



BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of EN ISO/IEC 27017:2021. It is identical to ISO/IEC 27017:2015. It supersedes BS ISO/IEC 27017:2015, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 14436 9

ICS 03.100.70; 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2015.

Amendments/corrigenda issued since publication

Date	Text affected
28 February 2021	This corrigendum renumbers BS ISO/IEC 27017:2015 as BS EN ISO/IEC 27017:2021

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

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.

**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*.

3 Definitions and abbreviations

3.1 Terms defined elsewhere

For the purposes of this Recommendation | International Standard, the terms and definitions given in ISO/IEC 27000, Rec. ITU-T Y.3500 | ISO/IEC 17788, Rec. ITU-T Y.3502 | ISO/IEC 17789 and the following definitions apply:

3.1.1 The following term is defined in ISO 19440:

- **capability**: Quality of being able to perform a given activity.

3.1.2 The following terms are defined in ISO/IEC 27040:

- **data breach**: Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed.
- **secure multi-tenancy**: Type of multi-tenancy that employs security controls to explicitly guard against data breaches and provides validation of these controls for proper governance.

NOTE 1 – Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than it would be in a dedicated, single-tenant environment.

NOTE 2 – In very secure environments, even the identity of the tenants is kept secret.

3.1.3 The following term is defined in ISO/IEC 17203:

- **virtual machine:** The complete environment that supports the execution of guest software.

NOTE – A virtual machine is a full encapsulation of the virtual hardware, virtual disks, and the metadata associated with it. Virtual machines allow multiplexing of the underlying physical machine through a software layer called a hypervisor.

3.2 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

IaaS	Infrastructure as a Service
PaaS	Platform as a Service
PII	Personally Identifiable Information
SaaS	Software as a Service
SLA	Service Level Agreement
VM	Virtual Machine

4 Cloud sector-specific concepts

4.1 Overview

The use of cloud computing has changed how organizations should assess and mitigate information security risks because of the significant changes in how computing resources are technically designed, operated and governed. This Recommendation | International Standard provides additional cloud-specific implementation guidance based on ISO/IEC 27002 and provides additional controls to address cloud-specific information security threats and risks considerations.

Users of this Recommendation | International Standard should refer to clauses 5 to 18 in ISO/IEC 27002 for controls, implementation guidance and other information. Because of the general applicability of ISO/IEC 27002, many of the controls, implementation guidance and other information apply to both the general and cloud computing contexts of an organization. For example, "6.1.2 Segregation of duties" of ISO/IEC 27002 provides a control that can be applied whether the organization is acting as a cloud service provider or not. Additionally, a cloud service customer can derive requirements for segregation of duties in the cloud environment from the same control, e.g., segregating the cloud service customers' cloud service administrators and cloud service users.

As an extension to ISO/IEC 27002, this Recommendation | International Standard further provides cloud service specific controls, implementation guidance and other information (see clause 4.5) that are intended to mitigate the risks that accompany the technical and operational features of cloud services (see Annex B). The cloud service customers and the cloud service providers can refer to ISO/IEC 27002 and this Recommendation | International Standard to select controls with the implementation guidance, and add other controls if necessary. This process can be done by performing an information security risk assessment and risk treatment in the organizational and business context where cloud services are used or provided (see clause 4.4).

4.2 Supplier relationships in cloud services

ISO/IEC 27002 clause 15 "Supplier relationships" provides controls, implementation guidance and other information for managing information security in supplier relationships. The provision and use of cloud services is a kind of supplier relationship, where the cloud service customer is an acquirer, and the cloud service provider is a supplier. Therefore, the clause applies to cloud service customers and cloud service providers.

Cloud service customers and cloud service providers can also form a supply chain. Suppose that a cloud service provider provides an infrastructure capabilities type service. In addition, another cloud service provider can provide an application capabilities type service. In this case, the second cloud service provider is a cloud service customer with respect to the first, and a cloud service provider with respect to the cloud service customer using its service. This example illustrates the case where this Recommendation | International Standard applies to an organization both as a cloud service customer and as a cloud service provider. Because cloud service customers and cloud service providers form a supply chain through the design and implementation of the cloud service(s), clause "15.1.3 Information and communication technology supply chain" of ISO/IEC 27002 applies.

The multi-part International Standard ISO/IEC 27036, "*Information security for supplier relationships*", provides detailed guidance on the information security in supplier relationships to the acquirer and supplier of products and services.

ISO/IEC 27036 Part 4 deals directly with the security of cloud services in supplier relationships. This standard is also applicable to cloud service customers as acquirers and cloud service providers as suppliers.

4.3 Relationships between cloud service customers and cloud service providers

In the cloud computing environment, cloud service customer data is stored, transmitted and processed by a cloud service. Therefore, a cloud service customer's business processes can depend upon the information security of the cloud service. Without sufficient control over the cloud service, the cloud service customer might need to take extra precautions with its information security practices.

Before entering into a supplier relationship, the cloud service customer needs to select a cloud service, taking into account the possible gaps between the cloud service customer's information security requirements and the information security capabilities offered by the service. Once a cloud service is selected, the cloud service customer should manage the use of the cloud service in such a way as to meet its information security requirements. In this relationship, the cloud service provider should provide the information and technical support that are necessary to meet the cloud service customer's information security requirements. When the information security controls provided by the cloud service provider are preset and cannot be changed by the cloud service customer, the cloud service customer may need to implement additional controls of its own to mitigate risks.

4.4 Managing information security risks in cloud services

Cloud service customers and cloud service providers should both have information security risk management processes in place. They are advised to refer to ISO/IEC 27001 for the requirements to conduct risk management in their information security management systems, and to refer to ISO/IEC 27005 for further guidance on information security risk management itself. ISO 31000, to which ISO/IEC 27001 and ISO/IEC 27005 conform, can also help general understanding of risk management.

In contrast to the general applicability of the information security risk management processes, cloud computing has its own types of risk sources, including threats and vulnerabilities, which are derived from its features, e.g., networking, scalability and elasticity of the system, resource sharing, self-service provisioning, administration on-demand, cross-jurisdictional service provisioning, and limited visibility into the implementation of controls. Annex B provides references that give information on these risk sources and associated risks in the provision and use of cloud services.

The controls and implementation guidance given in clauses 5 to 18 and Annex A of this Recommendation | International Standard address cloud computing specific risk sources and risks.

4.5 Structure of this standard

This Recommendation | International Standard is structured in a format similar to ISO/IEC 27002. This Recommendation | International Standard includes clauses 5 to 18 of ISO/IEC 27002 by stating the applicability of its texts at each clause and paragraph.

When objectives and controls specified in ISO/IEC 27002 are applicable without a need for any additional information, only a reference to ISO/IEC 27002 is provided.

When an objective with controls, or a control under an objective from ISO/IEC 27002, is needed in addition to those of ISO/IEC 27002, they are given in normative Annex A: Cloud service extended control set. When a control of ISO/IEC 27002 or Annex A of this Recommendation | International Standard needs additional cloud service specific implementation guidance related to the control, it is given under the subtitle "**Implementation guidance for cloud services**". The guidance is provided in one of the following two types:

Type 1 is used when there is separate guidance for the cloud service customer and the cloud service provider.

Type 2 is used when the guidance is the same for both the cloud service customer and the cloud service provider.

Type 1

Cloud service customer	Cloud service provider