

Should you be ISO/IEC 27001 Certified?



ISO/IEC 27001 is the internationally recognised specification standard for information security management. The implementation of an information security management system along the lines of this Standard is certainly good practice, and in these days of increasing cybercrime should be considered as common sense.

Areas covered by the Standard include:

- Risk assessment
- Security policy – management direction



- Organisation of information security – governance of information security
- Asset management – inventory and classification of information assets
- Human resources security – security aspects for employees joining, moving and leaving an organisation
- Physical and environmental security – protection of the computer facilities
- Communications and operations management – management of technical security controls in systems and networks
- Access control – restriction of access rights to networks, systems, applications, functions and data
- Information systems acquisition, development and maintenance – building security into applications
- Information security incident management – anticipating and responding

appropriately to information security breaches

- Business continuity management – protecting, maintaining and recovering business-critical processes and systems
- Compliance – ensuring conformance with information security policies, standards, laws and regulations

Why certify?

Certification against the Standard is not a process to be undertaken lightly. Whilst actual certification is often not strictly necessary, there are a number of valid reasons to obtain certification. These include:

- Organisational assurance
- Service provider assurance
- Business trading partner assurance
- Demonstrable and effective way of showing appropriate information security in place
- Competitive advantage
- Reduce trade barriers – international acceptance
- Reduce costs of regulation, corporate governance etc.

The actual certification audit can only be performed by an accredited certification body. It may be combined

with certification against other management system standards (eg ISO/IEC 9001, BS 25999).

The certification process

The certification process depends to some extent on the certification body employed. However in practice there are three stages for the initial assessment.

Stage 1 – Desktop review

- Security policy
- Risk assessment
- Risk treatment plan
- Statement of applicability
- Statement of scope
- Documented procedures
- Required records (eg asset register, role profiles, etc.)

Stage 2 – Implementation audit

- Interviews
- Evidence

Stage 3 – Conclusion

- Recommend certification
- Recommend certification after completion of an action plan

- Partial re-audit
- Complete re-audit

Ongoing audits

- Surveillance audits over a 3 year period
 - In addition to internal audits etc. (which may be performed by Kingston Smith Consulting if required)
 - Annually, or every 6 or 3 months
 - First one usually 3 months after certification audit, to ensure that required remediation is in place
- Triennial audit
 - Similar to the original certification audit

Gap analysis

It is highly advisable to perform a gap analysis well in advance of the Stage 1 audit. To avoid a conflict of interest, this must not be performed by anyone connected with the certification body.

The gap analysis will:

- Assist with statement of applicability
- Assist with definition of scope
- Identify deficiencies
- Recommend action plan
- Assist with action plan implementation (eg writing policies, defining controls, etc)

The number of controls to be assessed and the size of the scope of the certification are the greatest factors in the overall cost of certification – both financially and in terms of resources.

Kingston Smith Consulting employ qualified and experienced ISO 27001 Lead Assessors who are completely familiar with the certification process. They will ensure that you are in the best position to pass the certification audit first time. Recommendations are always cost-effective and based on the needs and culture of your organisation. Our consultants work with your staff where possible, to transfer relevant skills.

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010 info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD