International Standard

ISO/IEC 27017

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services

Sécurité de l'information, cybersécurité et protection de la vie privée — Contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Second edition
2026-07

Reference number
ISO/IEC 27017:2026(en)

Horizontal document

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **vi**

Introduction ..... **vii**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 2

4 Guidance for using this document **2**
4.1 Relation between this document and ISO/IEC 27002:2022 2
4.2 Structure of this document 3
4.3 Cloud computing specific concepts 3
4.3.1 Supplier relationships in cloud services 3
4.3.2 Relationships between CSCs and CSPs 3
4.3.3 Managing information security risks in cloud services 4

5 Cloud service specific guidance related to organizational controls **5**
5.1 Policies for information security 5
5.2 Information security roles and responsibilities 6
5.3 Segregation of duties 6
5.4 Management responsibilities 6
5.5 Contact with authorities 6
5.6 Contact with special interest groups 6
5.7 Threat intelligence 7
5.8 Information security in project management 7
5.9 Inventory of information and other associated assets 7
5.10 Acceptable use of information and other associated assets 7
5.11 Return of assets 8
5.12 Classification of information 8
5.13 Labelling of information 8
5.14 Information transfer 8
5.15 Access control 8
5.16 Identity management 8
5.17 Authentication information 9
5.18 Access rights 9
5.19 Information security in supplier relationships 9
5.20 Addressing information security within supplier agreements 10
5.21 Managing information security in the ICT supply chain 10
5.22 Monitoring, review and change management of supplier services 11
5.23 Information security for use of cloud services 11
5.24 Information security incident management planning and preparation 11
5.25 Assessment and decision on information security events 11
5.26 Response to information security incidents 12
5.27 Learning from information security incidents 12
5.28 Collection of evidence 12
5.29 Information security during disruption 12
5.30 ICT readiness for business continuity 12
5.31 Legal, statutory, regulatory and contractual requirements 13
5.32 Intellectual property rights 14
5.33 Protection of records 14
5.34 Privacy and protection of PII 14
5.35 Independent review of information security 14
5.36 Compliance with policies, rules and standards for information security 15
5.37 Documented operating procedures 15
5.38 CLD - Shared roles and responsibilities within a cloud computing environment 15

© ISO/IEC 2026 – All rights reserved

5.39 CLD - Agreement on the roles and responsibilities of the cloud service partner 16

6 Cloud service specific guidance related to people controls 17
6.1 Screening 17
6.2 Terms and conditions of employment 18
6.3 Information security awareness, education and training 18
6.4 Disciplinary process 18
6.5 Responsibilities after termination or change of employment 18
6.6 Confidentiality or non-disclosure agreements 18
6.7 Remote working 18
6.8 Information security event reporting 19

7 Cloud service specific guidance related to physical controls 19
7.1 Physical security perimeters 19
7.2 Physical entry 19
7.3 Securing offices, rooms and facilities 19
7.4 Physical security monitoring 19
7.5 Protecting against physical and environmental threats 19
7.6 Working in secure areas 19
7.7 Clear desk and clear screen 19
7.8 Equipment siting and protection 19
7.9 Security of assets off-premises 20
7.10 Storage media 20
7.11 Supporting utilities 20
7.12 Cabling security 20
7.13 Equipment maintenance 20
7.14 Secure disposal or re-use of equipment 20

8 Cloud service specific guidance related to technological controls 20
8.1 User endpoint devices 20
8.2 Privileged access rights 21
8.3 Information access restriction 21
8.4 Access to source code 21
8.5 Secure authentication 21
8.6 Capacity management 22
8.7 Protection against malware 22
8.8 Management of technical vulnerabilities 22
8.9 Configuration management 23
8.10 Information deletion 23
8.11 Data masking 24
8.12 Data leakage prevention 24
8.13 Information backup 24
8.14 Redundancy of information processing facilities 25
8.15 Logging 25
8.16 Monitoring activities 26
8.17 Clock synchronization 26
8.18 Use of privileged utility programs 27
8.19 Installation of software on operational systems 27
8.20 Network security 27
8.21 Security of network services 27
8.22 Segregation of networks 28
8.23 Web filtering 28
8.24 Use of cryptography 28
8.25 Secure development life cycle 28
8.26 Application security requirements 29
8.27 Secure system architecture and engineering principles 29
8.28 Secure coding 29
8.29 Security testing in development and acceptance 29
8.30 Outsourced development 29
8.31 Separation of development, test and production environments 29

© ISO/IEC 2026 – All rights reserved

8.32 Change management 29
8.33 Test information 30
8.34 Protection of information systems during audit and testing 30
8.35 CLD - Segregation in virtual computing environments 30
8.36 CLD - Detection and prevention of unauthorized use of cloud services 31

Annex A (Informative) **Correspondence between this document and the first edition (ISO/IEC 27017:2015)** **33**

Annex B (informative) **Monitoring of cloud services** **38**

Bibliography **39**

© ISO/IEC 2026 – All rights reserved

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with ITU-T (as Rec. ITU-T X.1631), and in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and Data Protection,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/IEC 27017:2015 | Rec. ITU-T X.1631:2015), which has been technically revised.

The main changes are as follows:

— the title and the scope have been modified;

— the structure of the document has been changed, presenting the controls using a simple taxonomy and associated attributes;

— some controls have been merged, some have been removed and several new controls have been introduced.

This document has been given the status of a horizontal document in accordance with the ISO/IEC Directives, Part 1.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Introduction

The guidance contained within this document is aligned with and complements the guidance given in ISO/IEC 27002.

Specifically, this document provides guidance supporting the implementation of information security controls for cloud service customers (CSCs) and cloud service providers (CSPs). Some guidance is intended for CSCs who implement the controls and other guidance is for CSPs to support the implementation of those controls. The determination of the appropriate information security controls and the extent of the utilization of the guidance provided depends on the results of the relevant risk assessment and the existence of any legal, regulatory, contractual, or other cloud-computing specific information security requirements.

© ISO/IEC 2026 – All rights reserved

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services

1 Scope

This document provides guidance for information security controls, based on ISO/IEC 27002, applicable to the provision and use of cloud services. This document provides:

— additional guidance for relevant controls specified in ISO/IEC 27002:2022;

— additional controls with guidance that specifically relate to cloud services.

This document provides controls and guidance for cloud service customers (CSCs) and cloud service providers (CSPs).

This document is considered to be a horizontal document as it provides a foundation and a common understanding of security regarding the provision and use of cloud services.

NOTE This document applies to all types of cloud deployment models including the private cloud. When applying this document to the private cloud, the controls and guidance of this document are applicable, although adjustments can be necessary to adapt to the relationships and abilities of an organization's internal departments.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22123-1, *Information technology — Cloud computing — Part 1: Vocabulary*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27002, ISO/IEC 22123-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1.1
capability
ability to perform a specific activity

[SOURCE: ISO 19440:2020, 3.5]

© ISO/IEC 2026 – All rights reserved

3.2 Abbreviated terms

API	application programming interface
CSC	cloud service customer
CSN	cloud service partner
CSP	cloud service provider
CSU	cloud service user
IaaS	infrastructure as a service
ICT	information and communication technology
PaaS	platform as a service
PII	personally identifiable information
RTO	recovery time objective
RPO	recovery point objective
SaaS	software as a service
SLA	service level agreement

4 Guidance for using this document

4.1 Relation between this document and ISO/IEC 27002:2022

This document provides:

— additional guidance for relevant controls specified in ISO/IEC 27002:2022;

— additional controls with guidance that specifically relate to cloud services.

This document refers to the attributes, controls, purposes, guidance and other information from ISO/IEC 27002:2022, Clauses 5 to 8. Owing to the general applicability of ISO/IEC 27002:2022, many of the controls, guidance and other information apply to both the general and cloud computing contexts of an organization. For example, ISO/IEC 27002:2022, 5.3, “Segregation of duties” provides a control that can be applied whether the organization is acting as a CSP or not. Additionally, a CSC can derive requirements for segregation of duties in the cloud computing environment from the same control, e.g. a CSC segregating the CSCs' cloud service administrators from other CSUs.

This document also provides attributes, controls, purposes, guidance and other information that are specific to cloud services and are intended to mitigate the risks that accompany the technical and operational features of cloud services (see 5.38, 5.39, 8.35 and 8.36). Annex A provides the mappings between the set of controls of this document and the previous edition (ISO/IEC 27017:2015[1)]).

The CSCs and the CSPs can refer to ISO/IEC 27002:2022 and this document to identify guidance on general and cloud service specific controls as 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 4.3.3).

1) Cancelled and replaced by this document (ISO/IEC 27017:2026).

© ISO/IEC 2026 – All rights reserved