

ISO/IEC 27000:2018

ISO/IEC 27000 provides foundational concepts and terminology for establishing and operating an information security management system.



What it is

ISO/IEC 27000 is an international information security management framework that establishes the foundational concepts, principles, and terminology used within Information Security Management Systems (ISMS). It provides organizations with clear definitions and a structured vocabulary to support effective cybersecurity risk management and data protection efforts.

Developed and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27000 is utilized by security professionals, compliance teams, and auditors implementing or maintaining ISMS aligned with the ISO/IEC 27000 family of standards, including ISO/IEC 27001. The framework covers key areas such as information security controls, risk assessment, privacy governance, and compliance oversight.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION ISO/IEC 27000 (latest published edition)
EFFECTIVE 2018	DOMAIN Cybersecurity	FAMILY ISO Management Systems
REGION International	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.iso.org/standard/73906.html>

Why it matters

- **Strengthen security governance** Provide a common terminology that improves coordination and decision-making among security teams, management, and stakeholders.
- **Enhance compliance support** Clarify key ISMS concepts and requirements, facilitating alignment with global regulations and streamlining compliance initiatives.
- **Improve risk management effectiveness** Support consistent identification, assessment, and management of information security risks by standardizing language and definitions.
- **Increase audit readiness** Enable clear communication during internal and external audits, reducing misunderstandings and supporting successful certification processes.

How SmartSuite supports ISO 27000

Standardized Security Vocabulary

Use consistent ISMS terminology across policies, controls, risks, and audits.

Policy and Procedure Templates

Create repeatable templates for policies, procedures, and control narratives.

Control Library Consistency

Normalize control naming and structure to reduce ambiguity during audits.

Risk and Incident Definitions

Standardize how risks, events, and incidents are logged and managed.

Training and Onboarding Support

Publish definitions and guidance for faster team alignment and adoption.

Governance Reporting

Report consistent status across ISMS artifacts using shared definitions.

Common framework mappings

CIS Controls v8.1

ISO 27001:2022

ISO 27002:2022

ISO 27017

ISO 27018

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

Official resources

ISO/IEC 27000 Overview and Vocabulary

Defines foundational concepts and vocabulary for Information Security Management Systems (ISMS).
iso.org/standard/73906.html

ISO/IEC 27001 Standard

Provides requirements for establishing, implementing, and maintaining an ISMS.
iso.org/isoiec-27001-information-security.html

ISO/IEC 27002 Security Controls Guidance

Provides implementation guidance supporting ISO 27001 Annex A security controls.
iso.org/standard/75652.html

ISO 27000 Family Overview

Describes the structure and relationship of ISO information security standards.
iso.org/isoiec-27001-information-security.html

Frequently asked questions

What is ISO/IEC 27000 used for?

ISO/IEC 27000 is used to provide a structured vocabulary and foundational concepts for Information Security Management Systems (ISMS). It ensures a consistent understanding of information security terminology, principles, and processes, serving as a reference point for organizations building or maintaining ISMS aligned with other standards in the ISO/IEC 27000 series.

Is ISO/IEC 27000 certifiable or required by law?

ISO/IEC 27000 itself is not certifiable and is not mandated by law. It acts as an overview and reference standard. Certification is available for ISO/IEC 27001, which relies on the definitions and guidance provided by ISO/IEC 27000.

What organizations does ISO/IEC 27000 apply to?

ISO/IEC 27000 is applicable to organizations of all sizes and sectors looking to establish, implement, or improve an ISMS. It is relevant to IT, compliance, and security teams aiming to align security management practices with recognized international standards.

What are the key concepts and artifacts defined in ISO/IEC 27000?

Key concepts in ISO/IEC 27000 include definitions of information security, ISMS, risk management, controls, stakeholders, and continual improvement. The standard provides baseline terminology and describes artifacts such as risk registers, policies, procedures, and ISMS documentation.

How does an organization implement ISO/IEC 27000?

Organizations use ISO/IEC 27000 as a foundational reference when building or refining their ISMS. Implementation involves adopting the terminology and concepts, conducting risk assessments, selecting security controls, and ensuring documentation is consistent with the ISO/IEC family requirements.

What is the relationship between ISO/IEC 27000, ISO/IEC 27001, and ISO/IEC 27002?

ISO/IEC 27000 provides vocabulary and overview for the entire ISO/IEC 27000 series. ISO/IEC 27001 sets out ISMS requirements, while ISO/IEC 27002 details control implementation guidance. ISO/IEC 27000 ensures cohesive understanding for applying the requirements and controls found in these related standards.

What are the ongoing compliance requirements related to ISO/IEC 27000?

While ISO/IEC 27000 itself does not impose operational requirements, it supports ongoing ISMS governance by clarifying key terms and processes. Organizations should periodically review definitions, update documentation, and ensure that all ISMS activities align with the terminology and principles outlined in ISO/IEC 27000.

How would SmartSuite support ISO/IEC 27000?

SmartSuite helps organizations operationalize ISO/IEC 27000 by providing integrated workspaces for maintaining control libraries, risk registers, and policy documentation. It enables risk tracking, manages security controls, facilitates evidence collection, ensures audit readiness, and delivers compliance reporting dashboards to monitor and govern ISMS activities according to the ISO/IEC 27000 framework.

License included / downloadable: No ISO/IEC 27000 is published by the International Organization for Standardization and the International Electrotechnical Commission. Access to the full standard typically requires purchasing official documentation through authorized standards organizations. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27000-information-security-management-systems-overview-and-vocabulary