SmartSuite

Framework / Cloud Security / ISO 27000 Series

ISO/IEC 27017:2015

ISO/IEC 27017 provides cloud-specific security controls to help organizations protect data and manage cloud-related risks.

What it is

ISO/IEC 27017 is an international code of practice for cloud security controls that helps organizations strengthen data protection and manage cybersecurity risks in cloud environments. The framework provides guidance on implementing security controls specifically tailored for cloud services, addressing unique challenges associated with cloud computing.

Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27017 extends the ISO/IEC 27001 and 27002 standards. It is used by cloud service providers and customers to establish, implement, and maintain controls covering cloud-specific threats, data privacy, risk management, and the shared responsibility model in cloud ecosystems.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION 2015
EFFECTIVE 2015	DOMAIN Cloud Security	FAMILY ISO 27000 Series
REGION International	INDUSTRY Cloud & Technology Providers	ADOPTION MODEL Risk Management
IMPLEMENTATION COMPLEXITY High		

Source: https://www.iso.org/standard/43757.html

Why it matters

- **Strengthen cloud cybersecurity governance** Clarify roles, responsibilities, and accountability for security in shared cloud models, supporting more effective risk management and oversight.
- **Promote regulatory and contractual alignment** Align cloud controls with international standards to help meet legal, regulatory, and contractual requirements across multiple jurisdictions.
- **Enhance data protection practices** Implement safeguards that specifically address cloud-based data storage, access, and processing, thereby reducing the risk of unauthorized exposure.
- **Increase audit and compliance readiness** Enable organizations to more efficiently demonstrate cloud control effectiveness during audits and regulatory assessments.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 27017

Cloud Security Control Extensions

Manage cloud-specific controls and guidance layered onto your ISMS program.

Shared Responsibility Model Tracking

Document cloud provider vs. customer responsibilities and required evidence for each.

Cloud Configuration Evidence

Store architecture, IAM, logging, and configuration proof tied to each control.

Vendor and Cloud Provider Oversight

Track provider assurance artifacts, reviews, and renewal schedules.

Change Management for Cloud Services

Manage configuration changes, approvals, and verification for cloud environments.

Cloud Security Reporting

Report cloud control coverage, open gaps, and exceptions by provider and service.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | 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

What is ISO/IEC 27017 used for?

ISO/IEC 27017 provides guidance on implementing cloud-specific security controls to protect data and manage cybersecurity risks in cloud computing environments. The standard helps organizations address the unique security requirements posed by cloud services for both providers and customers.

Is ISO/IEC 27017 certification required or available?

ISO/IEC 27017 is not a standalone certifiable standard but is often used as an extension to ISO/IEC 27001 certification. Organizations can be assessed for conformance with ISO/IEC 27017 controls, typically as part of a broader ISO/IEC 27001 audit or attestation.

Who should use ISO/IEC 27017?

ISO/IEC 27017 is designed for organizations that provide or utilize cloud services, including cloud service providers (CSPs) and cloud customers. It is applicable to any entity seeking to improve their cloud security posture and align with international best practices.

What are the key controls or artifacts required by ISO/IEC 27017?

Key controls under ISO/IEC 27017 address cloud service agreements, responsibilities in the shared-responsibility model, data segregation, customer data monitoring, and incident response processes specific to cloud environments. Organizations are expected to document mappings of these controls within their information security management systems (ISMS).

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does an organization implement ISO/IEC 27017?

Implementation involves mapping ISO/IEC 27017 controls to existing security management programs, conducting cloud-specific risk assessments, and ensuring operational and technical controls cover all relevant cloud threats and responsibilities. It also requires training personnel and integrating cloud-specific requirements into vendor management processes.

How does ISO/IEC 27017 relate to ISO/IEC 27001 and ISO/IEC 27002?

ISO/IEC 27017 extends the baseline controls of ISO/IEC 27001 and ISO/IEC 27002 by providing additional guidance and clarifications specific to cloud service scenarios. It supplements the existing standards by addressing gaps and risks unique to cloud computing that are not fully covered in the base standards.

What ongoing compliance activities are required for ISO/IEC 27017?

Maintaining alignment with ISO/IEC 27017 requires organizations to perform regular risk assessments, update cloud-specific controls, monitor compliance, and review responsibilities with cloud providers and customers. Continuous evidence collection and audit readiness should be incorporated into ongoing governance and review cycles.

How would SmartSuite support ISO/IEC 27017?

SmartSuite supports ISO/IEC 27017 by providing structured control libraries, integrated risk registers, and automated evidence collection tools for cloud security compliance. It enables organizations to manage cloud controls, monitor compliance status, streamline remediation workflows, and generate audit-ready reports through centralized dashboards and scheduled assessments.

License included / downloadable: No ISO/IEC 27017 requires purchase through the ISO catalogue. License not included with platform

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

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.