

STN	Informačné technológie Bezpečnostné metódy Súbor postupov na opatrenia v informačnej bezpečnosti založené na ISO/IEC 27002 pre cloudové služby (ISO/IEC 27017: 2015)	STN EN ISO/IEC 27017 97 4112
------------	---	--

Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 07/21

Obsahuje: EN ISO/IEC 27017:2021, ISO/IEC 27017:2015

132563

EUROPEAN STANDARD

EN ISO/IEC 27017

NORME EUROPÉENNE

EUROPÄISCHE NORM

January 2021

ICS 35.030

English version

Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)

Technologies de l'information - Techniques de sécurité
- Code de pratique pour les contrôles de sécurité de
l'information fondés sur l'ISO/IEC 27002 pour les
services du nuage (ISO/IEC 27017:2015)

Informationstechnik - Sicherheitsverfahren -
Anwendungsleitfaden für
Informationssicherheitsmaßnahmen basierend auf
ISO/IEC 27002 für Cloud Dienste (ISO/IEC
27017:2015)

This European Standard was approved by CEN on 20 December 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 27017:2021 (E)

Contents	Page
European foreword.....	3

European foreword

The text of ISO/IEC 27017:2015 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 27017:2021 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 July 2021, and conflicting national standards shall be withdrawn at the latest by July 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 27017:2015 has been approved by CEN as EN ISO/IEC 27017:2021 without any modification.

INTERNATIONAL STANDARD

ISO/IEC 27017

First edition
2015-12-15

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

*Technologies de l'information — Techniques de sécurité — Code de
pratique pour les contrôles de sécurité de l'information fondés sur
l'ISO/IEC 27002 pour les services du nuage*

Reference number
ISO/IEC 27017:2015(E)



ISO/IEC 27017:2015(E)**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2015

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
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.

ISO/IEC 27017 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 ITU-T. X.1631 (07/2015).

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1631

(07/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security
design

**Information technology – Security techniques –
Code of practice for information security
controls based on ISO/IEC 27002 for cloud
services**

Recommendation ITU-T X.1631

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

**INTERNATIONAL STANDARD ISO/IEC 27017
RECOMMENDATION ITU-T X.1631****Information technology – Security techniques – Code of practice for information security
controls based on ISO/IEC 27002 for cloud services****Summary**

Recommendation ITU-T X.1631 | ISO/IEC 27017 provides guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1631	2015-07-14	17	11.1002/1000/12490

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2015

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	<i>Page</i>	
1	Scope	1
2	Normative references.....	1
2.1	Identical Recommendations International Standards	1
2.2	Additional References	1
3	Definitions and abbreviations	1
3.1	Terms defined elsewhere.....	1
3.2	Abbreviations	2
4	Cloud sector-specific concepts	2
4.1	Overview	2
4.2	Supplier relationships in cloud services	2
4.3	Relationships between cloud service customers and cloud service providers	3
4.4	Managing information security risks in cloud services	3
4.5	Structure of this standard.....	3
5	Information security policies	4
5.1	Management direction for information security	4
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	6
7.3	Termination and 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 requirements of access control	8
9.2	User access management.....	9
9.3	User responsibilities	10
9.4	System and application access control	10
10	Cryptography.....	11
10.1	Cryptographic controls.....	11
11	Physical and environmental security	12
11.1	Secure areas.....	12
11.2	Equipment	12
12	Operations security	13
12.1	Operational procedures and responsibilities.....	13
12.2	Protection from malware	14
12.3	Backup	14
12.4	Logging and monitoring.....	15
12.5	Control of operational software.....	16
12.6	Technical vulnerability management	16
12.7	Information systems audit considerations	17
13	Communications security	17
13.1	Network security management.....	17
13.2	Information transfer.....	17
14	System acquisition, development and maintenance	18
14.1	Security requirements of information systems	18
14.2	Security in development and support processes.....	18

	<i>Page</i>
14.3 Test data	19
15 Supplier relationships	19
15.1 Information security in supplier relationships	19
15.2 Supplier service delivery management.....	20
16 Information security incident management	20
16.1 Management of information security incidents and improvements.....	20
17 Information security aspects of business continuity management.....	22
17.1 Information security continuity	22
17.2 Redundancies	22
18 Compliance.....	22
18.1 Compliance with legal and contractual requirements.....	22
18.2 Information security reviews.....	23
Annex A – Cloud service extended control set.....	25
Annex B – References on information security risk related to cloud computing	29
Bibliography	30

Introduction

The guidelines contained within this Recommendation | International Standard are in addition to and complement the guidelines given in ISO/IEC 27002.

Specifically, this Recommendation | International Standard provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Some guidelines are for cloud service customers who implement the controls, and others are for cloud service providers to support the implementation of those controls. The selection of appropriate information security controls and the application of the implementation guidance provided, will depend on a risk assessment and any legal, contractual, regulatory or other cloud-sector specific information security requirements.

**INTERNATIONAL STANDARD
ITU-T RECOMMENDATION****Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services****1 Scope**

This Recommendation | International Standard gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

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.

2.1 Identical Recommendations | International Standards

- Recommendation ITU-T Y.3500 (in force) | ISO/IEC 17788: (in force), *Information technology – Cloud computing – Overview and vocabulary*.
- Recommendation ITU-T Y.3502 (in force) | ISO/IEC 17789: (in force), *Information technology – Cloud computing – Reference architecture*.

2.2 Additional References

- ISO/IEC 27000: (in force), *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*.

koniec náhľadu – text ďalej pokračuje v platenej verzii STN