



ISO 27001

Datasheet

ISO 27001 Essentials

International management system standard reflecting **information security best practice** and **continuous improvement**.



'Business' (not IT) **Standard** aimed at protecting **Confidentiality, Integrity and Availability** of **information assets**.



Provides a **practical framework** i.e. information security management system (**ISMS**).



Risk-based Standard suitable for **any organisation** irrespective of size and **industry sector**.

What Does the ISO 27001 Standard Contain?

Like other ISO standards, the main clauses of ISO 27001 provide mandatory requirements for the development, implementation, and continual improvement of an ISMS, including such things as:

- **Setting a scope for the ISMS**
- **Gaining senior management commitment**
- **Conducting a risk assessment and selecting controls**
- **Developing/documenting specific policies & procedures**
- **Conducting audits and management reviews**



In addition to the main requirement clauses of ISO 27001, there is an **Annex A** which includes 114 controls (security measures) spread across 14 categories (e.g. human resources, cryptography, access control, physical security, supplier relationships).

All 114 controls must be considered (and others as appropriate), however their selection and implementation will ultimately be determined by the risk assessment. Implementation guidance on the 114 controls can be found in the separate ISO 27002 Standard.

What is ISO 27001 Certification?

Demonstration that you have appropriately implemented ISO 27001. In order to achieve ISO 27001 certification, an organisation must undertake a 2-staged assessment of its ISMS by an external accredited (ideally UKAS) certification body.

The organisation must provide evidence that it meets the requirements of the main clauses of the Standard, i.e. establishing, implementing, maintaining and continually improving its ISMS.



This involves assessing and treating risks, developing processes to manage information security effectively, documenting and implementing those processes and ensuring they are performing as expected.

Typically, it takes 9-12 months to implement and embed an ISMS and be able to produce the required evidence ahead of a formal certification body assessment.

Benefits of ISO 27001 Certification?



1



Provides assurance to stakeholders, and customers in particular, that the security of information is being managed effectively and demonstrates a commitment to continual improvement.

2



Provides a number of commercial benefits including meeting tender requests, providing competitive advantage and helping to win new business.

3



Ensures good corporate and security governance and helps meet legal obligations.

4



Raises the profile of information security internally, motivates staff to be vigilant and reduces likelihood of a security breach or incident, thereby protecting an organisation's brand and reputation.

How Can URM Help?

As the UK's leading ISO 27001 consultancy, URM's role is to assist organisations implement an ISMS which complies with the requirements of the Standard and which will achieve certification if required.

Our mission is to ensure organisations implement ISO 27001 in a manageable, pragmatic and appropriate manner.

We do this through the delivery of consultancy and training services and risk management products.



URM offers a totally flexible service which can include 'full lifecycle' or ad hoc services, including providing advice and guidance, conducting risk assessments and gap analyses, developing policies, assisting with internal audits and providing interim resources.

Why URM?

- Track record of assisting over 250 organisations to gain & maintain certification to ISO 27001
- 100% certification guarantee
- All consultants have at least 5 years' experience implementing and managing ISMS'
- Assurance that any implementation is 'appropriate', pragmatic and maximises what is already in place.



URM Consulting Services Ltd
+44 (0)118 206 5410

info@urmconsulting.com
www.urmconsulting.com