SmartSuite

Framework / Cloud Security / ISO 27000 Series

ISO/IEC 27017:2026 Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27017:2026 gives cloud security control guidance for customers and providers, built on ISO/IEC 27002:2022, with four cloud-specific controls; it replaced the 2015 edition.



What it is

ISO/IEC 27017 is the international standard that gives information security control guidance for providing and using cloud services, based on ISO/IEC 27002 and addressed to both cloud service customers (CSCs) and cloud service providers (CSPs). The current edition is ISO/IEC 27017:2026, the second edition, published in July 2026 (ISO's publication stage was reached on July 27, 2026); it was prepared by ISO/IEC JTC 1/SC 27 in collaboration with ITU-T (as Rec. ITU-T X.1631) and cancels and replaces the 2015 first edition, which ISO withdrew on the same date.

At a glance

PUBLISHER
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

TYPE
Standard

VERSION
Second edition (ISO/IEC 27017:2026; replaces ISO/IEC 27017:2015)

EFFECTIVE
July 2026

DOMAIN
Cloud Security

FAMILY
ISO 27000 Series

REGION
International

INDUSTRY
Cloud & Technology Providers

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
High

Source: iso.org/standard/82878.html

Why it matters

- **Responsibilities are named** Control 5.38 covers shared roles and responsibilities within a cloud computing environment, and 5.39 covers agreeing the roles and responsibilities of the cloud service partner.
- **Supplier relationships are cloud-aware** Clause 4.3.1 explains supplier relationships in cloud services, and the supplier controls 5.19 to 5.23, including information security for use of cloud services (5.23), are covered in Clause 5.
- **Four cloud-only controls** 5.38, 5.39, 8.35 and 8.36 address matters that exist only in cloud services, such as segregation in virtual computing environments and detection of unauthorized use.
- **Monitoring is addressed** Annex B (informative) covers monitoring of cloud services, alongside the logging (8.15) and monitoring activities (8.16) controls.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 27017

Cloud Provider Register

Use Third Party Risk Management to record each cloud service with its owner, assessment and review dates (Clause 4.3.1 and controls 5.19 to 5.23).

Shared Responsibility Matrix

Record in Compliance Management which control belongs to the customer, which to the provider, and who agreed it (controls 5.38 and 5.39).

Cloud Control Library

Hold the controls of Clauses 5 to 8, including the four CLD controls, with owners, applicability and implementation status.

Cloud Risk Register

Use Cyber & IT Risk to link cloud risks to the controls chosen to treat them (Clause 4.3.3).

Monitoring and Evidence

Attach logs, monitoring reports and provider evidence to the controls they support (8.15, 8.16 and Annex B).

Edition Crosswalk

Keep the Annex A correspondence beside each record so teams moving from the 2015 edition can see how its controls map.

Common framework mappings

CSA CCM v4 | CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | ISO 27005:2022 | ISO 27018 | ISO 27701 | NIST 800-53 Rev.5

Official resources

ISO/IEC 27017 Standard

Defines guidelines for cloud-specific information security controls complementary to ISO/IEC 27002.

iso.org/standard/43757.html

ISO/IEC 27017 Implementation Guidelines

Provides implementation guidance for the security controls specific to cloud services.

iso.org/standard/43757.html

ISO/IEC 27036-4 Cloud Security

Outlines guidance for security in supplier relationships for cloud computing.

iso.org/standard/66680.html

Frequently asked questions

Is ISO/IEC 27017:2015 still current?

No. ISO's records show the 2015 first edition as withdrawn on July 27, 2026 and replaced by ISO/IEC 27017:2026, the second edition, which cancels and replaces it (Foreword). The 2026 edition is based on ISO/IEC 27002:2022 rather than the 2013 edition.

Which controls are specific to cloud services in ISO/IEC 27017:2026?

Four controls marked CLD: 5.38 shared roles and responsibilities within a cloud computing environment, 5.39 agreement on the roles and responsibilities of the cloud service partner, 8.35 segregation in virtual computing environments, and 8.36 detection and prevention of unauthorized use of cloud services. Clauses 5 to 8 otherwise follow the controls of ISO/IEC 27002:2022.

Is ISO/IEC 27017 for cloud customers or cloud providers?

Both. Clause 1 says it provides controls and guidance for cloud service customers and cloud service providers, and the Introduction says some guidance is for customers who implement the controls and some for providers who support their implementation. It also applies to private cloud (Clause 1, Note).

Can an organization be certified to ISO/IEC 27017?

It is guidance on controls and has no management system requirements of its own. Certification is of an ISMS under ISO/IEC 27001, and an organization can take controls from any source when it determines them under Clause 6.1.3 b, so ISO/IEC 27017 can supply the cloud controls in the Statement of Applicability.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What changed from the 2015 edition to the 2026 edition?

The Foreword lists three main changes: the title and scope were modified, the structure now presents controls with a simple taxonomy and attributes, and some controls were merged, some removed and several introduced. Annex A of the 2026 edition gives the correspondence with the first edition.

License included / downloadable: No ISO/IEC 27017:2026 is a paid standard sold by ISO and national standards bodies, and the text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27017-cloud-security-controls-code-of-practice

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.