

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

ILNAS-EN ISO/IEC 27006:2020

Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management

Technologies de l'information -Techniques de sécurité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de

Informationstechnik - IT-Sicherheitsverfahren - Anforderungen an Institutionen, die Audits und Zertifizierungen von

01011010010 0011010010110100101010101111

National Foreword

This European Standard EN ISO/IEC 27006:2020 was adopted as Luxembourgish Standard ILNAS-EN ISO/IEC 27006:2020.

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!

EUROPEAN STANDARD EN ISO/IEC 27006:2020 ISO/IEC 27006

NORME EUROPÉENNE

EUROPÄISCHE NORM

November 2020

ICS 03.120.20; 35.030

English version

Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems (ISO/IEC 27006:2015, including Amd 1:2020)

Technologies de l'information - Techniques de sécurité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information (ISO/IEC 27006:2015, y compris Amd 1:2020)

Informationstechnik - IT-Sicherheitsverfahren -Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managmentsystemen anbieten (ISO/IEC 27006:2015, einschließlich Amd 1:2020)

This European Standard was approved by CEN on 16 November 2020.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 24 February 2021.

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, Turkey and United Kingdom.





Contents	Page
European foreword	

European foreword

The text of ISO/IEC 27006:2015, including Amd 1:2020, 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 27006:2020 by Technical Committee CEN/CLC/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 May 2021, and conflicting national standards shall be withdrawn at the latest by May 2021.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN 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, 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, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27006:2015, including Amd 1:2020, has been approved by CEN as EN ISO/IEC 27006:2020 without any modification.

ILNINGTER PATIONAL STANDARD

ISO/IEC 27006

Third edition 2015-10-01

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

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 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		
Fore	eword		v	
Intr	oductio	n	vi	
1	Scon	e	1	
	-			
2		Normative references		
3	Tern	Terms and definitions		
4	Prin	ciples	1	
5	Gene	eral requirements	2	
	5.1	Legal and contractual matters		
	5.2	Management of impartiality		
		5.2.1 IS 5.2 Conflicts of interest		
	5.3	Liability and financing	2	
6	Stru	ctural requirements	2	
7	Reso	ource requirements	2	
	7.1	Competence of personnel		
		7.1.1 IS 7.1.1 General considerations		
		7.1.2 IS 7.1.2 Determination of Competence Criteria		
	7.2	Personnel involved in the certification activities		
	7.2	7.2.1 IS 7.2 Demonstration of auditor knowledge and experience		
	7.3	Use of individual external auditors and external technical experts	/	
		audit team	7	
	7.4	Personnel records		
	7.5	Outsourcing		
8	Info	mation requirements	8	
Ū	8.1	Public information		
	8.2	Certification documents		
		8.2.1 IS 8.2 ISMS Certification documents		
	8.3	Reference to certification and use of marks		
	8.4	Confidentiality		
	8.5	8.4.1 IS 8.4 Access to organizational records Information exchange between a certification body and its clients	 Ω	
9		ess requirements		
	9.1	Pre-certification activities 9.1.1 Application	_	
		9.1.2 Application review		
		9.1.3 Audit programme		
		9.1.4 Determining audit time		
		9.1.5 Multi-site sampling		
		9.1.6 Multiple management systems		
	9.2	Planning audits		
		9.2.1 Determining audit objectives, scope and criteria		
		9.2.2 Audit team selection and assignments 9.2.3 Audit plan		
	9.3	Initial certification		
	2.0	9.3.1 IS 9.3.1 Initial certification audit		
	9.4	Conducting audits		
		9.4.1 IS 9.4 General		
		9.4.2 IS 9.4 Specific elements of the ISMS audit		
	9.5	9.4.3 IS 9.4 Audit report		
	9.5	Certification decision		
		/1012 10 /10 UCI 01110U01011 UCC1010111		