ISO27001:2022 Overview and Guidance

Introduction

The ISO 27001 standard details requirements for Information Security management systems and the aim of this standard is to help organisations review, identify and manage key information assets and data. Often considered an Information Technology standard, ISO 27001 is actually much broader and like other management system standards such as ISO 9001 the standard is primarily concerned with the management system. Where ISO 27001 differs is that it includes an Annex (**Annex A**) listing various controls which need to be considered in the risk treatment process.

The current version of the standard, ISO 27001:2022, is structured following Annex SL and therefore the clauses are very similar to the structure of ISO 9001 and other Annex SL standards. The standard requires a clearly defined organisational structure with roles and responsibilities defined with the involvement and commitment from top management. Other requirements of this standard are that documented information is controlled, risks and opportunities are considered and that actions to address risks and opportunities are identified and managed.

The standard requires quite a lot of documentation to be prepared including Information Security Policies and evidence that all the Annex A controls have been addressed in a statement of applicability. The risk assessment / risk treatment process may include review and consideration of IT infrastructure and systems and therefore may require some competent assessment / review of IT systems.

Information Security Management

There are quite specific documentation requirements for this standard and a full review of all the **Annex A** controls is required with a statement of applicability detailing whether the control is relevant, or justifying why it isn't, and then detailing relevant controls.

A full review of information within the organisation, where it is stored, accessed and how it is disseminated as well as the controls in place to preserve the information and ensure it is protected from unauthorised access, is protected from accidental corruption or alteration and that the Information systems in place are robust and reliable to ensure availability of information when required for business continuity.

Key requirements of this standard include;

- **Relevant Policies** – various topic specific policies detailed in the standard need to be in place and all workers aware.
- **Risk assessment** –information security risk assessment to identify and rate the information security risks. Owners of the risks must also be identified.
- **Information security risk treatment** –risk treatment process to address the risks identified, including identifying required controls.
- **Statement of applicability** –Controls are split into four different categories; organisational, people, physical and technological.
- **Information Security Arrangements** – various arrangements are required including staff awareness / training, screening, user management, access control, confidentiality agreements.
- **IT Equipment and Physical Security** – various arrangements pertaining to management of all devices, networks and information systems.

ISO27001:2022 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 other things you can prepare and have in place prior to the audit;

- Completed and up-to-date management review
- Completed internal audit(s) covering information security
- Documented information regarding identification of information security risks and risk treatment plan
- Information Security of Software and Systems - Event logging, Monitoring and arrangements
- Protection of Information Assets – Information Classification applied to key assets

- Business continuity arrangements and evidence of testing of arrangements and backups
- Management of IT Equipment and Physical Security
- Controls in place to protect Confidentiality, Integrity and Availability of information assets
- Controls detailed on Statement of Applicability adequate and correct
- Evidence of roles and responsibilities for information assets clearly identified
- Evidence of staff information security awareness training and competency
- Staff Information Security Arrangements – Awareness, Access Control, Confidentiality
- Information Security Risk Management - Information Security Incidents managed effectively
- Information security objectives and plans to achieve them
- Information Security arrangements with third parties

Presenting evidence during the audit

For guidance on the audit process and how to prepare for the audit and an overview of the audit plan and the certification audit process please review the **Certification Audit Guidance** which is available **online here**.

In an audit involving a site visit, the auditor will likely just view evidence in person, whilst asking questions, a site tour may also be conducted. For remote audits it is often requested that photographs / videos are submitted as evidence.

Further support

- Management system documentation & resources: **isomanaged.com/alphazdocuments**
- Remote support: **isomanaged.com/remote-support**
- ISO Consultancy: **isoassured.co.uk/iso-consultancy**