



Institut luxembourgeois de la normalisation  
de l'accréditation, de la sécurité et qualité  
des produits et services

## ILNAS-EN ISO/IEC 27001:2023

### **Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)**

Sécurité de l'information, cybersécurité  
et protection de la vie privée - Systèmes  
de management de la sécurité de  
l'information - Exigences (ISO/IEC

Informationssicherheit, Cybersicherheit  
und Datenschutz -  
Informationssicherheitsmanagementsyst  
eme - Anforderungen (ISO/IEC

07/2023



## National Foreword

This European Standard EN ISO/IEC 27001:2023 was adopted as Luxembourgish Standard ILNAS-EN ISO/IEC 27001:2023.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

### **THIS PUBLICATION IS COPYRIGHT PROTECTED**

Nothing from this publication may be reproduced or utilized in any form or by any mean - electronic, mechanical, photocopying or any other data carries without prior permission!

ILNAS-EN ISO/IEC 27001:2023

EUROPEAN STANDARD **EN ISO/IEC 27001**

NORME EUROPÉENNE

EUROPÄISCHE NORM

July 2023

ICS 03.100.70; 35.030

Supersedes EN ISO/IEC 27001:2017

English version

**Information security, cybersecurity and privacy protection**  
**- Information security management systems -**  
**Requirements (ISO/IEC 27001:2022)**

Sécurité de l'information, cybersécurité et protection  
de la vie privée - Systèmes de management de la  
sécurité de l'information - Exigences (ISO/IEC  
27001:2022)

Informationssicherheit, Cybersicherheit und  
Datenschutz -  
Informationssicherheitsmanagementsysteme -  
Anforderungen (ISO/IEC 27001:2022)

This European Standard was approved by CEN on 23 July 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



**CEN-CENELEC Management Centre:**  
**Rue de la Science 23, B-1040 Brussels**

Contents	Page
European foreword.....	3

## European foreword

The text of ISO/IEC 27001:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27001:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2024, and conflicting national standards shall be withdrawn at the latest by January 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27001:2017.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

## Endorsement notice

The text of ISO/IEC 27001:2022 has been approved by CEN-CENELEC as EN ISO/IEC 27001:2023 without any modification.

# INTERNATIONAL STANDARD

# ISO/IEC 27001

Third edition  
2022-10

---

---

## Information security, cybersecurity and privacy protection — Information security management systems — Requirements

*Sécurité de l'information, cybersécurité et protection de la vie  
privée — Systèmes de management de la sécurité de l'information —  
Exigences*



Reference number  
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2022

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  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>iv</b>
<b>Introduction</b>	<b>v</b>
<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 Context of the organization</b>	<b>1</b>
4.1 Understanding the organization and its context	1
4.2 Understanding the needs and expectations of interested parties	1
4.3 Determining the scope of the information security management system	2
4.4 Information security management system	2
<b>5 Leadership</b>	<b>2</b>
5.1 Leadership and commitment	2
5.2 Policy	3
5.3 Organizational roles, responsibilities and authorities	3
<b>6 Planning</b>	<b>3</b>
6.1 Actions to address risks and opportunities	3
6.1.1 General	3
6.1.2 Information security risk assessment	4
6.1.3 Information security risk treatment	4
6.2 Information security objectives and planning to achieve them	5
<b>7 Support</b>	<b>6</b>
7.1 Resources	6
7.2 Competence	6
7.3 Awareness	6
7.4 Communication	6
7.5 Documented information	6
7.5.1 General	6
7.5.2 Creating and updating	7
7.5.3 Control of documented information	7
<b>8 Operation</b>	<b>7</b>
8.1 Operational planning and control	7
8.2 Information security risk assessment	8
8.3 Information security risk treatment	8
<b>9 Performance evaluation</b>	<b>8</b>
9.1 Monitoring, measurement, analysis and evaluation	8
9.2 Internal audit	8
9.2.1 General	8
9.2.2 Internal audit programme	9
9.3 Management review	9
9.3.1 General	9
9.3.2 Management review inputs	9
9.3.3 Management review results	9
<b>10 Improvement</b>	<b>10</b>
10.1 Continual improvement	10
10.2 Nonconformity and corrective action	10
<b>Annex A (normative) Information security controls reference</b>	<b>11</b>
<b>Bibliography</b>	<b>19</b>