

ISO/IEC 27001:2022

Cheat sheet for the information security management standard

What it is

- A standard for running an information security management system (ISMS): a managed, repeating process, not a one-off project.
- Organisations can be certified by an accredited body. Certificates run for three years with yearly surveillance audits.

The management clauses (4-10)

- 4 Context and scope. 5 Leadership and policy. 6 Planning: risks and objectives. 7 Support: resources, awareness, documents.
- 8 Operation: carry out the risk treatment. 9 Performance evaluation: monitoring, internal audit, management review. 10 Improvement.

Annex A: 93 controls in four themes

- Organisational (37), People (8), Physical (14), Technological (34).
- You choose which controls apply and record why in the Statement of Applicability.

Documents auditors expect

- ISMS scope. Information security policy. Risk assessment method and results. Risk treatment plan. Statement of Applicability.
- Internal audit reports and management review minutes. Records that controls actually run.

First five actions

- 1. Define scope and get management backing. 2. List assets and run a risk assessment. 3. Select controls and write the Statement of Applicability. 4. Put the controls in place and keep evidence. 5. Run an internal audit and management review before the certification audit.