

ISO/IEC 27001:2013

ISO/IEC 27001:2013 specifies requirements for an ISMS to manage and protect information confidentiality, integrity, and availability.



What it is

ISO/IEC 27001:2013 is an international information security management standard that enables organizations to establish, implement, maintain, and continually improve an Information Security Management System (ISMS). Its primary purpose is to help organizations systematically manage and protect sensitive data, mitigate cybersecurity risks, and ensure the confidentiality, integrity, and availability of information assets.

Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001:2013 is widely adopted by organizations of all sizes and industries seeking a structured approach to information security. The standard covers a broad scope, including information security controls, risk assessment and treatment, policy development, incident response, and compliance oversight, aligning with frameworks such as the NIST Risk Management Framework.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION 2013
EFFECTIVE 2013	DOMAIN Cybersecurity	FAMILY ISO 27000 Series
REGION International	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY High

Source: <https://www.iso.org/isoiec-27001-information-security.html>

Why it matters

- Strengthen cybersecurity governance** Establish clear policies and processes that improve oversight and accountability across the organization's information security practices.
- Enhance regulatory alignment** Support compliance with global privacy and security regulations by providing a recognized, comprehensive framework for controls and documentation.
- Increase audit readiness** Prepare organizations for internal and external audits by maintaining systematic records that demonstrate effective risk management and control implementation.
- Promote operational resilience** Reduce the impact of security incidents through continuous risk assessment, incident response planning, and proactive business continuity efforts.

How SmartSuite supports ISO 27001

ISMS Control Library and Statement of Applicability

Manage Annex A controls, applicability decisions, and the Statement of Applicability within a structured control framework.

Risk Register and Treatment Plans

Track information security risks, mitigation strategies, control mappings, and residual risk acceptance across systems and assets.

Policy Governance and Attestations

Publish security policies, manage review cycles, and collect employee acknowledgements with complete audit history.

Evidence Collection and Control Monitoring

Centralize evidence linked to controls and maintain proof of control operation through scheduled reviews and documentation.

Internal Audit Planning and ISMS Compliance

Plan internal audits, record findings, and manage remediation tasks to maintain compliance with ISMS requirements.

ISMS Certification and Executive Reporting

Provide dashboards showing ISMS performance, open risks, control status, and readiness for certification audits.

Common framework mappings

CIS Controls v8.1

FedRAMP Rev. 5

ISO 27002:2022

ISO 27017

ISO 27018

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

ISO/IEC 27001:2013 Standard

Official publication outlining requirements for an Information Security Management System (ISMS).
iso.org/standard/54534.html

ISO/IEC 27002:2022 Controls Guidance

Provides guidance for implementing security controls supporting ISO/IEC 27001.
iso.org/standard/75652.html

ISO 27001 Implementation Guidance

Offers official advice on implementing and certifying against ISO/IEC 27001.
iso.org/isoiec-27001-information-security.html

ISO 27000 Series Overview

Describes the framework and standards within the ISO 27000 family.
iso.org/isoiec-27001-information-security.html

Frequently asked questions

What is ISO 27001 used for?

ISO 27001 is used to establish, implement, and maintain an Information Security Management System (ISMS). It helps organizations systematically manage sensitive information, mitigate cybersecurity risks, and ensure the confidentiality, integrity, and availability of information assets.

Is ISO 27001 certification mandatory?

ISO 27001 certification is not mandatory by law, but many organizations pursue certification to meet client, partner, or regulatory requirements and to demonstrate a robust information security posture. Certification is achieved through an accredited external audit and is recognized internationally.

What does the ISMS scope mean in practice?

The ISMS scope defines the organizational boundaries and information assets covered by ISO 27001 controls. It should include the locations, systems, people, and data that are subject to the ISMS, and is documented in the ISMS scope statement to ensure clarity and auditability.

What is the Statement of Applicability (SoA) in ISO 27001?

The Statement of Applicability (SoA) lists all ISO 27001 Annex A security controls, specifying which controls are implemented or excluded, along with justifications. It serves as a key artifact for auditors, demonstrating how controls are selected and tailored based on the organization's risk assessment.

How does the risk assessment process work for ISO 27001 compliance?

The risk assessment process in ISO 27001 involves identifying information security risks, evaluating their potential impact and likelihood, and determining how to treat them through the application of appropriate controls. The findings directly inform the choice of controls documented in the SoA.

How does ISO 27001 relate to other standards like ISO 27002 or NIST?

ISO 27001 outlines the requirements for establishing an ISMS, while ISO 27002 provides detailed guidance on the implementation of the controls referenced in ISO 27001 Annex A. ISO 27001 is also aligned with other frameworks, such as the NIST Risk Management Framework, to support integrated risk management.

What is required to maintain ongoing ISO 27001 compliance?

Maintaining ISO 27001 compliance requires regular internal audits, continual risk assessments, periodic management reviews, and timely remediation of nonconformities. Organizations must continually improve their ISMS, update documentation, and ensure controls remain effective against emerging threats.

How would SmartSuite support ISO 27001?

SmartSuite helps organizations manage ISO 27001 by enabling risk tracking, control management, and evidence collection within a centralized platform. It supports audit readiness through compliance dashboards, automated reminders, and document management, streamlining reporting, policy governance, and remediation workflows.

License included / downloadable: No ISO/IEC 27001:2013 requires purchase from the ISO/IEC standards catalog. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27001-2013-information-security-management-system-isms