
**Information technology — Security
techniques — Information security
management systems — Overview
and vocabulary**

*Technologies de l'information — Techniques de sécurité — Systèmes de
gestion de sécurité de l'information — Vue d'ensemble et vocabulaire*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, 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	v
0 Introduction	1
0.1 Overview	1
0.2 ISMS family of standards	1
0.3 Purpose of this International Standard	2
1 Scope	2
2 Terms and definitions	2
3 Information security management systems	14
3.1 General	14
3.2 What is an ISMS?	14
3.2.1 Overview and principles	14
3.2.2 Information	15
3.2.3 Information security	15
3.2.4 Management	15
3.2.5 Management system	16
3.3 Process approach	16
3.4 Why an ISMS is important	16
3.5 Establishing, monitoring, maintaining and improving an ISMS	17
3.5.1 Overview	17
3.5.2 Identifying information security requirements	17
3.5.3 Assessing information security risks	18
3.5.4 Treating information security risks	18
3.5.5 Selecting and implementing controls	18
3.5.6 Monitor, maintain and improve the effectiveness of the ISMS	19
3.5.7 Continual improvement	19
3.6 ISMS critical success factors	20
3.7 Benefits of the ISMS family of standards	20
4 ISMS family of standards	21
4.1 General information	21
4.2 Standards describing an overview and terminology	22
4.2.1 ISO/IEC 27000 (this International Standard)	22
4.3 Standards specifying requirements	22
4.3.1 ISO/IEC 27001	22
4.3.2 ISO/IEC 27006	22
4.4 Standards describing general guidelines	22
4.4.1 ISO/IEC 27002	22
4.4.2 ISO/IEC 27003	23
4.4.3 ISO/IEC 27004	23
4.4.4 ISO/IEC 27005	23
4.4.5 ISO/IEC 27007	23
4.4.6 ISO/IEC TR 27008	23
4.4.7 ISO/IEC 27013	24
4.4.8 ISO/IEC 27014	24
4.4.9 ISO/IEC TR 27016	24
4.5 Standards describing sector-specific guidelines	25
4.5.1 ISO/IEC 27010	25
4.5.2 ISO/IEC 27011	25
4.5.3 ISO/IEC TR 27015	25
4.5.4 ISO/IEC 27017	25
4.5.5 ISO/IEC 27018	26
4.5.6 ISO/IEC TR 27019	26
4.5.7 ISO 27799	26

Annex A (informative) **Verbal forms for the expression of provisions**.....28

Annex B (informative) **Term and term ownership**.....29

Bibliography33

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This fourth edition cancels and replaces the third edition (ISO/IEC 27000:2014), which has been technically revised.