International Standard

ISO/IEC 27017

Second edition
2026-07

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

Reference number
ISO/IEC 27017:2026(en)

Horizontal document

COPYRIGHT PROTECTED DOCUMENT

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

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.

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.

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]

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).

4.2 Structure of this document

This document follows the structure used in ISO/IEC 27002:2022 for the description of controls.

This document adapts the information security controls included in ISO/IEC 27002:2022, Clauses 5 to 8 to better fit cloud computing. As in ISO/IEC 27002:2022, the categorization of controls given in Clauses 5 to 8 is referred to as themes and the attributes of each control identified in ISO/IEC 27002:2022 also apply.

When controls specified in ISO/IEC 27002:2022 are applicable to both the CSCs and the CSP without a need for any additional information, only a reference to ISO/IEC 27002:2022 is provided.

In addition to the controls of ISO/IEC 27002:2022, cloud service extended controls are prefixed with "CLD" (CLouD service extended controls). When a control specified in ISO/IEC 27002:2022 needs additional guidance that is specific to cloud services related to the control, it is given as "guidance for cloud services". The guidance is provided in one of the following two types:

— Type 1 (shown in Table 1), used when there is separate guidance for the CSC and the CSP;

— Type 2 (shown in Table 2), used when the guidance is the same for both the CSC and the CSP.

Table 1 — Type 1

CSC	CSP
CSC guidance	CSP guidance

Table 2 — Type 2

CSC	CSP
CSC and CSP guidance	

4.3 Cloud computing specific concepts

4.3.1 Supplier relationships in cloud services

ISO/IEC 27002:2022, 5.19 to 5.22 provide controls, the purpose of each control, guidance and other information for managing information security in supplier relationships. The provision and use of cloud services is similar to a supplier relationship, where the CSC is an acquirer and the CSP is a supplier. Therefore, ISO/IEC 27002:2022, 5.19 to 5.22 apply to CSCs and CSPs.

CSCs and CSPs can also form a supply chain. For example, a CSP provides a cloud service of infrastructure capabilities type. On top of this service, another CSP can provide a cloud service of application capabilities type. In this case, the second CSP is a CSC with respect to the first, and a CSP with respect to the CSC using its service. In this scenario, the organization has both CSC and CSP roles. Every organization should consider which controls are applicable to it in its roles as the CSC and the CSP. This example illustrates the case where this document applies to an organization both as a CSC and as a CSP. Since CSCs and CSPs form a supply chain through the provision and use of the cloud service, ISO/IEC 27002:2022, 5.21 applies as it covers the management of information security in the ICT supply chain.

The ISO/IEC 27036 series provides detailed guidance on the information security in supplier relationships to the acquirer and supplier of products and services. ISO/IEC 27036-4 deals directly with information security of cloud services in supplier relationships. ISO/IEC 27036-4 is also applicable to CSCs as acquirers and CSPs as suppliers.

4.3.2 Relationships between CSCs and CSPs

In the cloud computing environment, CSC data are stored, transmitted and processed by a cloud service. Therefore, a CSC's business processes depend upon the information security of the cloud service. Without sufficient control over the cloud service, it can be necessary for the CSC to take extra precautions with its own information security practices.

Before entering into a supplier relationship, the CSC is expected to select a cloud service, taking into account the possible gaps between the CSC's information security requirements and the information security capabilities offered by the service. Once a cloud service is selected, the CSC should manage the use of the cloud service in such a way as to meet its own information security requirements. In this relationship, collaborative effort between the CSC and the CSP for the use and provision of the cloud service is necessary for the CSC to achieve its objectives for information security management. It includes shared roles and responsibilities between the CSC and the CSP. The CSP should provide the information and technical support that are necessary to meet the CSC's information security requirements. When the information security controls provided by the CSP are pre-set and cannot be changed by the CSC, it is possible that the CSC implements additional controls of its own to mitigate risks. More information on allocation of the shared roles and responsibilities can be found in 5.38.

It is important to understand that there are different cloud deployment models that are used in cloud computing environments. Some of the cloud deployment models include:

— private cloud;

— public cloud;

— multi-cloud;

— federated cloud;

— hybrid cloud;

— hybrid multi-cloud;

— inter-cloud.

There are three fundamental approaches that can be taken in these different cloud deployment models.

— The CSC controls and manages the cloud services that are being delivered by each of the CSPs including their orchestration into a cloud solution (e.g. multi-cloud).

— One CSP combines cloud services from multiple CSPs with varying degrees of orchestration, control and management activities (e.g. inter-cloud).

— Multiple CSPs form a partnership through out-of-band collaboration and share their resources to create cloud services (e.g. federated cloud which uses a cloud service federation management system to orchestrate access to the CSPs resources).

It is important to note that these approaches are not mutually exclusive and it is possible to combine them. Further explanation of these cloud deployment models can be found in ISO/IEC 5140.

4.3.3 Managing information security risks in cloud services

CSCs and CSPs should both have information security risk management processes in place. They can refer to ISO/IEC 27001 for the requirements related to risk management for information security management systems, and to ISO/IEC 27005 for further guidance on information security risk management itself. ISO 31000, to which ISO/IEC 27001 and ISO/IEC 27005 are aligned, can also help with a general understanding of risk management.

The controls and guidance provide CSCs with:

— guidance on information security measures relating to the use of cloud services;

— guidance on information and capabilities of the cloud services to be obtained from CSPs.

The controls and guidance also cover how CSPs can provide information and capabilities as a part of cloud services to support CSCs' information security risk management. The information and capabilities can be provided in agreements and other documents available for CSCs.