BRITISH STANDARD

BS ISO/IEC 27003:2010

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

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

AVA Documents Document Sharing Hub
British Standards

Full document details: BS ISO/IEC 27003:2010

National foreword

This British Standard is the UK implementation of ISO/IEC 27003:2010.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2010

© BSI 2010

ISBN 978 0 580 55344 8

Amendments/corrigenda issued since publication

Date	Comments

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27003:2010

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)

Documents
Document Sharing Hub
© ISO/IEC 2010

Full document details: BS ISO/IEC 27003:2010

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/IEC 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27003:2010

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Structure of this International Standard 2
4.1 General structure of clauses 2
4.2 General structure of a clause 3
4.3 Diagrams 3

5 Obtaining management approval for initiating an ISMS project 5
5.1 Overview of obtaining management approval for initiating an ISMS project 5
5.2 Clarify the organization's priorities to develop an ISMS 7
5.3 Define the preliminary ISMS scope 9
5.4 Create the business case and the project plan for management approval 11

6 Defining ISMS scope, boundaries and ISMS policy 12
6.1 Overview of defining ISMS scope, boundaries and ISMS policy 12
6.2 Define organizational scope and boundaries 15
6.3 Define information communication technology (ICT) scope and boundaries 16
6.4 Define physical scope and boundaries 17
6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries 18
6.6 Develop the ISMS policy and obtain approval from management 19

7 Conducting information security requirements analysis 20
7.1 Overview of conducting information security requirements analysis 20
7.2 Define information security requirements for the ISMS process 22
7.3 Identify assets within the ISMS scope 23
7.4 Conduct an information security assessment 24

8 Conducting risk assessment and planning risk treatment 25
8.1 Overview of conducting risk assessment and planning risk treatment 25
8.2 Conduct risk assessment 27
8.3 Select the control objectives and controls 28
8.4 Obtain management authorization for implementing and operating an ISMS 29

9 Designing the ISMS 30
9.1 Overview of designing the ISMS 30
9.2 Design organizational information security 33
9.3 Design ICT and physical information security 38
9.4 Design ISMS specific information security 40
9.5 Produce the final ISMS project plan 44

Annex A (informative) **Checklist description** 45

Annex B (informative) **Roles and responsibilities for Information Security** 51

Annex C (informative) **Information about Internal Auditing** 55

Annex D (informative) **Structure of policies** 57

Annex E (informative) **Monitoring and measuring** 62

Bibliography 68

Documents
Document Sharing Hub

© ISO/IEC 2010 – All rights reserved

Full document details: BS ISO/IEC 27003:2010

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*.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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).

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27003:2010

INTERNATIONAL STANDARD ISO/IEC 27003:2010(E)

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

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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.

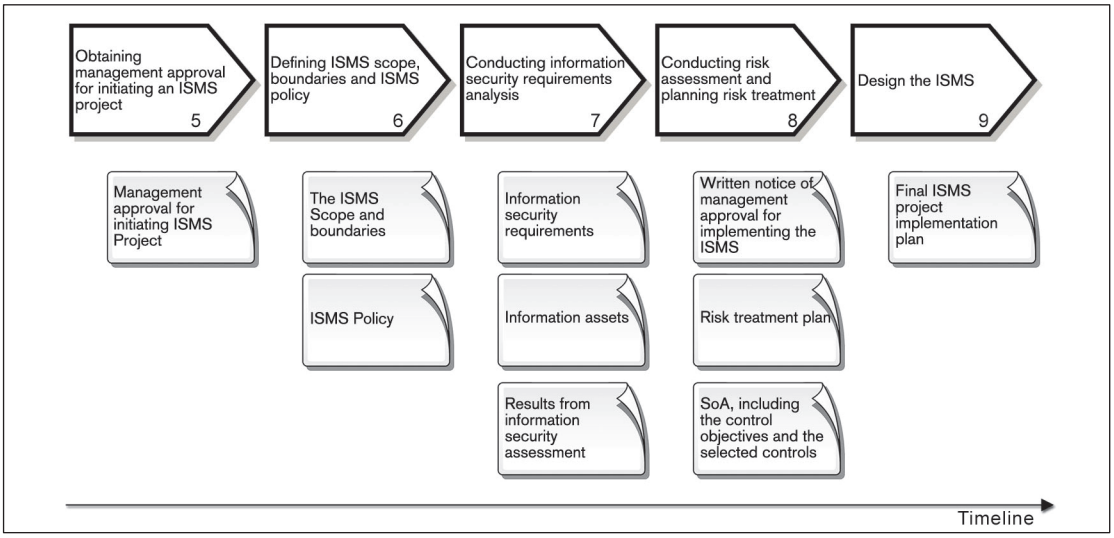

Figure 1 — ISMS project phases

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

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

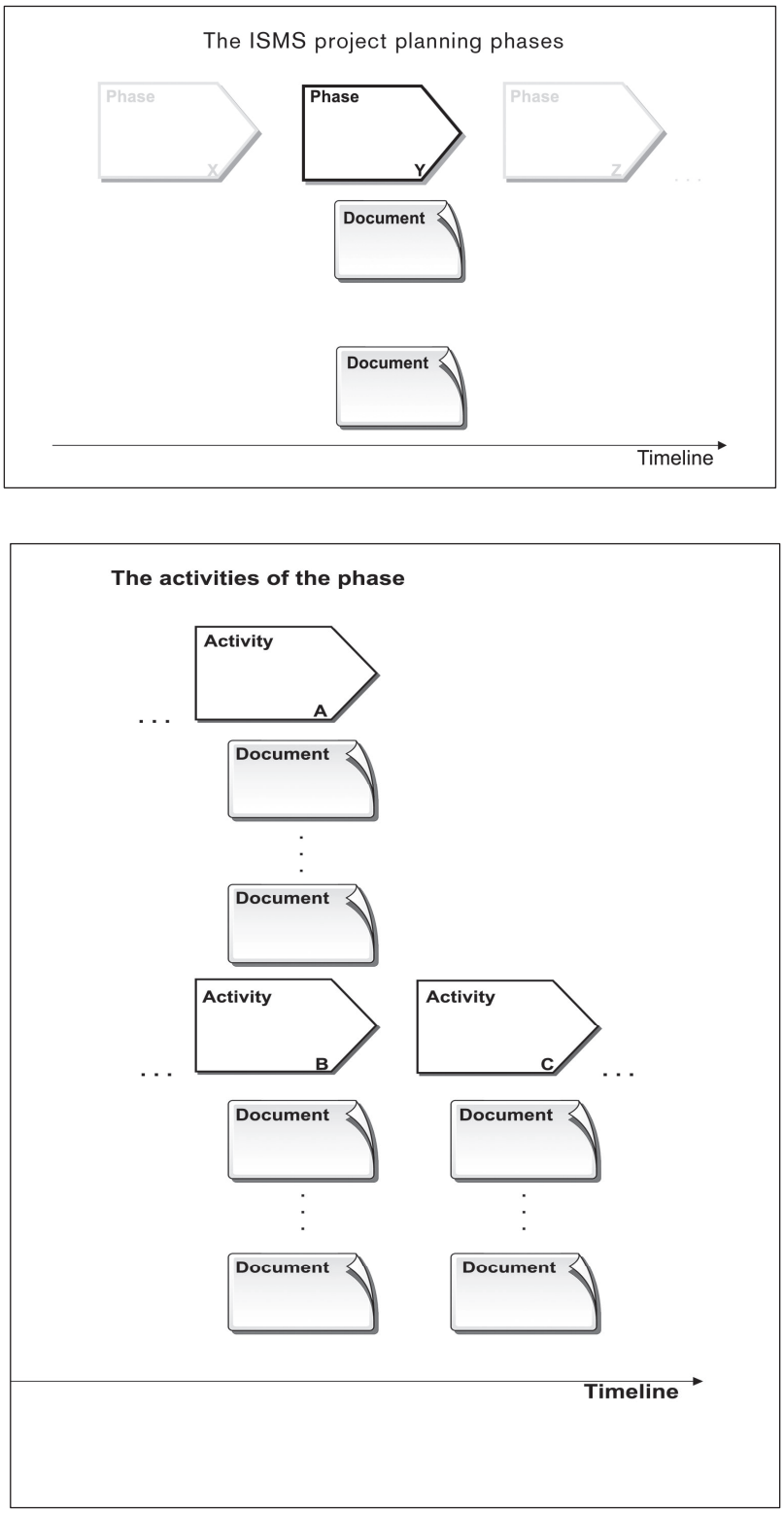

Figure 2 — Flow diagram legend

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

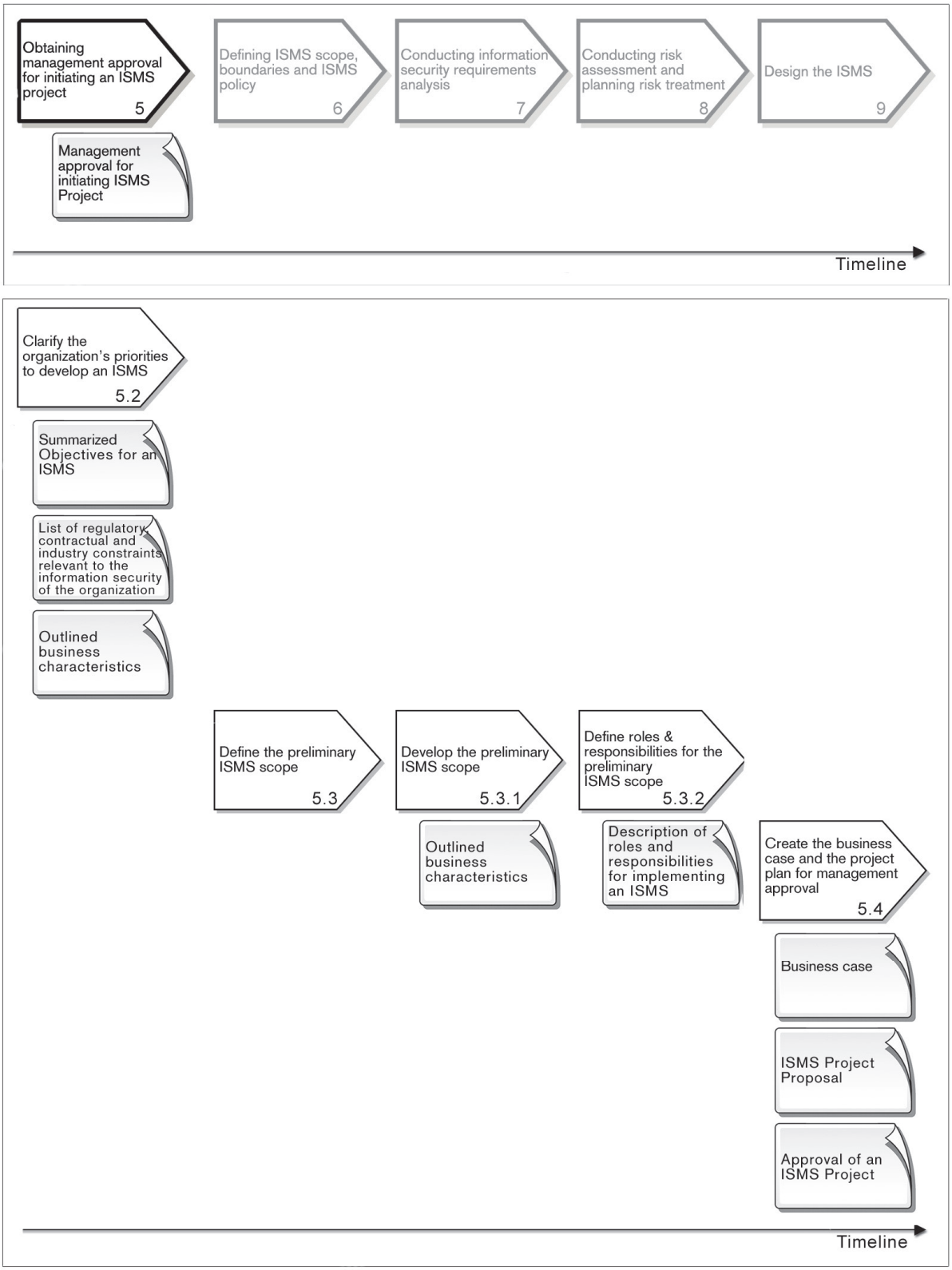

Figure 3 — Overview of obtaining management approval for initiating an ISMS project

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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)?

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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

Documents
Document Sharing Hub
© ISO/IEC 2010 – All rights reserved
Full document details: BS ISO/IEC 27003:2010

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.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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)

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

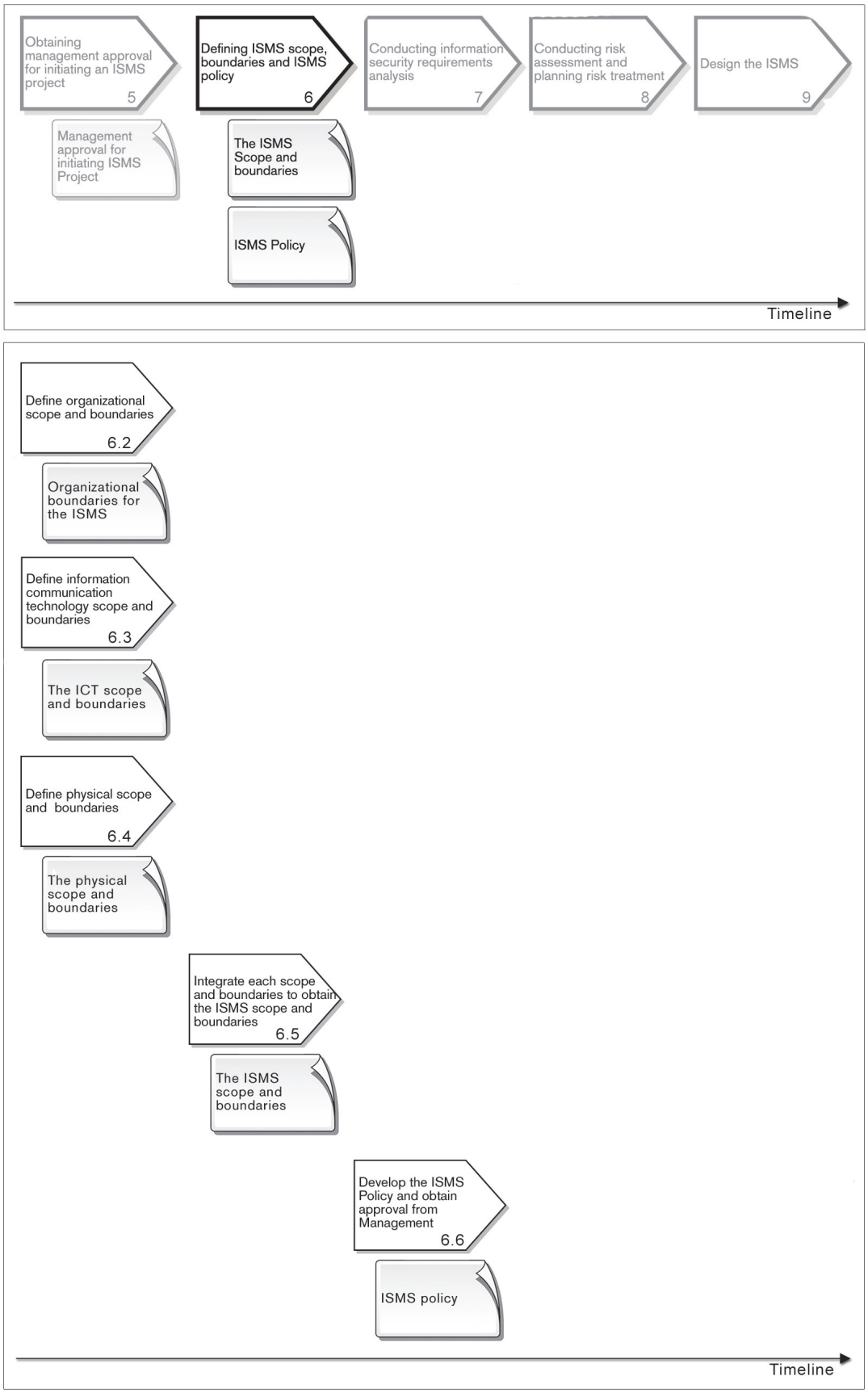

Figure 4 — Overview of defining ISMS scope, boundaries and ISMS policy

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010

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

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27003:2010