Belgian Standard

ISO/IEC 27009:2016

NBN ISO/IEC 27009:2016

Information technology - Security techniques — Sector-specific application of ISO/IEC 27001 - Requirements (ISO/IEC 27009:2016)

Valid from 21-12-2016

ICS: 03.100.70, 03.120.20, 35.030

Bureau for Standarisation
Rue Joseph II 40 PO box 6
1000 Brussels

T. +32 2 738 01 11
F. +32 2 733 42 64
info@nbn.be

BTW BE0880.857.592
IBAN BE69 6790 0009 5178
BIC Code PCHQBEBB

www.nbn.be

INTERNATIONAL STANDARD

ISO/IEC 27009

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)

COPYRIGHT PROTECTED DOCUMENT

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

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*.

INTERNATIONAL STANDARD **ISO/IEC 27009:2016(E)**

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.

