CAMBRIDGE RISK SOLUTIONS

ISO 27001 Implementation Tips

With ever greater concerns about cyber security and data breaches, and changes to the data protection regulations, businesses are more aware of the steps that they need to take to protect information security. This is demonstrated by the global growth in the number of ISO 27001:2013 certificates that have been issued by accredited certification bodies. According to the latest figures available from the International Organisation for Standardisation (ISO), there were 31,910 certificates in place in 2018.

Interestingly, China holds the highest number of certificates by a significant degree (7199). Japan comes second, with 5093, followed by the UK with 2444. Surprisingly, the US has a significantly lower number, 911, but this low uptake is reflected in all management standard certification, so is not unique to information security.

If an organisation does decide to take the step towards certification, how to proceed will depend largely on your budget, staffing arrangements, whether you employ business continuity specialists, and the size/nature of your organisation. However, I have given some top tips for those of you thinking about gaining certification.

Why go for ISO 27001?

I do not intend to explore the ‘why?’ in great depth; the fact that you have chosen to read this article suggests that you are more interested in how to implement ISO 27001 rather than why! Suffice to say that, for most of the organisations that I work with, the drive towards ISO 227001 has been largely driven by customer requirements, particularly those dealing with patient identifiable data (PID). Organisations are gaining a better understanding of the requirements to look after their data and that of their customers. This requirement is being pushed down the supply chain, needing suppliers to provide reassurance that data is being handled to an equivalent or higher standard. Additionally, organisations require reassurance that any incidents will be rapidly escalated and communicated in order to enable an effective response.

Holding ISO 27001 certification demonstrates that the processes and procedures are in place to ensure an effective Information Security Management System (ISMS). It also assists in completion of tender questionnaires; as an example, one that I completed today stated that if you had certification, you did not need to answer the remaining 90 or so questions, or provide any documentary evidence.

Additionally, my clients all have found that the changes that were required to implement the standard have resulted in greater confidence that they ‘are doing things right’, and, in one instance, it has resulted in an improved working environment, albeit with quite a culture-shock with the transition to a clear desk policy!

How to Implement ISO 27001?

The following points are an outline guide to help you move towards certification to ISO 27001:

Read The Standard

This may seem to state the obvious, but it is staggering how often it is apparent that the standard has not been read, let alone understood. Simple tips include:

- When the standard states ‘should’ then this has to be done;
- When there are a number of sub-clauses, each of them has to be addressed; and
- When the standard asks for a process or procedure, then one has to be defined.

Additionally, ensure that you understand the terminology; the standard is written to be directly translated into almost 40 languages, thus ‘documented information’ is what you may call ‘records’, and ‘stakeholders’ are now ‘interested parties’.

Follow the Standard

You would be surprised at the number of organisations that I have worked with who have decided that a particular clause is not relevant to their organisation, or who have decided not to progress with some elements of the standard. You need to address every clause. You additionally need to address each of the Reference Control Objectives and Controls, and document these in your Statement of Applicability. There are 114 controls in 14 groups, such as human resource security, physical and environmental security, asset management and information security incident management. It is worth noting that there is a degree of overlap in many instances, and the controls for one of the groups may equally provide control in another area.

You will need to decide which of these controls are required for your organisation, and give justification for their inclusion or exclusion. There are a number of controls that would be difficult for any organisation to exclude such as information security incident management, information security continuity, human resource continuity or asset management. For those areas that are outside your control, such as in the case where IT services may be outsourced, then the direct responsibility for the implementation lies with the supplier. However, in these instances, the ownership of the risks will still lie with you and, therefore, the oversight of those controls will then come under A.15 Supplier relationships, which should then ensure that satisfactory controls are in place.

For a better understanding of what may be required for each control, ISO 27002 gives detailed guidance. If you are not sure, you may wish to get help from information security professionals.

Integrate the Management System

If you already operate management systems, so have processes in place for internal audit, management review, etc, then consider merging elements of the system together. Take care to ensure all the aspects of the information security requirements are included, but integrating systems will make it easier to manage, and helps to demonstrate embedding in your own organisational culture.

Use the Management System

For those that are new to Management Systems, they can seem quite time-consuming and complex. However, it is these systems that help drive your ISMS forward, and ensure Continual Improvement. The systems are not just there for show! They are a powerful tool, so use them!

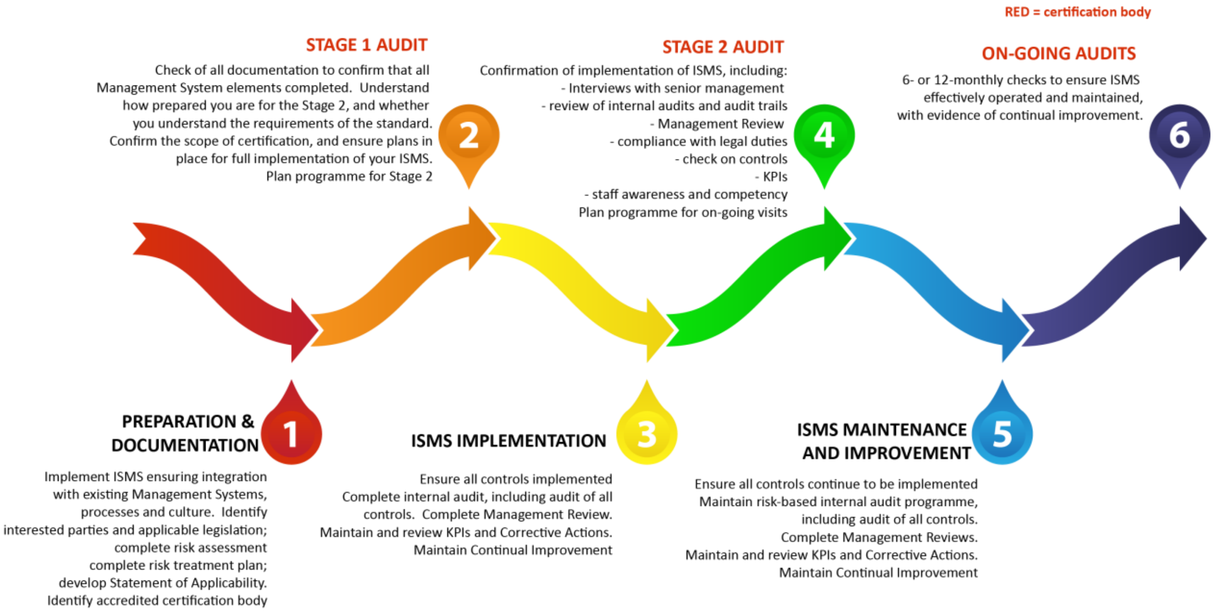
Keep it simple

Management systems should not be about creating significant additional work to make life easier for an auditor, and the more documents that you create, the more that have to be managed and controlled. Consider what best suits your organisational structure.

Understand the Certification Process

Accredited certification bodies will follow a similar process; the time required will depend on the size of your organisation, and will usually require at least a month between Stage 1 and Stage 2 assessments. You should also note that it may take a few weeks or even months before the first visit.

ISO 27001 CERTIFICATION PROCESS



RED = certification body

1 PREPARATION & DOCUMENTATION

Implement ISMS ensuring integration with existing Management Systems, processes and culture. Identify interested parties and applicable legislation; complete risk assessment complete risk treatment plan; develop Statement of Applicability. Identify accredited certification body

2 STAGE 1 AUDIT

Check of all documentation to confirm that all Management System elements completed. Understand how prepared you are for the Stage 2, and whether you understand the requirements of the standard. Confirm the scope of certification, and ensure plans in place for full implementation of your ISMS. Plan programme for Stage 2

3 ISMS IMPLEMENTATION

Ensure all controls implemented Complete internal audit, including audit of all controls. Complete Management Review. Maintain and review KPIs and Corrective Actions. Maintain Continual Improvement

4 STAGE 2 AUDIT

Confirmation of implementation of ISMS, including:
- Interviews with senior management
- review of internal audits and audit trails
- Management Review
- compliance with legal duties
- check on controls
- KPIs
- staff awareness and competency
Plan programme for on-going visits

5 ISMS MAINTENANCE AND IMPROVEMENT

Ensure all controls continue to be implemented Maintain risk-based internal audit programme, including audit of all controls. Complete Management Reviews. Maintain and review KPIs and Corrective Actions. Maintain Continual Improvement

6 ON-GOING AUDITS

6- or 12-monthly checks to ensure ISMS effectively operated and maintained, with evidence of continual improvement.

And finally…..Get Help

If you are not sure, then get help from others. The certification bodies offer pre-certification visits, which will do a sanity check of your documentation and confirm your readiness to proceed to certification. A number of consultancies will offer a similar service, but will also be in a position to offer consultancy within any such visits which will assist in your understanding of the standard and the development of your plan. Equally, if you want to implement information security and/or gain certification, and do not have the expertise in-house, then get help early.

I have briefly outlined some of the reasons for striving for certification, and have then looked at some key points for a successful certification. This short article does not seek to be a detailed guide to the route to certification. However, by following some of the points listed, I hope your certification journey is simplified.