" is used to select control objectives and controls for risk treatment. If there are no appropriate control objectives or controls in Annex A, the additional control objectives and controls should be specified and used. It is important to demonstrate how the selected controls will mitigate risks as required by the risk treatment plan.

The data given in ISO/IEC 27001:2005 Annex A is not meant to be exhaustive. Sector-specific controls may be identified to support the specific needs of the business as well as the ISMS.

In the case of risk reduction, managing the relationship between each risk and selected control objectives and controls is beneficial to designing the ISMS implementation. It could be added to the list that describes the relationship between the risks and the selected options for risk treatment.

To facilitate audits, the organization should compile a list of controls which have been selected as relevant and applicable to the organization's ISMS. This has the added advantage of improving business relationships, such as electronic outsourcing, by providing a summary of controls in place.

It is important to be aware of that the summary of controls is very likely to contain sensitive information. Therefore, appropriate care should be taken when making the summary of controls available to both internal and external recipients. It may actually be appropriate to take the information generated as part of the creation of the ISMS into account during the definition of assets.

Output

The deliverables of this activity are:

a) a list with selected controls and control objectives

b) the Risk Treatment Plan, with:

   1. A description of the relation between risks and selected risk treatment option

   2. A description of the relation between risks and selected control objectives and controls (especially in the case of risk reduction)

Other information

ISO/IEC 27002:2005

8.4 Obtain management authorization for implementing and operating an ISMS

Activity

Management approval should be obtained to implement an ISMS as well document the acceptance of residual risks.

Input

a) Output from Activities in 5.4 Create the business case and the project plan for management approval - The initial management approval for the ISMS Project

b) outputs from Activities in Clause 6 Defining ISMS scope, boundaries and ISMS policy – The documented statements of:

   1. the ISMS policy and objectives

   2. the scope of the ISMS

c) output from Activity 8.2 Conduct risk assessment – The documented:

   1. description of risk assessment methodologies

   2. the result of risk assessment

d) output from Activity 8.3 Select the control objectives and controls - The Risk Treatment Plan

Guidance

To obtain management approval, the documents described as the input of this subclause should be prepared for management evaluation and decisions.

The preparations for the Statement of Applicability (SoA) should be included as a part of the information security management efforts. The level of details in which controls are specified should meet the requirements needed to support the organization's management approval for the ISMS.

Approval should be obtained from high-level management for the decision to accept residual risks, and authorisation obtained for the actual operation of the ISMS. These decisions should be based upon an assessment of the risks and opportunities likely to occur as a result of the implementation of the ISMS, as compared with those resulting from not implementing it.

Output

The deliverables of this activity are:

a) written notice of management approval for implementing the ISMS

b) management acceptance of residual risks.

c) statement of applicability, including the control objectives and the selected controls

Other information

No other specific information.

9 Designing the ISMS

9.1 Overview of designing the ISMS

A detailed design of the ISMS project, planned activities for its implementation should now be developed. The final ISMS project plan will be unique in its detail for the specific organization, depending on results from previous activities as well as the results of the specific activities in the design phase described in this clause.

The specific final ISMS project implementation plan is the output of this clause. Based upon this plan, the ISMS project can be launched in the organization as part of the very first “DO” phase of the PDCA cycle as described in ISO/IEC 27001:2005.

It is assumed that management has committed to the implementation of the ISMS which is defined in the ISMS scope and ISMS policy. The information assets as well as the results of the information security assessment are assumed to be available. In addition, the risk treatment plan describing the risks, risk treatment options, with the identified selected control objectives and controls should also be available.

The ISMS design described here focuses upon the internal structure and requirements of the ISMS. It should be noted that, in certain cases, the ISMS design may have a direct or indirect impact on the design of business processes. Likewise it should be noted that there is usually a need to integrate ISMS components with pre-existing management and infrastructure arrangements.

Objective:

To complete the final implementation plan for the ISMS by: designing organizational security based on the selected risk treatment options, as well as requirements regarding recording and documents , and designing the controls integrating security provisions for ICT, physical and organizational processes, and designing the ISMS-specific requirements

ISO/IEC 27001: 2005 reference: 4.2.2 a)-e), h)

In designing the ISMS, the following matters should be considered:

a) organizational security – covers the administrative aspects of information security including the responsibility of the organization's operation for risk treatment. 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 organization's needs and risks.

b) ICT security – covers aspects of information security specifically related to the responsibility of the ICT operations for risk reduction. This is to fulfil the requirements set by the organization and the technical implementation of controls to reduce risks.

c) physical security – covers aspects of information security specifically related to the responsibility of the handling of the physical environment, such as buildings and their infrastructure for risk reduction. This is to fulfil the requirements set by the organization and the technical implementation of controls to reduce risks.

d) ISMS specific – covers the aspects of the different specific requirements for an ISMS according to ISO/IEC 27001:2005, 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 an operational ISMS which are:

    1. monitoring
    2. measuring
    3. internal ISMS auditing
    4. training and awareness
    5. incident management
    6. management review
    7. ISMS improvement including corrective and preventive actions

The development of the ISMS Project and the design of its related planned implementation of controls should involve and make use of the skills and experience of staff from those parts of the organization that are either within the ISMS scope or have ISMS related management responsibilities. The ISMS specific aspects requires dialogue with management.

To design the selected controls for the risk treatment, it is crucial to design the ICT and physical security environment and the organizational security environment. ICT security deals not only with information systems and networks but also with operational requirements. Physical security deals with all aspects of access control, non-repudiation, physical protection of information assets and what is stored or kept in, as well as being itself a means of protection for security controls itself.

The controls selected in activities described in clause 8.3 should be implemented according to a specific structured and detailed implementation plan, as part of the ISMS project plan. This specific part of the ISMS project plan should address how to handle each risk in order to achieve the control objectives. This specific part of the ISMS project plan is essential if the selected controls are to be properly and effectively implemented. The information security management team is responsible for drawing up this specific part of the implementation plan, which then constitutes the final ISMS project plan.

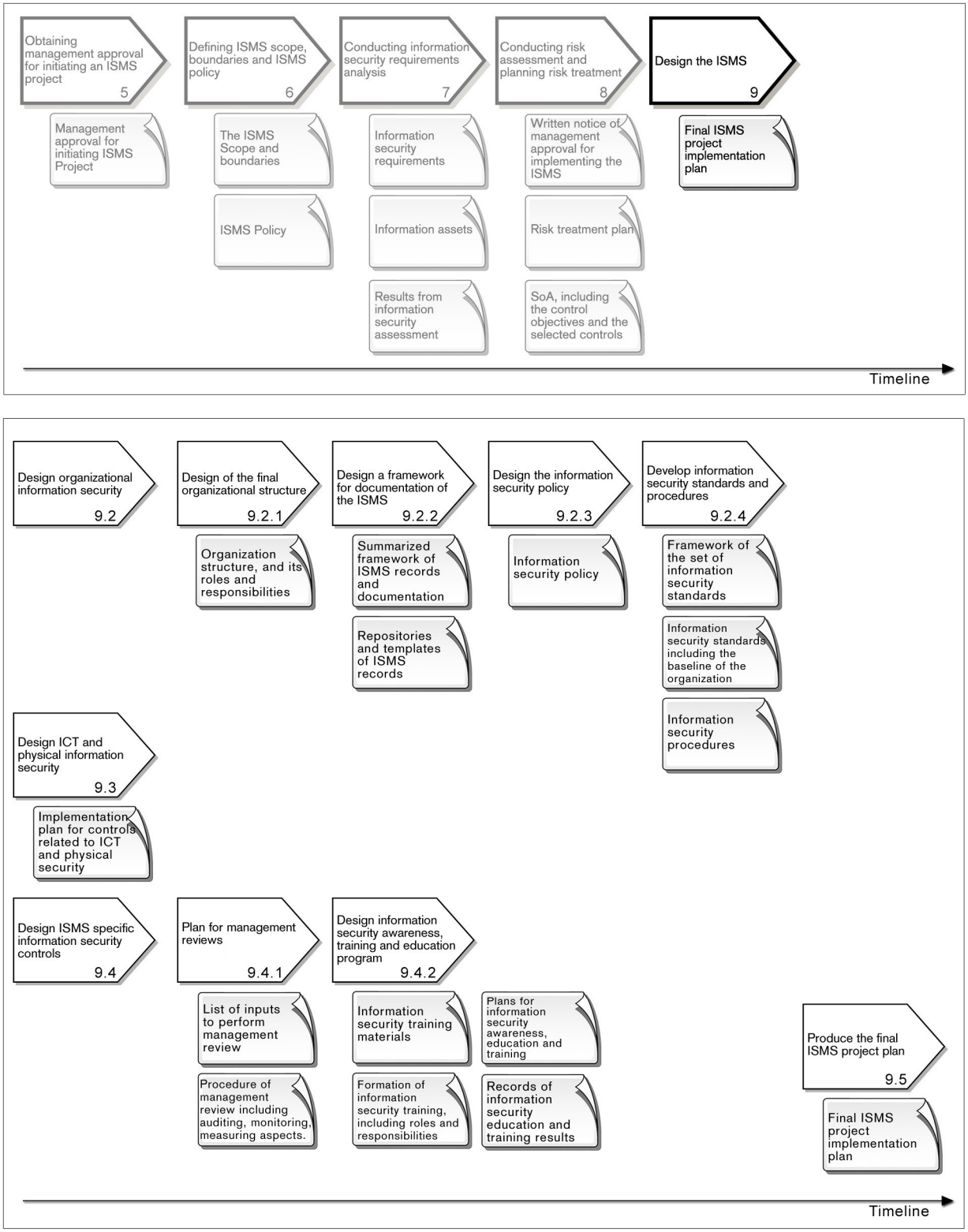


Figure 7 — Overview of designing the ISMS phase

9.2 Design organizational information security

9.2.1 Design of the final organizational structure for information security

Activity

The organizational functions, roles and responsibility for information security should be aligned with the risk treatment.

Input

a) output from Activity 5.3.2 Define roles & responsibilities for the preliminary ISMS scope - The table of roles and responsibilities

b) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

c) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

d) output from Activity 7.2 Define information security requirements for the ISMS process

e) output from Activity 7.3 Identify assets within the ISMS scope

f) output from Activity 7.4 Conduct an information security assessment

g) output from Activity 8.2 Conduct risk assessment – The results of risk assessment

h) output from Activity 8.3 Select the control objectives and controls

i) ISO/IEC 27002:2005

Guidance

The design of organizational structures and processes for internal ISMS operations should seek to build upon and integrate with pre-existing areas where appropriate. Likewise, the integration of the ISMS into broader pre-existing management structures (e.g. internal audit) should be taken into account in the ISMS design process.

The organizational structure designed for the ISMS should reflect activities for implementation and operation of ISMS as well, addressing, for example, the methods of monitoring and recording as a part of the ISMS operations.

Accordingly, the structure for ISMS operations should be designed based on the planned ISMS implementation by considering the following:

a) Is each role for ISMS implementation needed for ISMS operations?

b) Are the defined roles different from those for ISMS implementation?

c) What roles should be added for ISMS implementation?

For example, the following roles may be added for ISMS operations:

a) someone responsible for information security operations in each department

b) someone responsible for measuring the ISMS in each department

Consideration of the points outlined in Annex B “Roles and Responsibilities” may help to decide the structure and roles for ISMS operation by revising the structure and roles for ISMS implementation.

Output

The deliverable of this activity is a document summarizing:

a) organization structure, and its roles and responsibilities

Other information

Annex B - Information about roles and responsibilities

Annex C -Information about planning auditing

9.2.2 Design a framework for documentation of the ISMS

Activity

The records and documents in the ISMS should be controlled by identifying the requirements and the framework that enables fulfilling the requirements for ongoing control of records and documents in the ISMS.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

b) ISMS Scope and boundary definition

c) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

d) output from Activity 8.4 Obtain management authorization for implementing and operating an ISMS

e) output from Activity 9.2.1Design of the final organizational structure for information security

f) ISO/IEC 27002:2005

Guidance

Designing ISMS recording includes the following activities:

a) a framework describing principles for documentation of the ISMS, the structure of procedures for documenting the ISMS, roles involved, data formats, and reporting paths for the management

b) design the documentation requirements

c) design the recording requirements

The ISMS documentation should include records of management decisions; ensure that actions are traceable to management decisions and policies, and that the recorded results are reproducible.

ISMS documents should provide the evidence that controls are selected based on the results of risk assessment and risk treatment, and that such processes are implemented along with the ISMS policy and objectives.

Documentation is essential for the reproducibility of results and procedures. As for selected controls, the establishment and documentation of the procedures should have a reference to the person responsible for the actual piece of documentation.

The ISMS documentation should include the documentation as specified in ISO/IEC 27001:2005 reference: 4.3.1.

It is necessary for the ISMS documents to be managed and made available to personnel as required. This includes the following:

a) establish the administrative procedure of the ISMS document management

b) a formal approval of documents for adequacy prior to issue

c) ensuring that changes and the current revision status of documents are identified

d) protection and control the documents as an information asset of the organization

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 tracking to them if they are retained for any purpose.

Records should be created, maintained and controlled as evidence that the ISMS of the organization conforms to ISO/IEC 27001:2005, and to show the effectiveness of operations.

It is also required to keep records of implementation status for the entire PDCA phase, as well as records of information security incidents and events, 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) document the controls required to identify, store, protect, search, and discard data, and document its storage duration

b) define what should be recorded, and to what extent, in the operational management processes

c) when any period of retention is specified by relevant laws or legislation, the period of retention should be set pursuant to such legal requirement.

Output

The deliverables of this activity are:

a) a document summarizing the requirements for ISMS records and documentation control

b) repositories and templates for the required records of the ISMS

Other information

No other specific information

9.2.3 Design the information security policy

Activity

The management‘s and administration‘s strategic position of the information security objectives, with respect to the ISMS operation, should be documented.

Input

a) output from Activity 5.2 Clarify the organization's priorities to develop an ISMS –The summarized objectives and list of requirements

b) output from activity 5.4 Create the business case and the project plan for management approval – The initial management approval for the ISMS project

c) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMSI

d) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

e) output from Activity 7.2 Define information security requirements for the ISMS process

f) output from Activity 7.3 Identify assets within the ISMS scope

g) output from Activity 7.4 Conduct an information security assessment

h) output from Activity 8.2 Conduct risk assessment – The results of risk assessment output from Activity 8.3 Select the control objectives and controls

i) output from Activity 9.2.1 Design of the final organizational structure for information security

j) output from Activity 9.2.2 Design a framework for documentation of the ISMS

k) ISO/IEC 27002:2005 reference: 5.1.1

Guidance

The information security policy documents the organization's strategic position with respect to the information security objectives throughout the organization.

The policy is drawn up based on the information and knowledge. What has been identified by 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 of an information security policy 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, so that the staff is able to understand the intent of the policy. In addition, it should sufficiently distinguish what objectives are needed to address the set of regulations and organization objectives.

The size and structure of the information security policy should support the documents that are used in the next stage in the process for introducing an information security management system (see also appendix D - Information about policy structure).

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.

Guidance on the content of an information security policy document is provided in ISO/IEC 27002:2005 reference 5.1.1

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.

Output

The deliverable of this activity is a document of the information security policy.

Other information

Annex B – Information about roles and responsibilities

Annex D- Information about policy structure

9.2.4 Develop information security standards and procedures

Activity

The information security standards and procedures addressing either the entire organization or specific parts of it should be developed.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

b) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

c) output from Activity 8.2 Conduct risk assessment

d) output from Activity 8.3 Select the control objectives and controls

e) output from Activity 8.4 Obtain management authorization for implementing and operating an ISMS – The Statement of applicability, including the control objectives and the selected controls

f) output from Activity 9.2.1 Design of the final organizational structure for information security

g) output from Activity 9.2.2 Design a framework for documentation of the ISMS

h) output from Activity 9.2.3 Design the information security policy

i) ISO/IEC 27002:2005

Guidance

In order to provide a foundation for the information security work within the organization, information security standards as well as the set of applicable legal and regulatory requirements should be available to those who need to know.

Representatives of different parts of the organization covered by the scope of the ISMS should participate in the process of developing standards and procedures. Those participating should have authority and be representative of the organization. For example, the following roles may be included:

a) information security managers,

b) representatives for physical security,

c) information Systems owners, and

d) process owners of strategic and operational areas.

It is suggested to keep the editorial group as small as possible, with the option of appointing specialists to the team on a temporary basis as required. Each representative should liaise actively with their own area of the organization to provide seamless operational support. This then facilitates later refinement in the form of procedures and routines at the operational level.

Security standards and procedures should then be used as a basis for designing detailed technical or operational procedures.

A useful way to approach the development of information security standards and procedures is to consider each point of implementation guidance in ISO/IEC 27001:2005 and ISO/IEC 27002:2005 that is deemed applicable (based on the results of the risk assessment), and describe precisely how it should be applied.

An evaluation of any existing information security standards and procedures should be reviewed. For example, can they be refined and developed, or are do they need to be entirely replaced?

Relevant and up to date documentation should be provided to every member of staff in scope. The information security standards and procedures should apply to the entire organization or make it clear as to which roles, systems and areas are covered. A first version should be produced in a timely manner

The revision and review process should be defined at an early stage. A strategy should then be drawn up for how information on policy changes should be distributed.

Output

a) The deliverable of this activity is a structured and detailed implementation plan for controls relating to organizational security as part of the final ISMS project plan, to include a documented framework of the set of information security standards

b) information security standards including the baseline of the organization

c) information security procedures achieving the information security standards

Other Information

Annex D- Information about policy structure

9.3 Design ICT and physical information security

Activity

The controls for ICT and physical security environments should be designed.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

b) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

c) output from Activity 7.2 Define information security requirements for the ISMS process

d) output from Activity 7.3 Identify assets within the ISMS scope

e) output from Activity 7.4 Conduct an information security assessment

f) output from Activity 8.3 Select the control objectives and controls

g) output from Activity 8.4 Obtain management authorization for implementing and operating an ISMS-Statement of applicability, including the control objectives and the selected controls

h) ISO/IEC 27002:2005

Guidance

In this activity the following should be documented for each control, which should be a part of the ISMS project plan:

a) name of the person responsible for implementation of a control

b) priority of the control to be implemented

c) tasks or activities to implement controls

d) statement of the time by which the control should have been implemented

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

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

Initially, the ICT and physical security should be conceptually designed. The following should be considered:

Responsibilities for the initial implementation process generally include:

a) specification of control objectives with a description of the expected planned state

b) allocation of resources (workload, financial resources)

c) realistic time target for implementation of the control

d) integration options with ICT , physical and organizational security

After the conceptual design, actual design such as system development in order to achieve and implement the best practice for the organization should be done. The following should be considered:

Responsibilities for the actual implementation process include:

a) design for each of the selected controls for ICT, physical and organizational areas at operational level of the workplace

b) Instantiation of each control according to the agreed design

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

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

Depending on the type of controls (ICT, physical or organizational); it may not always be appropriate or necessary to draw a clear-cut line between the initial part and the final part of the implementation process.

The implementation of controls frequently requires cooperation between several different roles within an organization. Thus, for example, persons with system responsibility will be needed to procure, install and maintain technical facilities. Other roles for may be better suited to devising and documenting procedures governing the use of systems.

Information security should be integrated in organization-wide procedures and processes. If this proves difficult for a part of the organization, or a third party, to implement, the relevant parties should communicate this immediately so that a resolution can be agreed upon. Solutions to this type of issue include modifying the procedures and processes, reallocating 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 of implementation

Output

The deliverables of this activity is a structured and detailed implementation plan for controls relating to ICT and physical security as part of the ISMS Project Plan, to include, for each control:

a) detailed description

b) responsibilities for design and implementation

c) expected timescales

d) tasks involved

e) resources required

f) ownership (reporting lines)

Other information

No other specific information.

9.4 Design ISMS specific information security

9.4.1 Plan for management reviews

Activity

A plan should be developed to ensure management involvement and the commitment to review of the ISMS operation and ongoing improvement.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

b) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

c) output from Activity 8.4 Obtain management authorization for implementing and operating an ISMS- Statement of applicability, including the control objectives and the selected controls

d) output from Activity 9.2.3 Design the information security policy

e) ISO/IEC 27004:2009

Guidance

Management review of ISMS activities should begin at the earliest stages of ISMS specification and business case development and continue through to the regular review of ISMS operations. This close involvement provides a means to validate the ISMS against the needs of the business and to maintain the commitment of the business to the ISMS.

The planning of management reviews includes establishing when and how the management reviews should be conducted. Detailed information regarding prerequisites for management reviews is given in sub-clause 7.2 of ISO/IEC 27001:2005.

To plan the review, an assessment of which roles to involve has to be made. Management approval should be sought for the choice of roles, and these roles should then be informed as early as possible. It is advisable to provide management with adequate data regarding the necessity for, and purpose of, the review process. (See Annex B for further information about roles and responsibilities.)

Management reviews should be based upon results from ISMS measurements and other information collected during the operation of the ISMS. This information is used by the activities of ISMS management to determine the maturity and effectiveness of the ISMS. Required inputs and outputs to ISMS measurements are given in ISO/IEC 27001:2005, and further information on ISMS measurements is available in Annex E and ISO/IEC 27004:2009.

It should also be noted that this should include a review of the methodology and results of risk assessment. This should take place at planned intervals, taking into consideration any changes in the environment, such as organization and technology.

Planning for the internal ISMS audit should be done in order to be able to regularly evaluate the ISMS once it has been implemented. The results of the internal ISMS audit are important inputs of ISMS management review. Therefore, before management review is executed, internal ISMS audit should be planned. The internal ISMS audit should include the perspective whether the control objectives, controls, processes and procedures of the ISMS are effectively implemented and maintained and conform to:

a) the requirements of ISO/IEC 27001:2005,

b) relevant legislation or regulations, and

c) the identified information security requirements,

(See Annex C for further information about planning auditing.)

Preconditions of management reviews are the information collected based on the implemented and operated ISMS. The information provided to a management review team may include the following:

a) Incident reports for the last period of operation

b) Verification of control effectiveness and identified non-conformity

c) The results of other regular checks (more detail if the checks have revealed non-compliances with policy).

d) Recommendations for improvement of the ISMS.

A plan for monitoring should document the monitoring results that should be recorded and reported to management, (for additional information on monitoring see Annex E).

Output

The deliverable of this activity output is a document which summarizes the plan needed for the management review addressing:

a) inputs required to perform an ISMS management review

b) procedures for the management review covering the auditing and monitoring and measuring aspects

Other information

Annex B - Roles and Responsibilities for information security

Annex C - Information about Internal Auditing

Annex E - Information about setting up Monitoring and Measuring

9.4.2 Design information security awareness, training and education program

Activity

The Information security awareness, training and education program should be developed.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

b) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

c) output from Activity 7.2 Define information security requirements for the ISMS process- In particular the organizations requirements for information security training and education

d) output from activity 8.4 Obtain management authorization for implementing and operating an ISMS- Statement of applicability, including the control objectives and the selected controls

e) output from activity 8.3 Select the control objectives and controls - Risk treatment plan

f) output from activity 9.2:3 Design the information security policy

g) output from activity 9.2.4 Develop information security standards and procedures

h) overview of the organization´s general education and training program

Guidance

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 be aware of and 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 to ensure at this point that every employee within the ISMS scope receives the necessary security training and/or education. In large organizations, a single body of training material is generally not sufficient, as it will contain too much data which is relevant only to specific types of job, and therefore will be large, complex and hard to use. In these cases, it is usually appropriate to have different sets of training material designed for each broad type of role, such as office workers, IT staff or drivers, which is customised to their specific needs."

An information security awareness training and education program should ensure that records of security training and education are generated. These records should regularly be reviewed to ensure that all personnel have received the training that they require. A role should be made responsible for this process.

Information security training materials should be designed to tie in with other training materials used by the organization, especially training courses provided to users of IT systems. Training in relevant aspects of information security should ideally be integrated into every course for IT users.

Information security training material should contain the following points as a minimum, as appropriate to the target audience:

a) risks and threats regarding information security

b) basic terms of information security

c) clear definition of a security incident: guidance as to how one may be identified and how it should be dealt with and reported

d) information security policy, standards and procedures of the organization

e) responsibilities and reporting channels relating to information security in the organization

f) guidance on how to assist in improving information security

g) guidance on information security incidents and reporting

h) where to obtain further information.

An information security training team should be determined which may include the following tasks:

a) creating and managing training records

b) creating and managing training materials,

c) carrying out training

These tasks may be allocated using existing training staff. But the existing staff may require substantial training in information security concepts to ensure that these are presented effectively and accurately.

An information security awareness, training and education program should include a procedure to ensure that the training materials are reviewed and updated regularly. A role should be made explicitly responsible for reviewing and updating training materials.

Output

The deliverables of this activity are:

a) information security awareness, education and training materials

b) formation of information security awareness education and training, including roles and responsibilities

c) plans for information security awareness, education and training

d) actual records showing the results of information security awareness, education and training of employees

Other information

No other specific information.

9.5 Produce the final ISMS project plan

Activity

The ISMS project plan should be finalized including the activities necessary to implement selected controls.

Input

a) output from Activity 6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries - The scope and boundaries of the ISMS

b) output from Activity 6.6 Develop the ISMS policy and obtain approval from management – The ISMS policy

c) output from Activity 9.2 – Design Organizational Information Security

d) output from Activity 9.3 – Design ICT and Physical Information Security

e) output from Activity 9.4 – Design ISMS specific Information Security

f) ISO/IEC 27002:2005

Guidance

The activities required to implement selected controls and carry out other ISMS related activities should be formalized in a detailed implementation plan as part of the final ISMS project. The detailed implementation plan may also be supported by descriptions of proposed implementation tools and methods. As an ISMS Project involves many different roles in the organization, it is important that the activities are clearly assigned to responsible parties, and that the plan is communicated both early in the project, and throughout the organization.

As with all projects, it is of course essential that the person responsible for the project ensures that sufficient resources have been allocated to the project.

Output

The deliverable of this activity is the final ISMS project implementation plan.

Other information

No other specific information.

Annex A
(informative)

Checklist description

Purpose:

- to provide a checklist of activities required to establish and implement an ISMS
- to support monitoring of progress for an ISMS implementation
- Map related ISMS implementation activities to respective ISO/IEC 27001 requirements

Implementation Phase ISO/IEC 27003	Step number	Activity, reference ISO/IEC 27003	Step Pre-Requisite	Documented Output	Reference to ISO/IEC 27001
5 Obtaining Management Approval for the implementation of ISMS	1.	Gather corporation business objectives	None	List of corporation business objectives	N/A
	2.	Gain understanding of existing management systems	None	Description of existing management systems	N/A
	3.	5.2 Define objectives, information security needs, business requirements for ISMS	1, 2	Summary of the objectives, information security needs and business requirements for the ISMS	N/A
	4.	Gather relevant regulatory, compliance, and industry standards applicable to the corporation	None	Summary of regulatory, compliance, and industry standards that are applicable to the corporation	N/A
	5.	5.3 Define preliminary ISMS scope	3, 4	Description of preliminary scope of ISMS (5.3.1)	N/A
				Definition of ISMS roles and responsibilities (5.3.2)	N/A
	6.	5.4 Create the business case and the project plan for management approval	5	Business case and proposed project plan	N/A
	7.	5.5 Obtain management approval and commitment to initiate a project to implement an ISMS	6	Management approval to initiate a project to implement an ISMS	N/A

Implementation Phase ISO/IEC 27003	Step number	Activity, reference ISO/IEC 27003	Step Pre-Requisite	Documented Output	Reference to ISO/IEC 27001
6 Defining ISMS Scope and ISMS Policy	8.	6.2 Define organizational boundaries	7	• Description of organizational boundaries • Organization's functions and structure • information exchange through boundaries • Business processes and the responsibilities for the information assets of the scope and outside scope	4.2.1.a) (partially)
	9.	6.3 Define information communication technology boundaries	7	• Description of ICT boundaries • Description of information systems and telecommunication networks describing the inside and the outside of the scope	4.2.1.a) (partially)
	10.	6.4 Define physical boundaries	7	• Description of physical boundaries for the ISMS • Description of the organization and their geographical characteristics describing the internal and external scope	4.2.1.a) (partially)
	11.	6.5 Finalize boundaries for ISMS scope	8, 9, 10	A document describing the scope and boundaries of the ISMS	4.2.1.a)
	12.	6.6 Develop the ISMS policy	11	Management-approved ISMS Policy	4.2.1.b)

Implementation Phase ISO/IEC 27003	Step number	Activity, reference ISO/IEC 27003	Step Pre-Requisite	Documented Output	Reference to ISO/IEC 27001
7 Conducting Organization Analysis	13.	7.2 Define information security requirements supporting the ISMS	12	• List of the main processes, functions, location, information systems, communication networks	N/A
				Organization's requirements addressing confidentiality, availability, and integrity	N/A
				Organization's requirements addressing legal and regulatory, contractual and business information security requirements	4.2.1.c) 1) partially
				List of known vulnerabilities to the organization	4.2.1.d) 3)
	14.	7.3 Identify assets within the ISMS scope	13	Description of the main processes of the organization	N/A
				Identification of Information assets of the main processes of the organization	4.2.1.d) 1)
				Critical processes/assets classification	N/A

Implementation Phase ISO/IEC 27003	Step number	Activity, reference ISO/IEC 27003	Step Pre-Requisite	Documented Output	Reference to ISO/IEC 27001
	15.	7.4 Generate an information security assessment	14	• Document of organization's actual information security status and evaluation, including existing information security controls • Document of organization's assessed and evaluated deficiencies	4.2.1.e) 2) partially
8 Conducting Risk Assessment and Selecting Risk Treatment Options	16.	8.2 Conduct risk assessment	15	• Scope for risk assessment • Approved risk assessment methodology, aligned with organization's strategic risk management context • Risk acceptance criteria	4.2.1.c) 1)
	17.	8.3 Select the control objectives & controls	16	Documented high-level risk assessment	4.2.1.e) 3) partially;
				Identify the need for additional in-depth risk assessment	N/A
				Documented in-depth risk assessment	4.2.1.e) 3) partially
				Aggregated results of risk assessment	N/A
	18.	8.4 Obtain management approval for implementing an ISMS	17	Risks and their identified options for risk treatment	4.2.1.f)
				Selected control objectives and controls for risk reduction	4.2.1.g)

Implementation Phase ISO/IEC 27003	Step number	Activity, reference ISO/IEC 27003	Step Pre-Requisite	Documented Output	Reference to ISO/IEC 27001
	19.	Management approval of residual risks	18	Documented management approval of the proposed residual risks (should be output of 8.4)	4.2.1.h)
	20.	Management authorization of to implement and operate the ISMS	19	Documented management authorization to implement and operate ISMS (should be output of 8.4)	4.2.1.i)
	21.	Prepare statement of applicability	18	Statement of Applicability	4.2.1.j)
9 Designing the ISMS	22.	9.2 Design organizational security	20	Organization structure, and its information security related roles and responsibilities	5.1.c)
				• Identification of ISMS-related documentation • Templates for ISMS records and instructions for their use and storage	4.3
				Information security policy document	ISO/IEC 27002; 5.1.1
				Baseline of information security policies and procedures (and if applicable plans for developing specific policies, procedures etc.)	
	23.	9.3 Design ICT and physical Security	20, 21	• Implementation project plans for the implementation process for the selected security controls for ICT and physical information security	4.2.2.c) partially

Implementation Phase ISO/IEC 27003	Step number	Activity, reference ISO/IEC 27003	Step Pre-Requisite	Documented Output	Reference to ISO/IEC 27001
	24.	9.4 Design ISMS specific information security	22, 23	Procedures describing the the reporting and management review processes	7.1
	25.			• Descriptions for auditing, monitoring and measuring	4.2.3.a) partially 4.2.3.b) partially; 6
	26.			• A Training and Awareness Program	5.2.2
	27.	9.5 Produce the final ISMS project plan	25	Management-approved Implementation project plan for the implementation processes	N/A
	28.	The final ISMS project plan	28	An ISMS organization specific implementation project plan covering the planned execution of activities for organizational, ICT and Physical information security as well as ISMS specific requirements for implementing an ISMS according to the results of the activities covered in ISO/IEC 27003	N/A

Annex B
(informative)

Roles and responsibilities for Information Security

This annex provides additional guidance on roles and responsibility within an organization related to information security. The roles are first given in the organizational view for implementing an ISMS. A table summarizes this information and presents general examples of roles and responsibilities.

1. Role of the Information Security Committee

The information security committee should have a leading role for the ISMS in an organization. The information security committee should be responsible for handling the organization's information assets, and should have a sufficient understanding of information security for directing, monitoring, and completing necessary tasks.

The following are examples of possible information security committee roles:

a) Completion of risk management, establishing the plan for the ISMS documents, being responsible for determining the contents of these documents and acquiring acceptance from the management

b) Planning the purchase of new equipment and/or deciding the reuse of existing equipment that the organization already possesses

c) Handling any problems that may arise

d) Considering improvements arising from following implementation and measurement of the ISMS

e) Give strategic direction to the ISMS (both during the implementation project and in operation), and

f) liaison between senior management and the implementation project team and information security people.

2. Roles for the Information Security Planning Team

The project team responsible for the ISMS, when planning the project, 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 departmental boundaries. To do this, its members 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 for the duties above (if possible, members with one exclusive role) 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 organization". The people responsible for given operations in an organization may know their specific fields best. The many specialists who are experts in specific fields in their organization should be referred to in terms of ISMS 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 organization objectives. External consultants can give advice 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 organization's 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. Information Asset owners

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

In case of risk sharing, risk avoidance and risk retention, the necessary actions should be taken from the organizational security aspects. If the decision has been made to transfer risks, the appropriate actions should be taken, using contracts, insurance arrangements and organizational structure such as partnership and joint ventures.

Figure B.1 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.

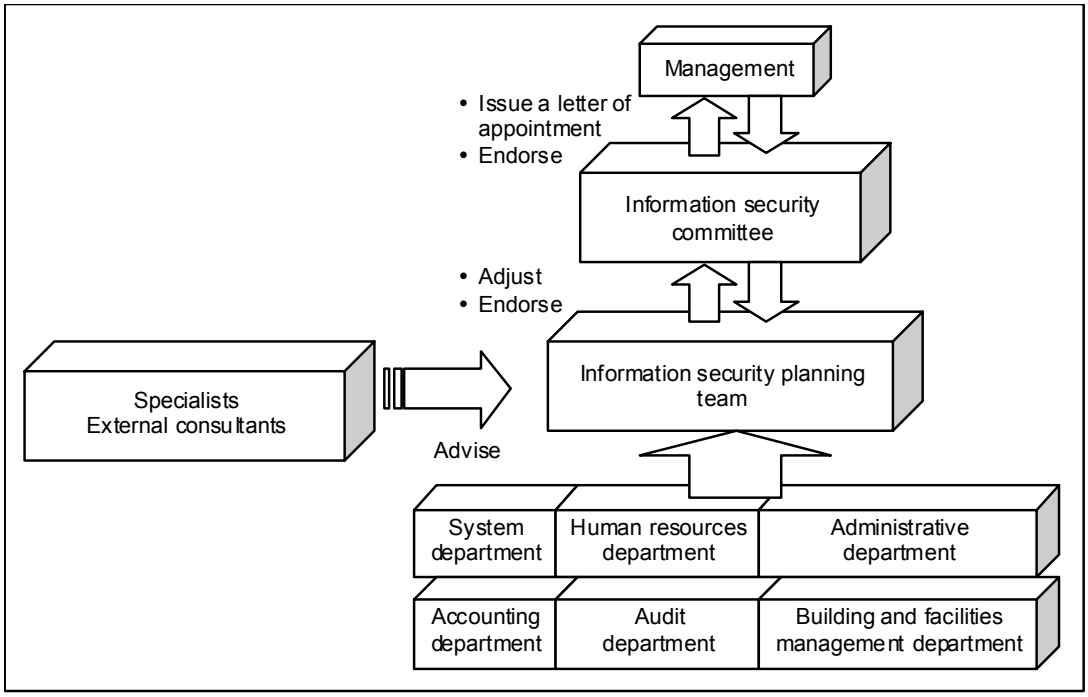


Figure B.1 — Example Organizational Structure for Establishing the ISMS

Interaction with the organization

All parties involved should review and become very familiar with the current requirements for protecting the organization's assets. Participation in organizational 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. organization unit heads)

e) process owners (i.e. representing important operational areas)

f) specialists and external consultants

Examples of general roles and responsibilities related to information security

Information security is a wide area that affects the whole organization. As such, clearly defined security responsibilities are essential for a successful implementation. As security related roles and responsibilities vary, an understanding of the different roles is fundamental for understanding some of the activities described later in this International Standard. The table below outlines security related roles and responsibilities. It should be noted that these roles are general, and specific descriptions are needed for each individual implementation of an ISMS.

Table B.1 — List of exemplified Roles and Responsibilities for Information Security

Role	Brief Description of Responsibility
Senior Management (e.g. COO, CEO, CSO and CFO)	for vision, strategic decisions and coordinates activities to direct and control the organization.
Line Managers	has the top responsibility for organizational functions.
Chief Information Security Officer	has the overall responsibility and governance for information security ensuring the correct handling of information assets.
Information Security Committee (member of)	handling the information assets and has a leading role for the ISMS in the organization.
Information Security Planning Team (member of)	During operations while the ISMS is being established. The planning team works across departments and resolves conflicts until the ISMS is established.
Stakeholder	In the context of the other roles' descriptions concerning information security, the stakeholder is primarily here defined as 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 such as shareholders in a private organization). 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 Manager	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 Manager.
Risk Management	The person/persons responsible for the organization's risk management framework including risk evaluation, risk treatment and risk monitoring.
Legal Advisor	Many information security risks have legal aspects and the legal advisor is responsible for taking these into consideration.
Human Resources	The person/persons with overall responsibility for the staff.

Role	Brief Description of Responsibility
Archive	All organizations have archives containing vital information that needs to be stored for the long term. The information may be located on multiple types of media and a specific person should be responsible for the security of 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 that oversees personal integrity and privacy issues.
System developer	If an organization develops their own information systems, someone has the responsibility for this development.
Specialist / Expert	The specialists and experts responsible for some operations in an organization should be referred to in terms of their intention about ISMS matters as it relates to use in their specific fields.
External Consultant	External consultants can give advice based on their macroscopic points of view of an organization and industry experience. However, consultants may not have the depth knowledge of the organization and operations of the organization.
Employee / Staff / User	Each employee is equally responsible for maintaining information security in the workplace and in his/her 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 organization that has local responsibility for IT matters, and possibly for information security as well.
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”.

Annex C
(informative)

Information about Internal Auditing

This Annex provides additional guidance to support the planning of auditing.

The implementation of an 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.

In an ISMS audit, auditing results should be determined based on evidence. Therefore, some suitable length of time during the ISMS operations should be allocated to collecting suitable evidence.

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.When organizations use external auditors, the following should be considered: external auditors are themselves familiar with the internal ISMS audits; however they may not have enough knowledge about the organizational environment of the organization. This information should be supplied by internal staff. On the other hand, internal auditors may be able to perform detailed audits considering the organization’s organizational environment, but may not have enough knowledge about performing ISMS audits. Organizations should recognize the characteristics and potential shortcomings of internal vs. external auditors carrying out the internal ISMS audits.

The effectiveness and efficiency of the implemented controls (see ISO/IEC 27004:2009) should be examined within the scope of internal audits.

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. Therefore, Organization units or individuals that are outside the scope 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. Depending on the size of the organization, it might be useful to call in external auditors to avoid the situation in which staff members become blinkered to their own work.

In an internal ISMS audit, it should be checked that the ISMS is being operated effectively and maintained and as expected. Auditors should 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 previous audits.

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. 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.

A manager who is responsible for a process being audited should ensure that nonconformities and their causes are appropriately addressed without delay. However, this does not mean that the nonconformity necessarily needs to 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 can be performed effectively as a part of, or in collaboration with, other internal audits of the organization. When performing the audit, it is a good idea to refer to "Requirements for bodies providing audit and certification of ISMS ISO/IEC 27006:2007”.

Annex D
(informative)

Structure of policies

This annex provides additional guidance on the structure of policies including the information security policy.

In general, a policy is statement of overall intention and direction as formally expressed by management (see FCD 27000 and ISO/IEC 27002). The content of a policy guides actions and decisions concerning the topic of the policy. An organization may have a number of policies; one for each of the activity areas that is important to the organization. Some policies are independent of each other, while other policies have a hierarchical relationship. In the area of security, policies are commonly organized hierarchically. Typically, the organization's security policy is the highest level policy. This is supported by a range of more specific policies, including the information security policy and the Information Security Management System policy. In turn the information security policy can be supported by a number of more detailed policies on specific topics related to aspects of information security. A number of these are discussed in ISO/IEC 27002, for example the information security policy is supported by policies concerning access control, clear desk and clear screen, the use of network services, and the use of cryptographic controls. It is possible that additional layers of policies may be added in some cases. This arrangement is shown in figure D1.

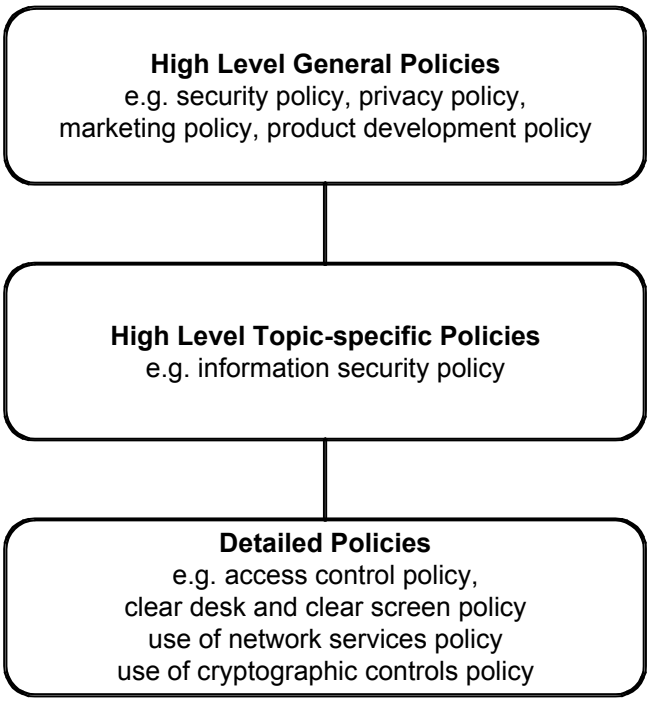


Figure D.1 — Policy hierarchy

ISO/IEC 27001 requires organizations to have both an ISMS policy and an information security policy. It does not, however specify any particular relationship between these policies. Requirements for the ISMS policy are given in clauses 4.2.1 of ISO/IEC 27001. Guidelines for information security policies are given in clause 5.1.1 of ISO/IEC 27002. These policies may be developed as peer policies, the ISMS policy may be subordinate to the information security policy, or the information security policy may be subordinate to the ISMS policy.

The content of policies is based on context in which an organization operates. Specifically the following should be considered when developing any policy within the policy framework.

1) The aims and objectives of the organization

2) Strategies adopted to achieve its objectives

3) The structure and processes adopted by the organization

4) Aims and objectives associated with the topic of the policy

5) The requirements of related higher level policies

This is shown in Figure D.2.

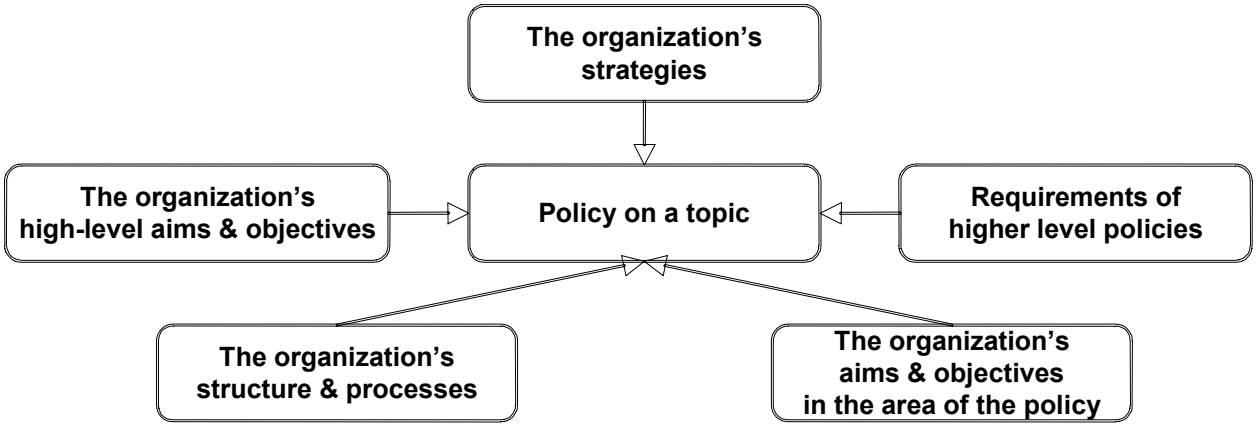


Figure D.2 — Inputs to the development of a policy

Policies can have the following structure:

1. Policy Summary – A one or two sentence overview. (This may sometimes be merged with the introduction.)

2. Introduction – a brief explanation of the topic of the policy.

3. Scope – describes those parts or activities of an organization that are affected by the policy. If relevant, the scope clause lists other policies that are supported by the policy.

4. Objectives – describes the intent of the policy.

5. Principles – describes the rules concerning actions and decisions for achieving the objectives. In some cases it can be useful to identify the key processes associated with the topic of the policy and then the rules for operating the processes.

6. Responsibilities – describes who is responsible for actions to meet the requirements of the policy. In some cases this may include a description of organizational arrangements as well as the responsibilities of people with designated roles.

7. Key Outcomes – describes the business outcomes if the objectives are met.

8. Related policies – describes other policies relevant to the achievement the objectives, usually by providing additional detail concerning specific topics.

NOTE Policy content can be organized in a variety of ways. For example, organizations that place emphasis on roles and responsibilities may simplify the description of objectives, and apply the principles specifically to the description of responsibilities.

The following is an example of an information security policy, showing its structure and example content.

Information Security Policy (Example)

Policy Summary

Information should always be protected, whatever its form and however it is shared, communicated or stored.

Introduction

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Scope

This policy supports the organization's general security policy.

This policy applies to all of the organization.

Information Security Objectives

1) Strategic and operational information security risks are understood and treated to be acceptable to the organization.

2) The confidentiality of customer information, product development and marketing plans is protected.

3) The integrity of accounting records is preserved.

4) Public web services and internal networks meet specified availability standards.

Information Security Principles

1) This organization encourages risk-taking and tolerates risks that might not be tolerated in conservatively managed organizations provided that information risks are understood, monitored and treated when necessary. Details of the approach taken to risk assessment and treatment are found in the ISMS policy.

2) All staff will be made aware and accountable for information security as relevant to their job-role.

3) Provision will be made for funding information security controls in operational and project management processes.

4) Possibilities for fraud associated with abuse of information systems will be taken into account in the overall management of information systems.

5) Information security status reports will be available.

6) Information security risks will be monitored and action taken when changes result in risks that are not acceptable.

7) Criteria for risk classification and risk acceptability are found in the ISMS policy.

8) Situations that could place the organization in breach of laws and statutory regulations will not be tolerated.

Responsibilities

1) The senior management team is responsible for ensuring that information security is adequately addressed throughout the organization.

2) Each senior manager is responsible for ensuring that the people who work under their control protect information is accordance with the organizations standards.

3) The chief security officer advises the senior management team, provides specialist support for the organization's staff, and ensures that information security status reports are available.

4) Every staff member has information security responsibilities as part of doing their job.

Key Outcomes

1) Information security incidents will not result in serious and unexpected costs or serious disruption of services and business activities.

2) Fraud losses will be known and within acceptable bounds.

3) Customer acceptance of product or services will not be adversely affected by concerns about information security.

Related Policies

The following detailed policies provide principles and guidance on specific aspects of information security.

1) the Information Security Management System (ISMS) policy

2) the access control policy

3) the clear desk and clear screen policy

4) the unauthorized software policy

5) the policy concerning obtaining files of software either from or via external networks

6) the policy concerning mobile code

7) the back-up policy

8) the policy concerning the exchange of information between organizations

9) the policy concerning acceptable use of electronic communications facilities

10) the record retention policy

11) the policy on the use of network services

12) the policy concerning mobile computing and communication

13) the teleworking policy

14) the policy on the use of cryptographic controls

15) the compliance policy

16) the policy on software licensing

17) the policy on software disposal

18) the data protection and privacy policy

All of these policies support:

- Risk identification, by providing a baseline of controls, that can be used to identify gaps in systems designs and implementations; and

- Risk treatment by supporting identification of treatments for identified vulnerabilities and threats.

Risk Identification and Risk Treatment are both processes defined under Principles section of the policy. Refer to the ISMS Policy for details.

Annex E
(informative)

Monitoring and measuring

This annex provides additional guidance to support the planning and designing monitoring and measuring.

Information on Setting Up Monitoring and Measuring

The design of the ISMS specific requirements includes security monitoring and measurement program for the ISMS that supports management review

Designing Monitoring

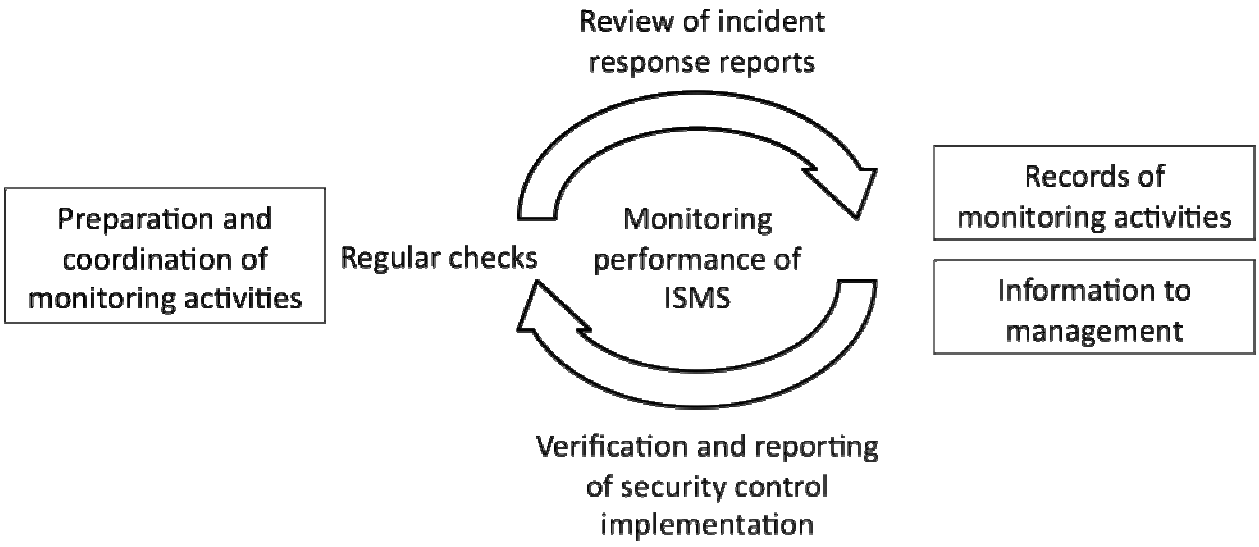


Figure E.1 — The Monitoring Process flow

Preparation and coordination: Identification of relevant assets for monitoring

It should be noted that monitoring is a continuous process and, as such, the design should 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 previously set organizational activities/processes and linked assets are the basic scope for monitoring (bullet “Against what” above). To design 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 and the selection of controls in order to find what should be monitored on the assets and linked organization activities/processes. (This will set both what to Detect and When.)

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

To ensure that the monitoring is truly effective, it is important to coordinate and make the final design of all activities for monitoring.

Monitoring activities

In order to maintain the level of information security, the information security controls identified as appropriate should be correctly applied; security incidents should be detected and responded to in a timely manner, and the performance of the information security management system should be monitored regularly. Regular checks should be performed to see whether all controls are being applied and implemented as planned in the information security concept. This should 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 motivation is recognised by all those involved as being 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, the results from the activities should be designed in terms of how records are made and information given to management. Formal documentation should be made to describe the design and covering principle activities and their purpose, as well as different responsibilities.

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 fulfil its management and supervisory duties should be recorded therein with the required level of detail.

b. Information to management for decision 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.

Setting up the information security measurement program

Overview for designing an information security measurement program

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 measurement program (ISO/IEC 27004:2009). The design of the program needs to be viewed in the perspective of 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 required 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, previously 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/IEC 27004:2009 for further details

b) Pay attention to the information needs, see ISO/IEC 27004:2009 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 person or organizational unit responsible 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's 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/IEC 27004:2009.

The result of the Plan Phase suitable measurements should be conducted to fulfil these objectives.

A suitable Information Security Measurement Programme could be different depending on the organization's structure:

- Size
- Complexity
- Overall risk profile/need of information security

Generally, the larger and more complex an organization, the more extensive the measurement program needed. But the level of overall risk affects the extent of the measurement program as well. If the impact of poor information security is severe, a comparatively smaller organization may need a more comprehensive measurement program in order to cover the risk 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 need to be covered and the results from the risk analysis.

Designing the information security measurement program

The person responsible for the information security measurement program should consider the following:

- Scope
- Measurements
- Carry out the measurements
- Periods of measurements
- Reporting

The scope of the measuring program should cover the scope, control objectives and controls of the ISMS. In particular, the objectives and boundaries of the ISMS Measurement should be set in terms of the characteristics of the organization, the organization, its location, assets and technology, and include 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 single measurements, ISO/IEC 27004:2009 Information Security Measurement Process stipulates that the starting point is the object of measure. In order to establish a measurement program these objects should be identified. These objects could be a process or a resource. (See ISO/IEC 27004:2009 for further details). When defining the program the objects defined by ISMS scope is often broken down to find the actual objects that should be measured. This defining process could be exemplified by the following example: The Organization is the overall object – Organization Process A/or IT system X is a part of that object and constitutes an object in itself– Objects within that process that affect 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 consider that the objects of measure may serve many organization processes within the ISMS scope, and may therefore 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 measurement interval may vary, but is preferable that the measurement is done or summarized at certain intervals in order to fit into the management review and the continual improvement process and ambitions of the ISMS. The design of the program should state this.

The reporting of the results should be designed so that communication is assured according to ISO/IEC 27004:2009.

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 its own measuring points, these have to be documented as part of the design phase; for further reference see ISO/IEC 27004:2009. This document may be quite comprehensive and does not necessarily need to be signed by management, as the details may change when implemented.

Measuring the effectiveness of the ISMS

When setting the scope for the Information Security Measurement Program that should be implemented, care should be taken so that the objects are not too numerous. If they are, it may be wise to divide the program into different parts. The scope of these parts may be seen as separate measurements for comparison, but their main purpose prevails: that a combination of the measurements provides an indication to evaluate ISMS effectiveness. These sub-scopes are normally an organizational unit that could be defined with clear boundaries. A combination of objects that serves many organization 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 is 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 27004:2009.)

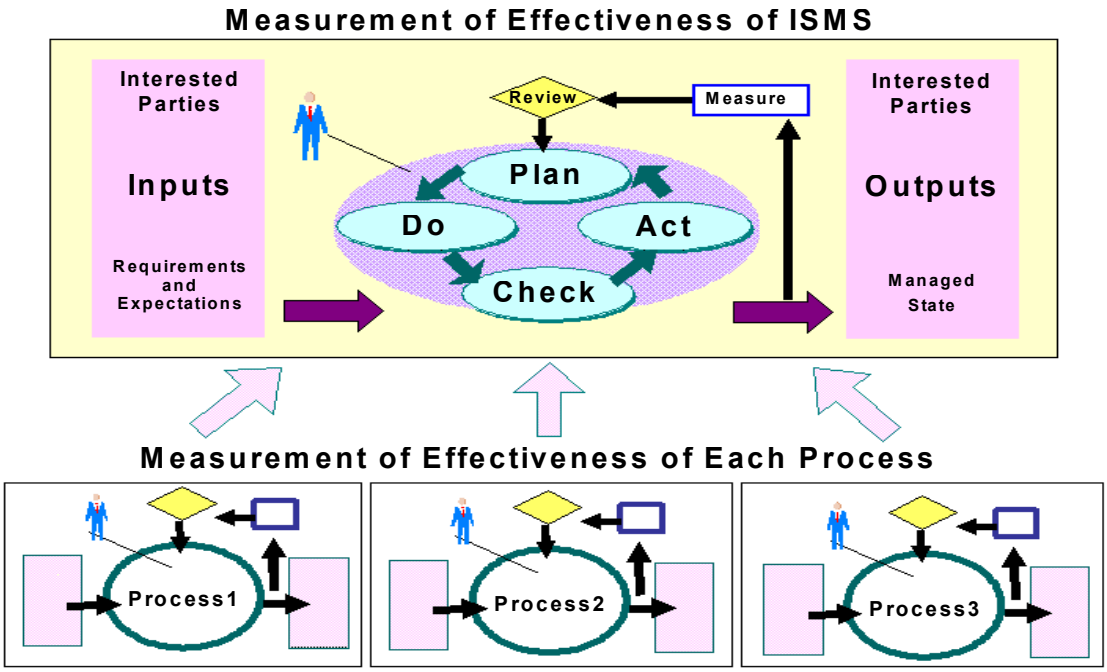


Figure E.2 — Two aspects of measurement effectiveness with the PDCA process of ISMS and the examples of process within the organization

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 person responsible for the measuring program should have 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 27001:2005 is “the measurement of controls or series of controls.” (see 4.2.2 d) in ISO/IEC 27001:2005)

NOTE 2 The requirement related to the effectiveness of the entire ISMS in ISO/IEC 27001:2005 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 27001:2005).

The actual carrying out of measurements could be done using internal personnel, 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 accustomed to internal audits, internal resources may be just as valid.

Bibliography

[1] ISO 9001:2008, *Quality management systems — Requirements*

[2] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*

[3] ISO/IEC 15026 (all parts), *Systems and software engineering — Systems and software assurance*[1)]

[4] ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[5] ISO/IEC 15408-2:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

[6] ISO/IEC 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

[7] ISO/IEC TR 15443-1:2005, *Information technology — Security techniques — A framework for IT security assurance — Part 1: Overview and framework*

[8] ISO/IEC TR 15443-2:2005, *Information technology — Security techniques — A framework for IT security assurance — Part 2: Assurance methods*

[9] ISO/IEC TR 15443-3:2007, *Information technology — Security techniques — A framework for IT security assurance — Part 3: Analysis of assurance methods*

[10] ISO/IEC 15939:2007, *Systems and software engineering — Measurement process*

[11] ISO/IEC 16085:2006, *Systems and software engineering — Life cycle processes — Risk management*

[12] ISO/IEC 16326:2009, *Systems and software engineering — Life cycle processes — Project management*

[13] ISO/IEC 18045:2008, *Information technology — Security techniques — Methodology for IT security evaluation*

[14] ISO/IEC TR 19791:2006, *Information technology — Security techniques — Security assessment of operational systems*

[15] ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*

[16] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[17] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*

[18] ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*

[19] ISO 21500, *Project management — Guide to project management*[2)]

[20] ISO/IEC 27006:2007 *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

1) To be published.

2) Under preparation.

ICS 35.040
Price based on 68 pages