ISO/IEC 27001

**ISO/IEC 27001** is an international standard on how to manage information security. The standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005 and then revised in 2013. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure. A European update of the standard was published in 2017. Organizations that meet the standard's requirements can choose to be certified by an accredited certification body following successful completion of an audit. The effectiveness of the ISO/IEC 27001 certification process and the overall standard has been addressed in a recent large-scale study.

## How the standard works

Most organizations have a number of information security controls. However, without an information security management system (ISMS), controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Security controls in operation typically address certain aspects of information technology (IT) or data s

ecurity specifically; leaving non-IT information assets (such as paperwork and proprietary knowledge) less protected on the whole. Moreover, business continuity planning and physical security may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization.

ISO/IEC 27001 requires that management:

* Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
* Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
* Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

## Certification[[edit](https://en.wikipedia.org/w/index.php?title=ISO/IEC_27001&action=edit&section=3" \o "Edit section: Certification)]

An ISMS may be certified compliant with ISO/IEC 27001 by a number of [Accredited Registrars](https://en.wikipedia.org/wiki/Accredited_Registrar) worldwide.[[7]](https://en.wikipedia.org/wiki/ISO/IEC_27001#cite_note-7) [Certification](https://en.wikipedia.org/wiki/Certification) against any of the recognized national variants of ISO/IEC 27001 (e.g. JIS Q 27001, the Japanese version) by an accredited certification body is functionally equivalent to certification against ISO/IEC 27001 itself.

In some countries, the bodies that verify conformity of management systems to specified standards are called "certification bodies", while in others they are commonly referred to as "registration bodies", "assessment and registration bodies", "certification/ registration bodies", and sometimes "registrars".

The ISO/IEC 27001 certification,[[8]](https://en.wikipedia.org/wiki/ISO/IEC_27001" \l "cite_note-8) like other ISO management system certifications, usually involves a three-stage external audit process defined by the ISO/IEC 17021[[9]](https://en.wikipedia.org/wiki/ISO/IEC_27001#cite_note-9) and ISO/IEC 27006[[10]](https://en.wikipedia.org/wiki/ISO/IEC_27001#cite_note-10) standards:

* **Stage 1** is a preliminary, informal review of the ISMS, for example checking the existence and completeness of key documentation such as the organization's information security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the auditors with the organization and vice versa.
* **Stage 2** is a more detailed and formal compliance [audit](https://en.wikipedia.org/wiki/Audit), independently testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors will seek evidence to confirm that the management system has been properly designed and implemented, and is in fact in operation (for example by confirming that a security committee or similar management body meets regularly to oversee the ISMS). Certification audits are usually conducted by [ISO/IEC 27001 Lead Auditors](https://en.wikipedia.org/wiki/ISO/IEC_27001_Lead_Auditor). Passing this stage results in the ISMS being certified compliant with ISO/IEC 27001.
* **Ongoing** involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended. These should happen at least annually but (by agreement with management) are often conducted more frequently, particularly while the ISMS is still maturing.

## Structure of the standard

The official title of the standard is "Information technology — Security techniques — Information security management systems — Requirements"

ISO/IEC 27001:2013 has ten short clauses, plus a long annex, which cover:

1. Scope of the standard

2. How the document is referenced

3. Reuse of the terms and definitions in ISO/IEC 27000

4. Organizational context and stakeholders

5. Information security leadership and high-level support for policy

6. Planning an [information security management system](https://en.wikipedia.org/wiki/Information_security_management#Information_security_management_system); risk assessment; risk treatment

7. Supporting an information security management system

8. Making an information security management system operational

9. Reviewing the system's performance

10. Corrective action

## Controls

There are 114 controls in 14 groups and 35 control categories:

A.5: Information security policies (2 controls)

A.6: Organization of information security (7 controls)

A.7: Human resource security - 6 controls that are applied before, during, or after employment

A.8: Asset management (10 controls)

A.9: Access control (14 controls)

A.10: Cryptography (2 controls)

A.11: Physical and environmental security (15 controls)

A.12: Operations security (14 controls)

A.13: Communications security (7 controls)

A.14: System acquisition, development and maintenance (13 controls)

A.15: Supplier relationships (5 controls)

A.16: Information security incident management (7 controls)

A.17: Information security aspects of business continuity management (4 controls)

A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)