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

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*

Bibliography

[1] ISO/IEC 5140, *Information technology — Cloud computing — Concepts for multi-cloud and the use of multiple cloud services*

[2] ISO/IEC 19086 (all parts), *Cloud computing — Service level agreement (SLA) framework*

[3] ISO 19440:2020, *Enterprise modelling and architecture — Constructs for enterprise modelling*

[4] ISO/IEC 22123-3:2023, *Information technology — Cloud computing — Part 3: Reference architecture*

[5] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[6] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[7] ISO/IEC 27017:2015[2)], *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[8] ISO/IEC 27018, *Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[9] ISO/IEC 27036-1:2021, *Cybersecurity — Supplier relationships — Part 1: Overview and concepts*

[10] ISO/IEC 27036-2:2022, *Cybersecurity — Supplier relationships — Part 2: Requirements*

[11] ISO/IEC 27036-3:2023, *Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security*

[12] ISO/IEC 27036-4:2016, *Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services*

[13] ISO/IEC 27040, *Information technology — Security techniques — Storage security*

[14] ISO 31000, *Risk management — Guidelines*

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