

This is a preview of "BS ISO/IEC 27009:2016...". Click here to purchase the full version from the ANSI store.

BS ISO/IEC 27009:2016



BSI Standards Publication

Information technology — Security techniques — Sector- specific application of ISO/IEC 27001 — Requirements

bsi.

This is a preview of "BS ISO/IEC 27009:201...". [Click here to purchase the full version from the ANSI store.](#)

This British Standard is the UK implementation of ISO/IEC 27009:2016.

The UK participation in its preparation was entrusted to Technical Committee IST/33/1, Information Security Management Systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 83471 4

ICS 03.120.20; 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2016.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

This is a preview of "BS ISO/IEC 27009:201...". [Click here to purchase the full version from the ANSI store.](#)

First edition
2016-06-15

Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

Technologies de l'information — Techniques de sécurité — Application de l'ISO/IEC 27001 à un secteur spécifique — Exigences

Reference number
ISO/IEC 27009:2016(E)



© ISO/IEC 2016

This is a preview of "BS ISO/IEC 27009:201...". Click here to purchase the full version from the ANSI store.



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

This is a preview of "BS ISO/IEC 27009:201...". Click here to purchase the full version from the ANSI store.

Contents

	Page
Foreword	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview of this International Standard	1
4.1 General.....	1
4.2 Structure of this International Standard.....	2
4.3 Expanding ISO/IEC 27001 requirements or ISO/IEC 27002 controls.....	3
5 Additional, refined or interpreted ISO/IEC 27001 requirements	3
5.1 General.....	3
5.2 Additional requirements.....	3
5.3 Refined requirements.....	4
5.4 Interpreted requirements.....	4
6 Additional or modified ISO/IEC 27002 guidance	4
6.1 General.....	4
6.2 Additional guidance.....	4
6.3 Modified guidance.....	5
Annex A (normative) Template for developing sector-specific standards related to ISO/ IEC 27001:2013 or ISO/IEC 27002:2013	6
Bibliography	9

This is a preview of "BS ISO/IEC 27009:201...". Click here to purchase the full version from the ANSI store.

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 is a preview of "BS ISO/IEC 27009:201...". [Click here to purchase the full version from the ANSI store.](#)

Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

1 Scope

This International Standard defines the requirements for the use of ISO/IEC 27001 in any specific sector (field, application area or market sector). It explains how to include requirements additional to those in ISO/IEC 27001, how to refine any of the ISO/IEC 27001 requirements, and how to include controls or control sets in addition to ISO/IEC 27001:2013, Annex A.

This International Standard ensures that additional or refined requirements are not in conflict with the requirements in ISO/IEC 27001.

This International Standard is applicable to those involved in producing sector-specific standards that relate to ISO/IEC 27001.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1

interpretation

explanation (in form of requirement or guidance) of an ISO/IEC 27001 requirement in a sector-specific context which does not invalidate any of the ISO/IEC 27001 requirements

3.2

refinement

sector-specific specification of an ISO/IEC 27001 requirement which does not remove or invalidate any of the ISO/IEC 27001 requirements

4 Overview of this International Standard

4.1 General

ISO/IEC 27001 is an International Standard that defines the requirements for establishing, implementing, maintaining and continually improving an information security management system.