INTERNATIONAL STANDARD

ISO/IEC 27003

Second edition
2017-03

Information technology — Security techniques — Information security management systems — Guidance

Technologies de l'information — Techniques de sécurité --Systèmes de management de la sécurité de l'information — Lignes directrices

Reference number
ISO/IEC 27003:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Context of the organization ... **1**
4.1 Understanding the organization and its context ... 1
4.2 Understanding the needs and expectations of interested parties ... 3
4.3 Determining the scope of the information security management system ... 4
4.4 Information security management system ... 6

5 Leadership ... **6**
5.1 Leadership and commitment ... 6
5.2 Policy ... 8
5.3 Organizational roles, responsibilities and authorities ... 9

6 Planning ... **10**
6.1 Actions to address risks and opportunities ... 10
6.1.1 General ... 10
6.1.2 Information security risk assessment ... 12
6.1.3 Information security risk treatment ... 15
6.2 Information security objectives and planning to achieve them ... 18

7 Support ... **21**
7.1 Resources ... 21
7.2 Competence ... 22
7.3 Awareness ... 23
7.4 Communication ... 24
7.5 Documented information ... 25
7.5.1 General ... 25
7.5.2 Creating and updating ... 27
7.5.3 Control of documented information ... 28

8 Operation ... **29**
8.1 Operational planning and control ... 29
8.2 Information security risk assessment ... 31
8.3 Information security risk treatment ... 31

9 Performance evaluation ... **32**
9.1 Monitoring, measurement, analysis and evaluation ... 32
9.2 Internal audit ... 33
9.3 Management review ... 36

10 Improvement ... **37**
10.1 Nonconformity and corrective action ... 37
10.2 Continual improvement ... 40

Annex A (informative) **Policy framework** ... **42**

Bibliography ... **45**

© ISO/IEC 2017 – 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition of ISO/IEC 27003 cancels and replaces the first edition (ISO/IEC 27003:2010), of which it constitutes a minor revision.

The main changes compared to the previous edition are as follows:

— the scope and title have been changed to cover explanation of, and guidance on the requirements of, ISO/IEC 27001:2013 rather than the previous edition (ISO/IEC 27001:2005);

— the structure is now aligned to the structure of ISO/IEC 27001:2013 to make it easier for the user to use it together with ISO/IEC 27001:2013;

— the previous edition had a project approach with a sequence of activities. This edition instead provides guidance on the requirements regardless of the order in which they are implemented.

© ISO/IEC 2017 – All rights reserved

Introduction

This document provides guidance on the requirements for an information security management system (ISMS) as specified in ISO/IEC 27001 and provides recommendations ('should'), possibilities ('can') and permissions ('may') in relation to them. It is not the intention of this document to provide general guidance on all aspects of information security.

Clauses 4 to 10 of this document mirror the structure of ISO/IEC 27001:2013.

This document does not add any new requirements for an ISMS and its related terms and definitions. Organizations should refer to ISO/IEC 27001 and ISO/IEC 27000 for requirements and definitions. Organizations implementing an ISMS are under no obligation to observe the guidance in this document.

An ISMS emphasizes the importance of the following phases:

— understanding the organization's needs and the necessity for establishing information security policy and information security objectives;

— assessing the organization's risks related to information security;

— implementing and operating information security processes, controls and other measures to treat risks;

— monitoring and reviewing the performance and effectiveness of the ISMS; and

— practising continual improvement.

An ISMS, similar to any other type of management system, includes the following key components:

a) policy;

b) persons with defined responsibilities;

c) management processes related to:

   1) policy establishment;

   2) awareness and competence provision;

   3) planning;

   4) implementation;

   5) operation;

   6) performance assessment;

   7) management review; and

   8) improvement; and

d) documented information.

An ISMS has additional key components such as:

e) information security risk assessment; and

f) information security risk treatment, including determination and implementation of controls.

This document is generic and intended to be applicable to all organizations, regardless of type, size or nature. The organization should identify which part of this guidance applies to it in accordance with its specific organizational context (see ISO/IEC 27001:2013, Clause 4).

© ISO/IEC 2017 – All rights reserved

For example, some guidance can be more suited to large organizations, but for very small organizations (e.g. with fewer than 10 persons) some of the guidance can be unnecessary or inappropriate.

The descriptions of Clauses 4 to10 are structured as follows:

— **Required activity**: presents key activities required in the corresponding subclause of ISO/IEC 27001;

— **Explanation**: explains what the requirements of ISO/IEC 27001 imply;

— **Guidance**: provides more detailed or supportive information to implement "required activity" including examples for implementation; and

— **Other information**: provides further information that can be considered.

ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005 form a set of documents supporting and providing guidance on ISO/IEC 27001:2013. Among these documents, ISO/IEC 27003 is a basic and comprehensive document that provides guidance for all the requirements of ISO/IEC 27001, but it does not have detailed descriptions regarding "monitoring, measurement, analysis and evaluation" and information security risk management. ISO/IEC 27004 and ISO/IEC 27005 focus on specific contents and give more detailed guidance on "monitoring, measurement, analysis and evaluation" and information security risk management.

There are several explicit references to documented information in ISO/IEC 27001. Nevertheless, an organization can retain additional documented information that it determines as necessary for the effectiveness of its management system as part of its response to ISO/IEC 27001:2013, 7.5.1 b). In these cases, this document uses the phrase "Documented information on this activity and its outcome is mandatory only in the form and to the extent that the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b))."

© ISO/IEC 2017 – All rights reserved

Information technology — Security techniques — Information security management systems — Guidance

1 Scope

This document provides explanation and guidance on ISO/IEC 27001:2013.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *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 27000:2016 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

4 Context of the organization

4.1 Understanding the organization and its context

Required activity

The organization determines external and internal issues relevant to its purpose and affecting its ability to achieve the intended outcome(s) of the information security management system (ISMS).

Explanation

As an integral function of the ISMS, the organization continually analyses itself and the world surrounding it. This analysis is concerned with external and internal issues that in some way affect information security and how information security can be managed, and that are relevant to the organization's objectives.

Analysis of these issues has three purposes:

— understanding the context in order to decide the scope of the ISMS;

— analysing the context in order to determine risks and opportunities; and

— ensuring that the ISMS is adapted to changing external and internal issues.

© ISO/IEC 2017 – All rights reserved