

**Guide to the
requirements of**

ISO 27001 2022

A plain English guide to the ISO 27001:2022
Information Security Management System

isoqar.com

Requirements of ISO 27001

The ISO 27001 Information Security Management Systems (ISMS) standard is one of the most popular ISO standards. Its popularity continues to grow as organisations and individuals become increasingly concerned about the security of confidential information and cyber security generally.

The Main Clauses of ISO 27001

Clause 1 – Scope

This describes the scope of the ISO 27001 standard. It doesn't outline any actual requirements.

Clause 2 – Normative references

This clause identifies other standards and documents that relate to and are referenced within ISO 27001.

Clause 3 – Terms and definitions

This explains certain key words and phrases that are used throughout the standard. It helps you understand some of the jargon.

Businesses choose to implement ISO 27001 because it helps address these challenges.



Clause 4

Context of the Organisation

Here is where you build a picture of the business environment in which you operate. You need to understand this before you can start to build your system.

- Determine the relevant external and internal factors that affect your organisation
- A SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis may prove useful.
- You should identify everyone with an interest in your business such as staff, suppliers, clients – known as ‘stakeholders’. This is particularly important as you are probably responsible for their confidential data and information relating to them
- You also need to determine the ‘scope’ of your system; that is, for example, what sites and services will be covered by your ISMS.

Clause 5

Leadership and Commitment

An ISMS won’t work without commitment from top management. This is key to the success of your system and auditors will look for evidence of this.

- Top management must be directly involved and take overall responsibility
- They should develop an Information Security Policy
- Roles and responsibilities must be clear
- The system must be properly resourced

Clause 6

Planning

Risk-based thinking is a key principle of ISO 27001. You should plan actions to address risks and opportunities. This is all about ensuring that you get the expected results and there are no nasty surprises. You should also be aiming for continual improvement.

- Define and apply an information security risk assessment process
- Identify, analyse and evaluate information security risks
- Apply an information security risk treatment process
- Establish information security objectives and plan how you are going to achieve them (who, what, how, where, when)

Clause 7

Support

You need to take steps to ensure that the ISMS is given the appropriate support from top management to enable it to function effectively.

- You need to make sure that the system is adequately resourced
- Employees must be aware of the ISMS and their role within it
- People must be competent in their roles
- You must have effective communications in place
- You need to keep appropriate documentation to allow the system to function effectively (but this need not be burdensome)

Clause 8

Operation

This is where your system comes to life. This clause is about the day-to-day activities that produce the products and services to deliver to your customers.

- Make sure what you do will result in the desired outcomes
- Information security risk assessments should be done at planned intervals
- The information security risk treatment plan must be implemented
- Outsourced processes must be controlled

Clause 9

Performance Evaluation

The only way to tell if your ISMS is working and you are raising standards is to measure what you do.

- Determine what needs to be monitored, how to monitor and when
- You must carry out internal audits
- The results must be measured, analysed and evaluated
- Top management must review the system and performance

Clause 10

Improvement

You must put things right when they go wrong. This is ‘corrective action’ which leads to continual improvement. This underpins the concept of ISO 27001 and all ISO management systems.

- Identify nonconformities and take corrective action
- Eliminate causes of nonconformity to prevent recurrence
- Make changes to the ISMS itself if needed
- Aim for continual improvement of the ISMS



About Alcumus ISOQAR

We help organisations create better workplaces through a huge range of common and sector-specific standards and compliance assessments, allowing them to demonstrate to their customers, competitors, suppliers and staff, that they are committed to being the best that they can by minimising risk, delivering change, driving improvement and winning more work.

As one of the UK's largest UKAS accredited certification bodies we can audit, certify and train organisations across multiple sectors.

We work worldwide, so we can help businesses gain a competitive edge anywhere they need us.

About Alcumus

Alcumus is a leading provider of software-led risk management solutions providing clients with advice, expertise and support to help them identify and mitigate risks, navigate compliance and keep people safe. It supports both UK and International clients – many of whom are on the FTSE 100 index – with a wide range of risk management services. This includes products across Supply Chain Management, EHSQ Software, UKAS Accredited Certification and HR and H&S support services.

Our people are at the heart of our business, building strong relationships with our clients to understand their needs, minimise risks and navigate compliance through our in-depth knowledge of your sector, regulations and challenges.

E: info@alcumus.com
T: 0333 920 8824
W: alcumus.com

