ISO 27001

Awareness Briefing

Issued 2026

ISO 27001:2022 is a specification for an information security management system (ISMS).

An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

ISO 27001 uses a top-down, risk-based approach and is technology-neutral. The specification defines a six-part planning process:

- Define a security policy.
- Define the scope of the ISMS.
- Conduct a risk assessment.
- Manage identified risks.
- Select control objectives and controls to be implemented.
- Prepare a statement of applicability.

The specification includes details for documentation, management responsibility, internal audits, continual improvement and risk management. The standard requires cooperation among all sections of an organisation.

ISO 27001:2022 is an information security standard that was published on 25 September 2022 and is a specification for an information security management system (ISMS). Organisations which meet the standard may be accredited by an independent certification body.

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

ISO 27001:2022 has ten short clauses, plus a long annex, which cover:

High-Level Structure (HLS)



The ten-clause Annex SL structure shared by ISO 27001 and other ISO management system standards

Annex A: List of controls and their objectives.

This structure mirrors the structure of other management system standards such as ISO 9001 (Quality Management).