STANDARD SUMMARY · CERT.GT

ISO/IEC 27001 overview

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: Management, security officers and compliance officers.

ISO/IEC 27001 is the international standard for managing information security. It does not tell you what technology to buy: it describes how to organize yourself to identify risks, decide which controls to apply and improve over time. It is the only standard in the 27000 family that can be certified.

The essentials

- The current version is the 2022 one. Certificates for the 2013 version stopped being valid on October 31, 2025.
- It asks you to implement an Information Security Management System (ISMS): policies, people in charge, risk analysis, controls and periodic review.
- It is risk-based: each organization decides which controls it applies and justifies that in writing.
- It applies to any size and sector; you define the scope (the whole company, one service, one site).

What it requires: clauses 4 to 10

4. Context of the organization	Understand the organization and its interested parties, and define the scope of the ISMS.
5. Leadership	Top management commitment, a security policy and assignment of roles.
6. Planning	Assess and treat risks, set objectives and plan changes.
7. Support	Resources, competence, awareness, communication and documented information.
8. Operation	Carry out the risk treatment and control the processes.
9. Performance evaluation	Measure, audit internally and review with top management.
10. Improvement	Correct nonconformities and improve continually.

The Annex A controls

Annex A lists 93 reference controls in four themes. Not all of them are mandatory: the Statement of Applicability states which ones you apply and why you exclude the rest.

Organizational (37)	Policies, roles, asset inventory, suppliers, cloud, incident management, continuity, compliance.
People (8)	Screening, contracts, awareness, disciplinary process, remote working, event reporting.
Physical (14)	Perimeter, access to offices, equipment off premises, media, cabling, maintenance.
Technological (34)	Access, encryption, backups, logs, vulnerabilities, networks, secure development.

What is new in the 2022 version

- Eleven new controls: threat intelligence, information security for use of cloud services, ICT readiness for business continuity, physical security monitoring, configuration management, information deletion, data masking, data leakage prevention, monitoring activities, web filtering and secure coding.
- The 114 controls from 2013 were reorganized and merged into 93.
- Each control has attributes (type, property it protects, cybersecurity concept) that make it easier to relate it to other frameworks.

How to get started

- Get explicit backing from top management: without budget or authority, the ISMS goes nowhere.
- Define a small, useful scope, for example the service that is most critical to your customers.
- Build the inventory of information assets and their owners.
- Assess the risks with a simple, repeatable method, and decide how each one will be treated.
- Write the Statement of Applicability and the risk treatment plan.
- Implement, measure, audit internally and hold the management review before seeking certification.

Certification

- It is granted by an accredited certification body, not by ISO.
- Stage 1: documentation review. Stage 2: audit of the implementation.
- The certificate lasts three years, with annual surveillance audits.
- It is not required in order to benefit from the standard: many organizations use it as a guide without getting certified.

Common mistakes

- Treating it as an IT project rather than a management system for the whole organization.
- Copying another company's policies that nobody reads or follows.
- Choosing a scope so broad that the project never ends.
- Documenting a lot and operating little: the auditor asks for evidence that the controls work.

Official text

ISO/IEC 27001:2022, published by ISO and IEC (iso.org). The official text must be purchased.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

Summary prepared by cert.gt for educational purposes; it is not the official text of the standard and does not replace legal or compliance advice. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).