

ISO/IEC 27011:2016



EN ISO/IEC 27011:2020

NBN EN ISO/IEC 27011:2020



**Information technology - Security techniques - Code of practice
for Information security controls based on ISO/IEC 27002 for
telecommunications organizations (ISO/IEC 27011:2016)**

Valid from 25-06-2020

Replaces NBN ISO/IEC 27011:2017

ICS: 03.100.70, 35.030

EUROPEAN STANDARD

EN ISO/IEC 27011

NORME EUROPÉENNE

EUROPÄISCHE NORM

May 2020

ICS 03.100.70; 35.030

English version

Information technology - Security techniques - Code of
practice for Information security controls based on
ISO/IEC 27002 for telecommunications organizations
(ISO/IEC 27011:2016)

Technologies de l'information - Techniques de sécurité
- Code de bonne pratique pour les contrôles de la
sécurité de l'information fondés sur l'ISO/IEC 27002
pour les organismes de télécommunications (ISO/IEC
27011:2016)

Informationstechnik - Sicherheitsverfahren - Leitfaden
für Informationssicherheitsmaßnahmen auf Grundlage
von ISO/IEC 27002 für
Telekommunikationsorganisatione (ISO/IEC
27011:2016)

This European Standard was approved by CEN on 3 May 2020.

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.



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

EN ISO/IEC 27011:2020 (E)

Contents

Page

European foreword..... 3

European foreword

The text of ISO/IEC 27011:2016 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 27011:2020 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 November 2020, and conflicting national standards shall be withdrawn at the latest by November 2020.

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 27011:2016 has been approved by CEN as EN ISO/IEC 27011:2020 without any modification.

INTERNATIONAL STANDARD

ISO/IEC 27011

Second edition
2016-12-01

Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

*Technologies de l'information — Techniques de sécurité — Code de
bonne pratique pour les contrôles de la sécurité de l'information fondés
sur l'ISO/IEC 27002 pour les organismes de télécommunications*

Reference number
ISO/IEC 27011:2016(E)



ISO/IEC 27011:2016(E)



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing 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
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

This second edition cancels and replaces first edition of ISO/IEC 27011:2008 which has been technically revised.

ISO/IEC 27011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as Rec. ITU-T X.1051.

CONTENTS

	<i>Page</i>	
1	Scope	1
2	Normative references.....	1
3	Definitions and abbreviations	1
	3.1 Definitions.....	1
	3.2 Abbreviations	2
4	Overview	2
	4.1 Structure of this Recommendation International Standard.....	2
	4.2 Information security management systems in telecommunications organizations.....	3
5	Information security policies	5
6	Organization of information security.....	5
	6.1 Internal organization	5
	6.2 Mobile devices and teleworking.....	6
7	Human resource security	6
	7.1 Prior to employment.....	6
	7.2 During employment	7
	7.3 Termination or change of employment	7
8	Asset management.....	7
	8.1 Responsibility for assets.....	7
	8.2 Information classification.....	8
	8.3 Media handling.....	8
9	Access control	8
	9.1 Business requirement for access control	8
	9.2 User access management.....	9
	9.3 User responsibilities	9
	9.4 System and application access control	9
10	Cryptography.....	9
11	Physical and environmental security	9
	11.1 Secure areas.....	9
	11.2 Equipment	10
12	Operations security.....	12
	12.1 Operational procedures and responsibilities.....	12
	12.2 Protection from malware.....	13
	12.3 Backup	13
	12.4 Logging and monitoring.....	13
	12.5 Control of operational software.....	13
	12.6 Technical vulnerability management	14
	12.7 Information systems audit considerations	14
13	Communications security	14
	13.1 Network security management.....	14
	13.2 Information transfer.....	15
14	System acquisition, development and maintenance	16
	14.1 Security requirements of information systems	16
	14.2 Security in development and support processes	16
	14.3 Test data	16
15	Supplier relationships	16
	15.1 Information security in supplier relationships.....	16
	15.2 Supplier service delivery management.....	17
16	Information security incident management	17
	16.1 Management of information security incidents and improvements.....	17
17	Information security aspects of business continuity management.....	19

	<i>Page</i>
17.1 Information security continuity	19
17.2 Redundancies	20
18 Compliance.....	20
Annex A – Telecommunications extended control set	21
Annex B – Additional guidance for network security	29
B.1 Security measures against network attacks	29
B.2 Network security measures for network congestion.....	30
Bibliography	31

Introduction

This Recommendation | International Standard provides interpretation guidelines for the implementation and management of information security controls in telecommunications organizations based on ISO/IEC 27002.

Telecommunications organizations provide telecommunications services by facilitating the communications of customers through their infrastructure. In order to provide telecommunications services, telecommunications organizations need to interconnect and/or share their services and facilities and/or use the services and facilities of other telecommunications organizations. Furthermore, the site location, such as radio sites, antenna locations, ground cables and utility provision (power, water), may be accessed not only by the organization's staff, but also by contractors and providers external to the organization.

Therefore, the management of information security in telecommunications organizations is complex, potentially:

- depending on external parties;
- having to cover all areas of network infrastructure, services applications and other facilities;
- including a range of telecommunications technologies (e.g., wired, wireless or broadband);
- supporting a wide range of operational scales, service areas and service types.

In addition to the application of security objectives and controls described in ISO/IEC 27002, telecommunications organizations may need to implement extra controls to ensure confidentiality, integrity, availability and any other security property of telecommunications in order to manage security risk in an adequate fashion.

1) *Confidentiality*

Protecting confidentiality of information related to telecommunications from unauthorized disclosure. This implies non-disclosure of communications in terms of the existence, the content, the source, the destination and the date and time of communicated information.

It is critical that telecommunications organizations ensure that the non-disclosure of communications being handled by them is not breached. This includes ensuring that persons engaged by the telecommunications organization maintain the confidentiality of any information regarding others that may have come to be known during their work duties.

NOTE – The term "secrecy of communications" is used in some countries in the context of "non-disclosure of communications".

2) *Integrity*

Protecting the integrity of telecommunications information includes controlling the installation and use of telecommunications facilities to ensure the authenticity, accuracy and completeness of information transmitted, relayed or received by wire, radio or any other method.

3) *Availability*

Availability of telecommunications information includes ensuring that access to facilities and the medium used for the provision of communication services is authorized, regardless of whether communications is provided by wire, radio or any other method. Typically, telecommunications organizations give priority to essential communications in case of emergencies, managing unavailability of less important communications in compliance with regulatory requirements.

Audience

The audience of this Recommendation | International Standard consists of telecommunications organizations and those responsible for information security; together with security vendors, auditors, telecommunications terminal vendors and application content providers. This Recommendation | International Standard provides a common set of general security control objectives based on ISO/IEC 27002, telecommunications sector-specific controls and information security management guidelines allowing for the selection and implementation of such controls.

INTERNATIONAL STANDARD ITU-T RECOMMENDATION

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

1 Scope

The scope of this Recommendation | International Standard is to define guidelines supporting the implementation of information security controls in telecommunications organizations.

The adoption of this Recommendation | International Standard will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

- ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this Recommendation | International Standard, the definitions given in ISO/IEC 27000 and the following apply:

3.1.1 co-location: Installation of telecommunications facilities on the premises of other telecommunications carriers.

3.1.2 communication centre: Building where facilities for providing telecommunications business are sited.

3.1.3 essential communications: Communications whose contents are necessary for the prevention of or relief from disasters and for the maintenance of public order in adverse conditions.

3.1.4 non-disclosure of communications: Requirement not to disclose the existence, the content, the source, the destination and the date and time of communicated information.

3.1.5 priority call: Telecommunications made by specific terminals in the event of emergencies, which should be handled with priority by restricting public calls.

NOTE – The specific terminals may span different services (voice over Internet protocol (VoIP), public switched telephone network (PSTN) voice, Internet protocol (IP) data traffic, etc.) for wired and wireless networks.

3.1.6 telecommunications applications: Applications such as Voice over IP (VoIP) that are consumed by end-users and built upon the network based services.

3.1.7 telecommunications business: Business to provide telecommunications services in order to meet the demand of others.

3.1.8 telecommunications equipment room: A secure location or room within a general building where equipment for providing telecommunications business are sited.

3.1.9 telecommunications facilities: Machines, equipment, wire and cables, physical buildings or other electrical facilities for the operation of telecommunications.