

# 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/IEC 2010

## 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/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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword .....	iv
Introduction.....	v
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>1</b>
<b>4 Structure of this International Standard .....</b>	<b>2</b>
<b>4.1 General structure of clauses .....</b>	<b>2</b>
<b>4.2 General structure of a clause .....</b>	<b>3</b>
<b>4.3 Diagrams .....</b>	<b>3</b>
<b>5 Obtaining management approval for initiating an ISMS project .....</b>	<b>5</b>
<b>5.1 Overview of obtaining management approval for initiating an ISMS project .....</b>	<b>5</b>
<b>5.2 Clarify the organization’s priorities to develop an ISMS.....</b>	<b>7</b>
<b>5.3 Define the preliminary ISMS scope .....</b>	<b>9</b>
<b>5.4 Create the business case and the project plan for management approval.....</b>	<b>11</b>
<b>6 Defining ISMS scope, boundaries and ISMS policy.....</b>	<b>12</b>
<b>6.1 Overview of defining ISMS scope, boundaries and ISMS policy .....</b>	<b>12</b>
<b>6.2 Define organizational scope and boundaries.....</b>	<b>15</b>
<b>6.3 Define information communication technology (ICT) scope and boundaries .....</b>	<b>16</b>
<b>6.4 Define physical scope and boundaries.....</b>	<b>17</b>
<b>6.5 Integrate each scope and boundaries to obtain the ISMS scope and boundaries.....</b>	<b>18</b>
<b>6.6 Develop the ISMS policy and obtain approval from management .....</b>	<b>19</b>
<b>7 Conducting information security requirements analysis.....</b>	<b>20</b>
<b>7.1 Overview of conducting information security requirements analysis.....</b>	<b>20</b>
<b>7.2 Define information security requirements for the ISMS process .....</b>	<b>22</b>
<b>7.3 Identify assets within the ISMS scope .....</b>	<b>23</b>
<b>7.4 Conduct an information security assessment .....</b>	<b>24</b>
<b>8 Conducting risk assessment and planning risk treatment.....</b>	<b>25</b>
<b>8.1 Overview of conducting risk assessment and planning risk treatment .....</b>	<b>25</b>
<b>8.2 Conduct risk assessment.....</b>	<b>27</b>
<b>8.3 Select the control objectives and controls .....</b>	<b>28</b>
<b>8.4 Obtain management authorization for implementing and operating an ISMS.....</b>	<b>29</b>
<b>9 Designing the ISMS .....</b>	<b>30</b>
<b>9.1 Overview of designing the ISMS.....</b>	<b>30</b>
<b>9.2 Design organizational information security .....</b>	<b>33</b>
<b>9.3 Design ICT and physical information security .....</b>	<b>38</b>
<b>9.4 Design ISMS specific information security.....</b>	<b>40</b>
<b>9.5 Produce the final ISMS project plan .....</b>	<b>44</b>
<b>Annex A (informative) Checklist description .....</b>	<b>45</b>
<b>Annex B (informative) Roles and responsibilities for Information Security .....</b>	<b>51</b>
<b>Annex C (informative) Information about Internal Auditing .....</b>	<b>55</b>
<b>Annex D (informative) Structure of policies .....</b>	<b>57</b>
<b>Annex E (informative) Monitoring and measuring.....</b>	<b>62</b>
<b>Bibliography.....</b>	<b>68</b>

## ISO/IEC 27003:2010(E)

### 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.

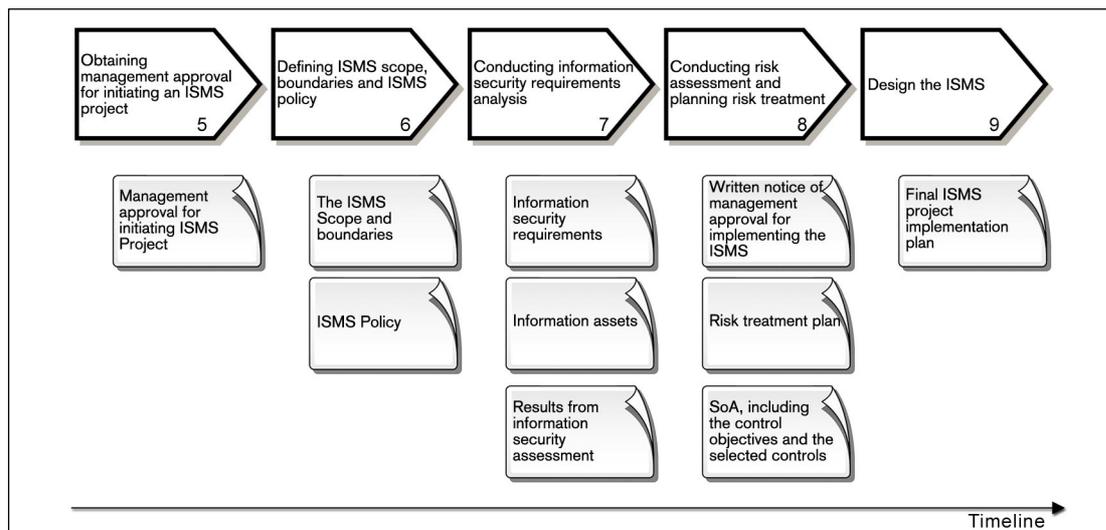


Figure 1 — ISMS project phases

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.

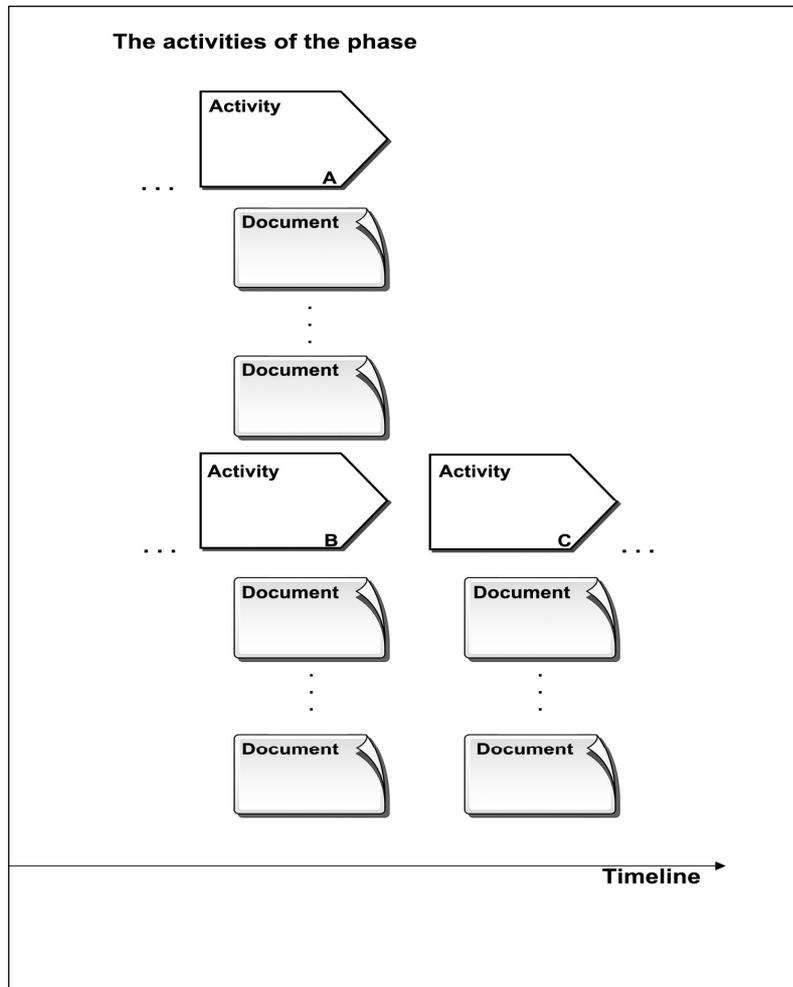
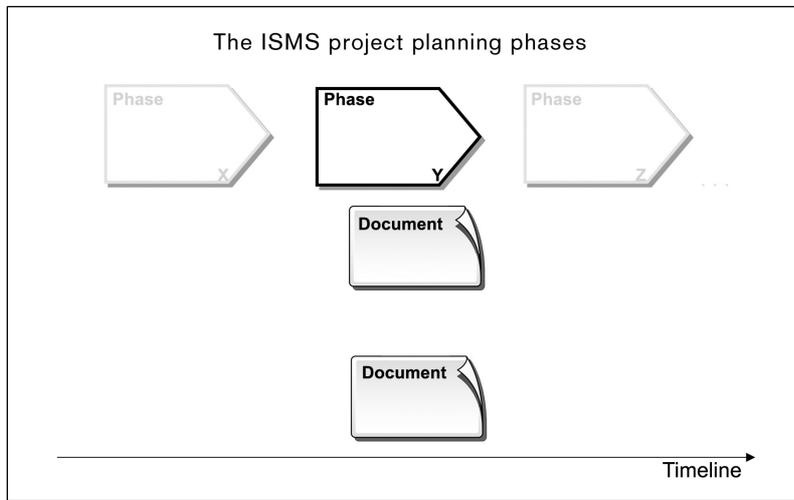


Figure 2 — Flow diagram legend

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.