

Second edition
2020-04

Information security, cybersecurity and privacy protection — Sector- specific application of ISO/IEC 27001 — Requirements

*Sécurité de l'information, cybersécurité et protection des données
personnelles — Application de l'ISO/IEC 27001 à un secteur
spécifique — Exigences*



Reference number
ISO/IEC 27009:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

This is a preview of "ISO/IEC 27009:2020". 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 document | 2 |
| 4.1 General | 2 |
| 4.2 Structure of this document | 3 |
| 4.3 Expanding ISO/IEC 27001 requirements or ISO/IEC 27002 controls | 3 |
| 5 Addition to, refinement or interpretation of ISO/IEC 27001 requirements | 3 |
| 5.1 General | 3 |
| 5.2 Addition of requirements to ISO/IEC 27001 | 4 |
| 5.3 Refinement of requirements in ISO/IEC 27001 | 4 |
| 5.4 Interpretation of requirements in ISO/IEC 27001 | 4 |
| 6 Additional or modified ISO/IEC 27002 guidance | 4 |
| 6.1 General | 4 |
| 6.2 Additional guidance | 5 |
| 6.3 Modified guidance | 5 |
| Annex A (normative) Template for developing sector-specific standards related to ISO/IEC 27001 and optionally ISO/IEC 27002 | 6 |
| Annex B (normative) Template for developing sector-specific standards related to ISO/IEC 27002 | 9 |
| Annex C (informative) Explanation of the advantages and disadvantages of numbering approaches used within Annex B | 16 |
| Bibliography | 18 |

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 ISO documents 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27009:2016), which has been technically revised.

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

- the scope has been updated to more clearly reflect the content of this document;
- former Annex A has been divided into [Annexes A](#) and [B](#);
- [Annex C](#) has been created.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.