iQMO First for Quality

A guide to ISO27001:2022 Certification

ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

Why is ISO/IEC 27001 important?
With cyber-crime on the rise and new threats constantly emerging, it can seem difficult or even impossible to manage cyber-risks. ISO/IEC 27001 helps organizations become risk-aware and proactively identify and address weaknesses.

ISO/IEC 27001 promotes a holistic approach to information security: vetting people, policies and technology. An information security management system implemented according to this standard is a tool for risk management, cyber-resilience and operational excellence.

Taken from ISO

The IQMO Approach:

- Our quotation covers all required actions to provide you with a compliant ISO27001 Management System.
- This is a comprehensive solution which includes Initial Assessment, thorough Gap Analysis, Implementation of the ISMS into your business
- We only assign International Register of Certificated Auditors (IRCA) qualified Lead Auditors (or equivalent) to implement ISO standards. They are experts in their field.
- Our auditor is involved throughout and will perform the following duties:
    - Design and build your bespoke management system based on current processes
    - Document required procedures and guide you through what needs to be done on site
    - Instruct your assigned internal auditor on how to complete a simple system audit
- We can arrange in-depth Internal Auditor Training to create experts in your company.
- The work will be completed within the stated timescales in the proposal assuming your reasonable availability and cooperation.
- We can organise for UKAS Accredited with a suitable Certification Body
- The IQMO implemented ISO Management System will pass any 3rd party audit.
- Most of the auditor's work is done off site so we will cause minimum disruption to your day-to-day operation.
- We do not send you templates with instructions for you to do the work yourselves.
- There are no stringent T&C's or long-term contracts associated with IQMO agreements.

Overview

ISO 27001:2022 is an international standard, revised in October 2022, that sets out how to implement an Information Security Management System (ISMS).

The standard helps organisations of all shape and size to;

- Identify suitable and proportionate security controls within the process of setting up an ISMS
- Achieve best practices in information security management
- Meet legal, statutory, regulatory, and contractual requirements in relation to information security
- Strengthen risk management and reduce the likelihood of information security breaches
- Increase confidence in the organization's Information Security management.

The revision of this standard in October 2022 brings a modern approach to managing security controls with attributes. The standard also contributes to UN Sustainable Development Goal 9 on industry, innovation, and infrastructure.

The standard aims to provide businesses, of every size and sector, with a new generation of security control guidance, with the aim of making the guidance modernised, simplified and versatile to granting organisations the autonomy to select and scope security controls as deemed fit.

Due to the COVID-19 pandemic, most businesses have been forced to accelerate their digital transformation and rely more on their cloud infrastructure, as many of their employees continue to adapt and move towards a hybrid work model.

Whilst organizations were finding their feet amongst these rapid changes, cybercriminals were finding ways to exploit vulnerabilities within these new systems with ever more sophisticated technology.

ISO 27001:2022 truly allows your organisation to meet the threats of today and tomorrow.

Security Controls & Objectives

ISO 27001:2022 is the most comprehensive Information Security Management System (ISMS) of its kind and is a product of countless submissions to ISO in Geneva. The technical committee responsible for creating the standard contains expertise from across the Cyber Security community.

In addition to the best practice elements of the standard it contains 93 controls an organisation must consider in order to gain compliance to ISO 27001:2022. These controls are grouped into 4 key themes;

- Organisational (37 Controls)
- People (8 Controls)
- Physical (14 Controls)
- Technological (34 Controls)

As a result of the launch of ISO 27001:2022 in October 2022 11 new controls have been added with a total of 93 controls available for consideration. Not all of these controls will need to be used by an organisation – we help you determine and document this in the Statement of Applicability.

The 11 new controls to be considered as part of an ISO 27001:2022 Implementation are:

- 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
- Secure coding

ISO/IEC 27001:2022 Implementation Process

1. Kick Off

A remote meeting to introduce you to your IQMO Consultant & Support Team, date set for initial meeting (Gap Analysis). Familiarisation with your business practices, domain and requirements & exchange of confidentiality agreements.

2. Information Security Policy

With support from your consultant an Information Security policy will be drafted and should be communicated throughout your organisation.

3. Information Assets Register

With support from your consultant an Information Asset(s) register will be created. We'll provide advice on populating this.

4. Risk Assessment

With our guidance we'll show you how to undertake a simple Risk Assessment of the above Asset Register. At the end of this exercise, you'll be left with a Risk Register.

5. Gap Analysis

Our consultant will conduct a full Gap Analysis of your existing systems, policies and documentation. This provides us with a list of required documentation, many of which will be crafted for you. This also informs us which of the 93 controls need to be created, amended or included if already in place. We then help you draft a Statement of Applicability (SoA)

6. Client Review

We'll review the Gap Analysis and Risk Assessment together. You'll then need to decide which risks should be addresses and how (Using controls detailed in the SoA).

7. Management System Creation

Our consultant will draft an ISMS Manual, Procedurals Manual and associated documentation (Internal Audit, Management Review, Personnel forms etc) for your review.

8. Client Approval

Client approves the Implementation Plan and all documents and manuals

We hope the above helps you in your quest for ISO Certification.

With many years' working within the ISO industry we will be delighted to assist with your ISO Implementation, ISO Internal Auditing, Certification Support and general Quality Management requirements.

Please feel free to Call us at iQMO 0330 320 0859 or email contact@iqmo.co.uk

We look forward to hearing from you. www.iqmo.co.uk