

# American National Standard

INCITS/ISO/IEC 27003:2010[2012]

(ISO/IEC 27003:2010, IDT)

*Information technology - Security techniques -  
Information security management system  
implementation guidance*

**Developed by**



*Where IT all begins*



## INCITS/ISO/IEC 27003:2010[2012]

### 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.

**Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.**

Date of ANSI Approval: 8/22/2012

Published by American National Standards Institute,  
25 West 43rd Street, New York, New York 10036

Copyright 2012 by Information Technology Industry Council  
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.  
Printed in the United States of America

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)



This is a preview of "INCITS/ISO/IEC 27003...". [Click here to purchase the full version from the ANSI store.](#)

**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

This is a preview of "INCITS/ISO/IEC 27003...". Click here to purchase the full version from the ANSI store.

## 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>

## 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 is a preview of "INCITS/ISO/IEC 27003...". [Click here to purchase the full version from the ANSI store.](#)

## 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).