

MAURITIAN  
STANDARD

**MS ISO/IEC  
27009:2020**

First edition  
2020-10-17

---

---

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

ICS 35.030



**Mauritius Standards Bureau  
Moka**

## National foreword

This Mauritian Standard is identical with the International Standard **ISO/IEC 27009:2020 Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements** It was adopted by the Mauritius Standards Bureau on the recommendation of the **Information Technology Standards Committee**. The standard was approved by the **Standards Council** on **25 September 2020** and notified in the Government Gazette on **17 October 2020**.

\* General Notice No. 1484 of 2020



**COPYRIGHT PROTECTED DOCUMENT**

© MSB 2020

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 permission in writing from Mauritius Standards Bureau at the address below

*Mauritius Standards Bureau  
Villa Road  
Moka  
Mauritius*

*Telephone*           + (230) 433 3648  
*Fax*                    + (230) 433 5051/ 433 5150  
*E-mail*                [msb@intnet.mu](mailto:msb@intnet.mu)

# Contents

	Page
Foreword .....	iv
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>1</b>
<b>4 Overview of this document .....</b>	<b>2</b>
4.1 General .....	2
4.2 Structure of this document .....	3
4.3 Expanding ISO/IEC 27001 requirements or ISO/IEC 27002 controls .....	3
<b>5 Addition to, refinement or interpretation of ISO/IEC 27001 requirements .....</b>	<b>3</b>
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
<b>6 Additional or modified ISO/IEC 27002 guidance .....</b>	<b>4</b>
6.1 General .....	4
6.2 Additional guidance .....	5
6.3 Modified guidance .....	5
<b>Annex A (normative) Template for developing sector-specific standards related to ISO/IEC 27001 and optionally ISO/IEC 27002 .....</b>	<b>6</b>
<b>Annex B (normative) Template for developing sector-specific standards related to ISO/IEC 27002 .....</b>	<b>9</b>
<b>Annex C (informative) Explanation of the advantages and disadvantages of numbering approaches used within <a href="#">Annex B</a> .....</b>	<b>16</b>
<b>Bibliography .....</b>	<b>18</b>

## 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](http://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](http://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](http://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](http://www.iso.org/members.html).

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

## 1 Scope

This document specifies the requirements for creating sector-specific standards that extend ISO/IEC 27001, and complement or amend ISO/IEC 27002 to support a specific sector (domain, application area or market).

This document explains how to:

- include requirements in addition to those in ISO/IEC 27001,
- refine or interpret any of the ISO/IEC 27001 requirements,
- include controls in addition to those of ISO/IEC 27001:2013, Annex A and ISO/IEC 27002,
- modify any of the controls of ISO/IEC 27001:2013, Annex A and ISO/IEC 27002,
- add guidance to or modify the guidance of ISO/IEC 27002.

This document specifies that additional or refined requirements do not invalidate the requirements in ISO/IEC 27001.

This document is applicable to those involved in producing sector-specific standards.

## 2 Normative references

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

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002, *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.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>