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

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.

This document is a preview generated by EVS



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

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

This document is a preview generated by EVS

© ISO/IEC 2010 – All rights reserved

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*.

This document is a preview generated by EVS

 © ISO/IEC 2010 – All rights reserved

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).

This document is a preview generated by EVS

© ISO/IEC 2010 – All rights reserved

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

This document is a preview generated by EVS

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