ISO 27001 Overview and Guidance

This guidance document provides an overview of the **ISO 27001:2022 Information Security Management Systems** standard.

Introduction

ISO 27001 Information Security Management Systems sets out the requirements for an information security management system (ISMS). Its aim is to help organisations identify and protect their key information assets, keeping information confidential, accurate and available when it is needed.

The current version of the standard is **ISO/IEC 27001:2022**. Amendment 1, published in 2024, adds that organisations must determine whether climate change is a relevant issue, and notes that relevant interested parties can have requirements related to climate change.

ISO 27001 follows the harmonised structure used by ISO management system standards (formerly known as Annex SL), so its clauses align closely with ISO 9001, ISO 14001 and other management system standards, which makes it straightforward to run them together as an integrated management system.

Where ISO 27001 differs is Annex A, which lists 93 information security controls in four themes (organisational, people, physical and technological). The controls chosen in the risk treatment process are compared with Annex A so that no necessary control is missed.

Roles and responsibilities must be clearly defined, with leadership and commitment from top management, and documented information must be controlled.

Information Security Management

There are specific documentation requirements for this standard. The Annex A controls are reviewed and a Statement of Applicability is prepared, showing the controls needed, the justification for including them, whether they are implemented and the justification for excluding any Annex A control.

The organisation needs a full picture of its information: where it is held, how it is accessed and shared, and the controls that protect it from unauthorised access, accidental change or loss, so that information systems are robust and information is available when required.

Key requirements of the standard include;

- An information security policy and topic-specific policies, approved and communicated to all workers
- Information security risk assessment, to identify and rate the risks, with risk owners identified
- Information security risk treatment, to address the risks and determine the controls needed
- A Statement of Applicability covering the 93 Annex A controls
- Arrangements for workers, including screening, awareness and training, confidentiality agreements, user accounts and access control

- Management of IT equipment, networks and physical security, including malware protection, backups, event logging and secure disposal
- Supplier and cloud service security, with information security requirements agreed and monitored

ISO 27001:2022 Certification Audit

During an audit the auditor(s) will be looking for objective evidence that each clause in the standard has been met and complied with.

As well as reviewing all the relevant clauses, there are various things you can prepare and have in place prior to the audit;

- Completed and up-to-date management review, including the results of risk assessment and the status of the risk treatment plan
- Completed internal audit(s) covering information security
- Information security risk assessment and an approved risk treatment plan
- A Statement of Applicability that is complete and correct for the controls in place
- Information security objectives and plans to achieve them
- Information classification applied to key information assets
- Event logging, monitoring and backup arrangements, with evidence of backups being tested
- ICT continuity arrangements, with evidence of testing
- Evidence of information security awareness training and competence
- Information security incidents logged and dealt with effectively
- Information security arrangements agreed with suppliers and other third parties
- Evidence that climate change has been considered when determining external and internal issues (clause 4.1)

More on the audit process and preparing for certification:

- **ISO Certification Guidance: isoassured.co.uk/resources/iso-certification-help**
- **Remote support: isomanaged.com/iso-consultancy-support**

More on ISO 27001, clause by clause, in the isomanaged.com knowledge base:

- **isomanaged.com/knowledge-base/iso-standards/iso-27001**