



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

## **ILNAS-EN ISO/IEC 27001:2017**

### **Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor**

Informationstechnik -  
Sicherheitsverfahren -  
Informationssicherheitsmanagementsyst  
eme - Anforderungen (ISO/IEC

Technologies de l'information -  
Techniques de sécurité - Systèmes de  
management de la sécurité de  
l'information - Exigences (ISO/IEC

**02/2017**



## National Foreword

This European Standard EN ISO/IEC 27001:2017 was adopted as Luxembourgish Standard ILNAS-EN ISO/IEC 27001:2017.

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!

ICS 03.100.70; 35.030

English Version

**Information technology - Security techniques -  
Information security management systems - Requirements  
(ISO/IEC 27001:2013 including Cor 1:2014 and Cor  
2:2015)**

Technologies de l'information - Techniques de sécurité  
- Systèmes de management de la sécurité de  
l'information - Exigences (ISO/IEC 27001:2013 y  
compris Cor 1:2014 et Cor 2:2015)

Informationstechnik - Sicherheitsverfahren -  
Informationssicherheits-Managementsysteme -  
Anforderungen (ISO/IEC 27001:2013 einschließlich  
Cor 1:2014 und Cor 2:2015)

This European Standard was approved by CEN on 26 January 2017.

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 of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

**CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels**

Contents	Page
European foreword.....	3

## European foreword

The text of ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015 has been prepared by Technical Committee ISO/IEC JTC 1 “Information technology” of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27001:2017.

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 August 2017, and conflicting national standards shall be withdrawn at the latest by August 2017.

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

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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

## Endorsement notice

The text of ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015 has been approved by CEN as EN ISO/IEC 27001:2017 without any modification.

---

---

## **Information technology — Security techniques — Information security management systems — Requirements**

*Technologies de l'information — Techniques de sécurité — Systèmes  
de management de la sécurité de l'information — Exigences*



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2013

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  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>iv</b>
<b>0 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	1
4.4 Information security management system	2
<b>5 Leadership</b>	<b>2</b>
5.1 Leadership and commitment	2
5.2 Policy	2
5.3 Organizational roles, responsibilities and authorities	3
<b>6 Planning</b>	<b>3</b>
6.1 Actions to address risks and opportunities	3
6.2 Information security objectives and planning to achieve them	5
<b>7 Support</b>	<b>5</b>
7.1 Resources	5
7.2 Competence	5
7.3 Awareness	5
7.4 Communication	6
7.5 Documented information	6
<b>8 Operation</b>	<b>7</b>
8.1 Operational planning and control	7
8.2 Information security risk assessment	7
8.3 Information security risk treatment	7
<b>9 Performance evaluation</b>	<b>7</b>
9.1 Monitoring, measurement, analysis and evaluation	7
9.2 Internal audit	8
9.3 Management review	8
<b>10 Improvement</b>	<b>9</b>
10.1 Nonconformity and corrective action	9
10.2 Continual improvement	9
<b>Annex A (normative) Reference control objectives and controls</b>	<b>10</b>
<b>Bibliography</b>	<b>23</b>