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)

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.

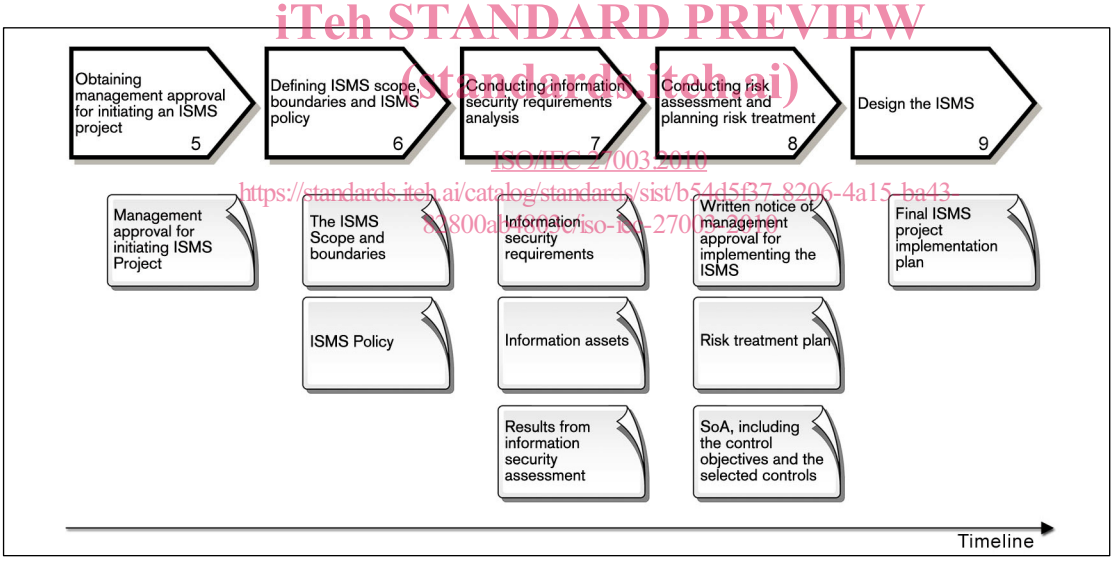


Figure 1 — ISMS project phases

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

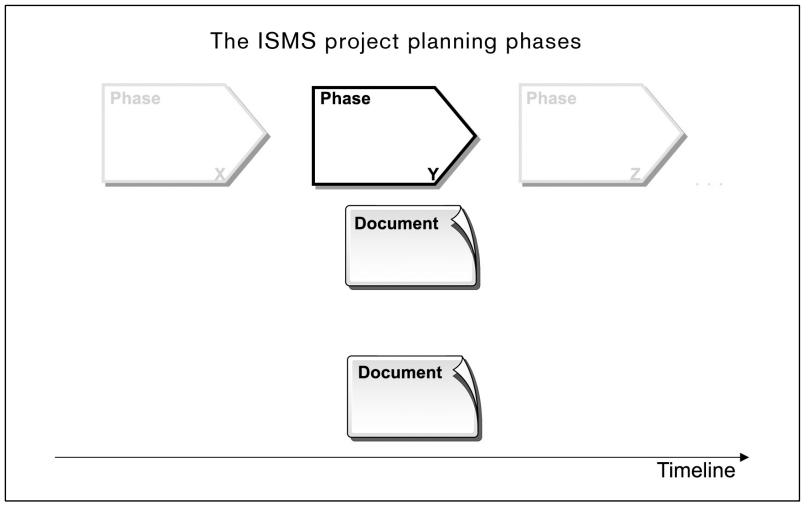
The other information provides any additional information that may assist in performing the activity, for example references to other standards.

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.



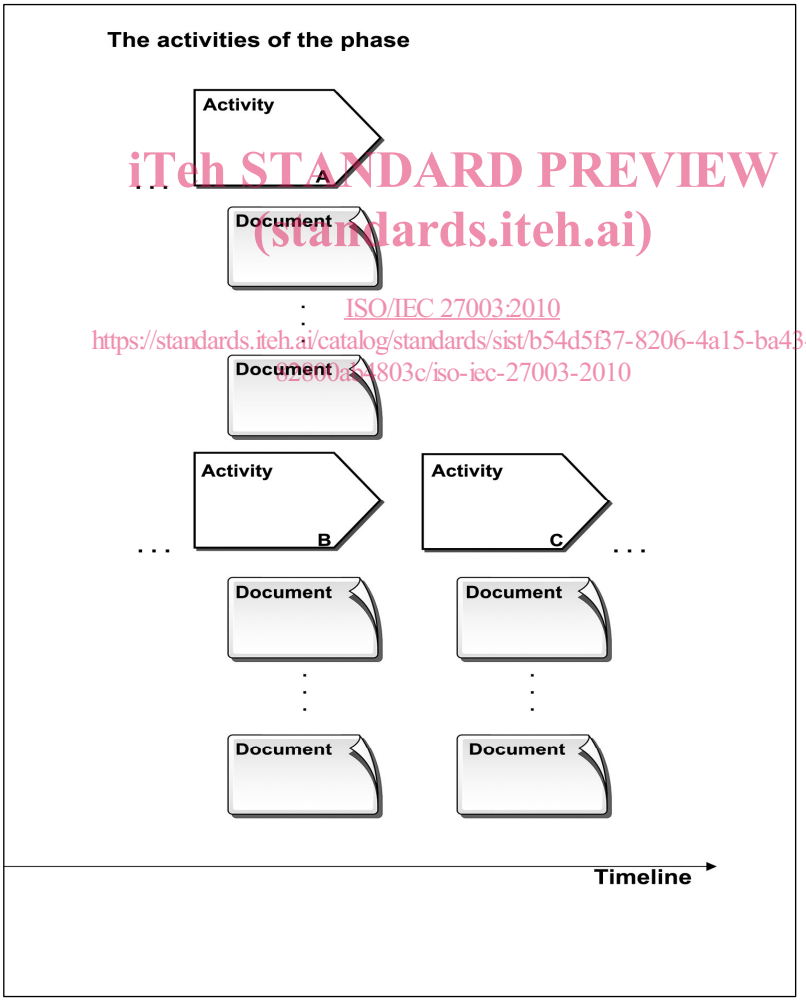


Figure 2 — Flow diagram legend

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.

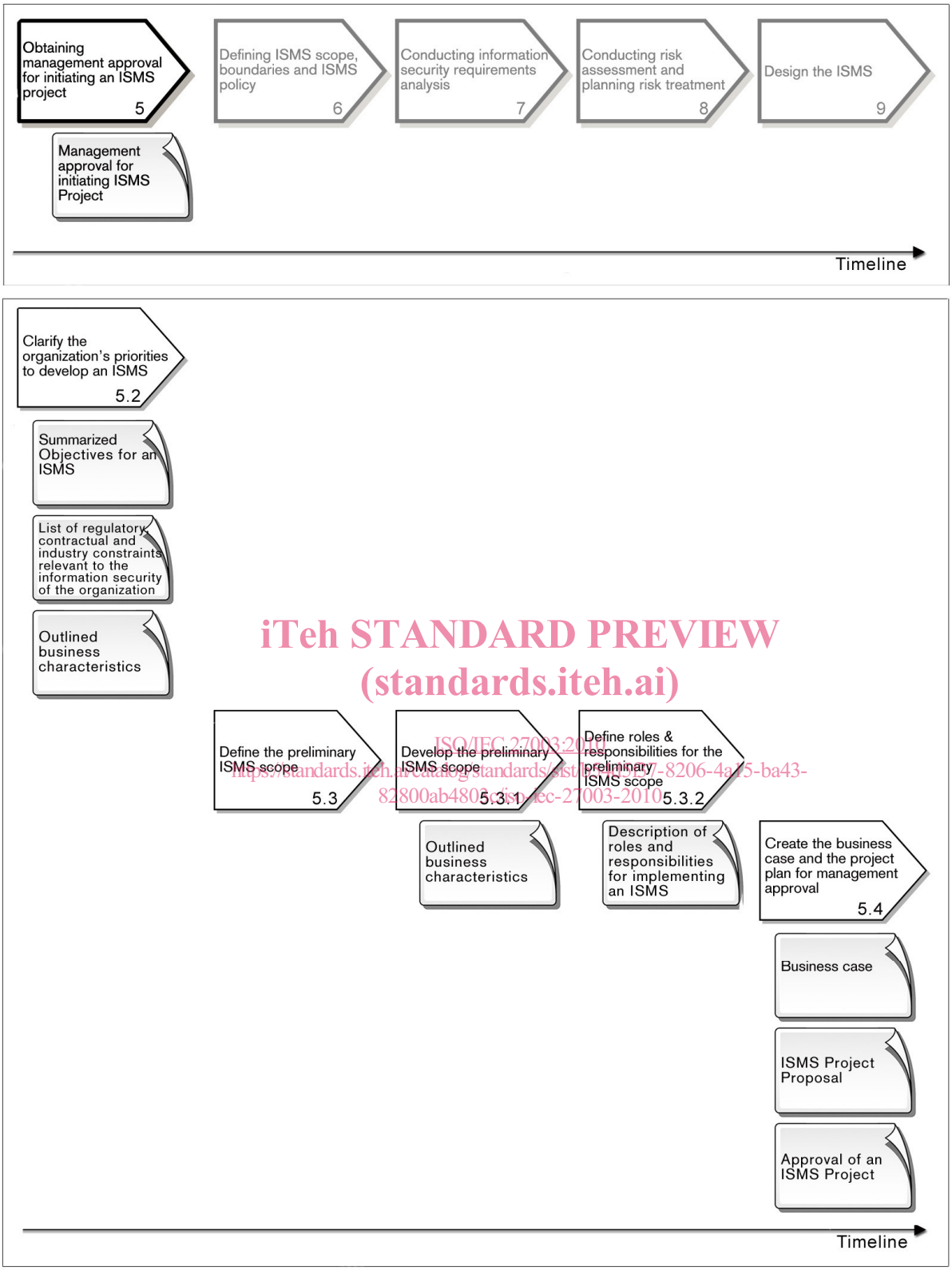


Figure 3 — Overview of obtaining management approval for initiating an ISMS project

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.