ISO PDF FREE DOWNLOAD

Our Essential Guide to:

ISO 27001:2015

Information Security Management

ISO CONSULTANTS

MAKING SENSE OF CERTIFICATION

Essential Guide To:

ISO 27001:2015

ISO CONSULTANTS
MAKING SENSE OF CERTIFICATION

What is ISO 27001:2015?

A management standard that:

- ☑ Helps companies to establish and maintain an effective Information Security Management System (ISMS).
- ☑ Systematically examines any risks to the organisation's information security and puts in place policies & procedures to manage those risks.
- ☑ Establishes a structured and managed approach to controlling your information securely.
- ☑ Acts as a differentiator in the market
- ☑ Adds credibility and status to your company
- ☑ Leads to improving and maintaining effective information security practices in a measurable way.

Does it work? What do certified businesses say?

- ☑ Significantly reduces the opportunity for data breaches to occur
- ☑ A clear sign to customers that looking after their data and your own is taken seriously.
- ☑ It helps businesses establish data ownership within their organisation, identifying who is responsible for what information, which in turn helps with staff engagement in developing the business.
- ☑ It also establishes access control measures ensuring only people who are authorised have access to specific data/systems within the business
- ☑ Opens up government tender possibilities (mandatory for some government tenders)
- ☑ It helps to develop and enhance existing best in-house practice.
- ☑ It provides an organisation with assurance, knowing that their processes and controls are secure.
- ☑ Improved organisation – an underrated benefit! Your business becomes more proactive
- ☑ A good ISMS can help you stay out of the news headlines and out of the courts.

Essential Guide To:

ISO 27001:2015

ISO CONSULTANTS
MAKING SENSE OF CERTIFICATION

What are the requirements of an ISO 27001:2015 Management System?

At the heart of ISO 27001:2015 is the information security management system (ISMS). This is a set of policies and procedures for systematically managing an organization's sensitive data, and that of its customers and suppliers. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the potential of a security breach and the impact of such a breach on your business.

An ISMS typically addresses employee behaviour and processes as well as data and technology. It should be implemented in a comprehensive way that becomes part of the company's culture, though if really necessary it can be designed to cover only certain parts of an organisation by restricting the scope of the system.

ISO 27001 is a specification for creating an ISMS. It does not mandate a specific format for the system, but it does have mandatory requirements for documentation, internal audits, continual improvement, and corrective and preventative action. It is a framework and template for your company to create its own truly bespoke system.

What Are the Key Areas of Focus?

Clauses. The broad and strategic view.

ISO 27001 follows a similar layout and structure as ISO 9001 and other standards which have adopted an internationally agreed template called the Annex SL structure; this structure breaks a management system standard down into several high-level sections. These structures target different aspects of a business and utilise clauses to integrate your management system (the ISMS) into all aspects of your business. The intention of this is that your management system becomes a living, breathing part of your business and not just a set of irrelevant procedures sitting in the background used as a tick-box exercise for your IT department once a year.

This overriding structure of ISO 27001; Annex SL is broken down into the following:

"The Context of The Organisation"

Simply, as a company:

"Who are we, what do we do and how do we do it"

"What are our aims?"

"What our key products and services?"

"Who are our customers and other affected parties (summarised)?"

"What are the limits of our management system (the scope or boundaries of where we wish to apply ISO 27001)?"

Essential Guide To:

ISO 27001:2015

ISO CONSULTANTS
MAKING SENSE OF CERTIFICATION

Leadership

This section covers defined and agreed roles and responsibilities within the business. This clause ensures that someone takes ownership of the ISMS from a supervisory position at a senior level but also lets you clearly layout and distribute responsibilities and ownership across all roles within the business.
Senior Management involvement is a vital aspect of this standard as there needs to be "buy in" to it at the highest level; this is because a good ISMS will affect all levels of management and the core operation of your business.

Planning

Having defined what your company actually does, and to whom, and what the risks and opportunities are, this section evaluates the impact of risks, and how to control them. It also considers setting quality objectives, as well as detailed plans of how these will be achieved. Who is responsible, and what time scales are involved? Finally, but crucially, it defines guidelines for managing changes.

Support

How can the resources required to complete tasks be controlled and measured? How do you know the method of measurement is known to be accurate? Which key people have mission-critical knowledge about your organisation's data management system? What are the levels of skill and awareness in your enterprise for what needs to be achieved? How are vital information and documents controlled?

Operation

The Operation section is aimed at covering what processes you have in place and how you manage them.

How do we plan and control the running of our business?
Broadly, how exposed is our current information? How do we currently protect it?

...and...

What are the resources required to achieve this? How do we measure if it's actually happening?

This develops into how you go about generating an Information Security Risk Assessment, and is then followed by how you address/treat/deal with the risks identified for your business.

Performance Evaluation

How do you know if the ISMS has delivered what was intended? Who checks it, and how? How do you know if customers are satisfied? How are internal audits conducted, what is the input of senior management to the ISMS and whole process? How do you intend to develop the business further, and what is the impact on the security of the information you have, or may have in the future?

Improvement

How do we improve, and stop things going wrong? How do we implement corrective actions when necessary, and continually improve your quality management system, keeping records as required?

Essential Guide To:

ISO 27001:2015

ISO CONSULTANTS
MAKING SENSE OF CERTIFICATION

Controls. Specific and Tactical.

Beyond the clauses used within the structure of the standard; ISO 27001 contains a list of 114 individual security controls relating to specific actions and processes your business needs to respond to. This list is called 'Annex A'. Don't panic though; although they all require a response, some may not be applicable to your business and you are probably already addressing some of the other controls, it just needs to be defined or documented.

The Annex A, ISO 27001:2013

Annex A specifies security related controls that cover many aspects of your business, without going into excessive detail, the area's these cover are:

- A.5: Information security policies (2 controls)
- A.6: Organization of information security (7 controls)
- A.7: Human resource security – (6 controls)
- A.8: Asset management (10 controls)
- A.9: Access control (14 controls)
- A.10: Cryptography (2 controls)
- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls)
- A.13: Communications security (7 controls)
- A.14: System acquisition, development and maintenance (13 controls)
- A.15: Supplier relationships (5 controls)
- A.16: Information security incident management (7 controls)
- A.17: Information security aspects of business continuity management (4 controls)
- A.18: Compliance; legal & Regulatory (8 controls)

What are the Practical Steps to ISO 27001 Certification?

Understand what it is! Is it simply a certificate on a boardroom wall gained after an auditor's visit? Is it purely the responsibility of the IT department? One common belief is that a single software package can magically generate certification. Misconceptions are common. We've blogged on the common mistakes, and why ISO 27001:2013 fails. Successful certification means that an effective ISMS serves your organisation's aims and is proven to help you do better business

Prepare your organization! Broadly define the "why", "what" and "how".

Gain commitment from senior management. The project needs to be driven by senior leadership. Integration of the ISMS in normal business life is essential. ISO 27001 is not a bolt-on, nice-to-have, IT-centric supplement to the main activities of your business. Successful implementation comes only through sound commitment from senior management. Hopefully, consideration of the standard's clauses makes this clear.

Essential Guide To:

ISO 27001:2015

ISO CONSULTANTS
MAKING SENSE OF CERTIFICATION

Gap Analysis

Simply, "Where are we – where do we need to be" in respect of your current information security management procedures. There are "gap analysis checklists" available for this task. Alternatively, use an external auditor (an ISO consultant) to carry this out.

Project Plan. Goals and timescales!

Here are some areas to consider:

- ☑ When will you start your ISMS implementation project?
- ☑ When do you want/need to complete implementation?
- ☑ What gaps exist in your existing procedures, and how long will they take to address?
- ☑ What resources are available or lacking?

Training

Training generates awareness and ownership, encourages participation. It should aid success! Potential parties to train:

- ☑ Project Manager(s)
- ☑ Team Leaders
- ☑ All significant employees, teams and internal auditors

Documentation

Create your ISMS starting from how you address the Annex A controls! Off-the-shelf software may help here.

Use and Improve the ISMS

Start using your ISMS ahead of a certification audit! Fine-tune or redesign as required. Conduct internal audits, management review meetings, and keep records.

Internal Audits

A test-run before 'The Big Day' of the external audit. An impartial third-party (such as your friendly ISO Consultant) should look for conformity, effectiveness, and potential non-compliance. You could even train up your own team of internal auditors. We can help with that, too.

ISO Registration

After running your ISMS for 2-3 months, it's time to arrange an external audit from a certification body. Again, your ISO Consultant should be able to assist with this.

Essential Guide To:

ISO 27001:2015

What is the cost of ISO 27001 certification? How prepared are you?

This determines the number of external consultant's days required. Alternatively, if you have sufficient in-house expertise, then a "certification toolkit" may work for you. We offer several options, with varying levels of help desk remote support.

The next stage?

If you've read this far, well done! We pride ourselves in our straightforward, practical and (occasionally) painfully honest approach. We want to make simple what others tend to make complex.

If it sounds like we could work together, please get in touch!

We can help you achieve certification in any one of three ways: