Feb 2005

ISO 27001 "Information Technology - Security Techniques"

- *Is the Sleeping Giant Awakening?*

What is it?

BS 7799 entitled "Information Security," soon to become ISO 27001 "Information Technology - Security Techniques - Information Systems - Requirements" is a very broad document affecting the whole organisation not just the IT department. Included within the standards are requirements covering all the resources a company might use to control information, physical, human, equipment, electronic data and activities to meet your legal obligations.

Until last year companies seeking approval to the standard were relatively low but during the last twelve months the number of companies approved has doubled to over 200 in the UK and 1000 worldwide. Based upon enquires and companies currently seeking approval both in the UK and overseas this trend looks as if it will continue into the foreseeable future with a potential greater than ISO 9001 standard for quality systems.

There is no clear reason for this trend and it is probably a combination of many things, competitors obtaining approval, organisations seeing a market advantage from being "1st in their sector" and the number of market sectors now requiring a statement on compliance is increasing. For example the Data Protection Act, local government, MoD, Law Society, Health Authorities, FSA, Home Office and the police forces and even insurance companies when recalculating your business policies. You may also find you are now asking for evidence not just a tick in the box.

The standard has been around approximately 10 years and is considered by some to be complex and difficult to implement/obtain approval to. This has lead to a perception of high costs to introduce and certainly some consultants and training organisations have presented an elaborate picture of the subject to justify their charges. It is actually relatively straight forward as the standard describes common sense and many requirements your organisation will have already addressed, therefore the costs should be relatively low.

How does it affect me and can I avoid it?

Most companies will have needed to address the underlying issues or they would not be in business today, what the standard does is to require the subject is addressed in a structured way. Can you avoid the subject **no**, unless you do not have any records, hard copy or electronic or deal with any of the bodies described above. Can you avoid meeting the

BS7799/ISO 27001 requirements **yes** but it will make tenders and ITT's more difficult to respond too, the risk you take is that you do not know the size of the risk to your business.

It is a useful exercise, approval is a target to measure against and leave you with one less unknown for your business. This exercise may identify weaknesses, it will provide management with confidence and accountability within the organisation. Whilst buying insurance might protect you against the financial costs of and disaster affecting your IT system, it is unlikely to cover you for the impact in disruption, loss of business and customer confidence, introducing ISO 27001 requirements will rediuce the impact.

What does the standard require?

There are actually two standard ISO 27001:2005 "Information Security" which is the high level requirements for a system, processes, documentation, reviews, audits etc and ISO 19977:2005 which provides guidelines on the subjects that could be addressed. Within ISO 27001 there is a requirement for a "Statement of Applicability" of the subjects of ISO 19977. The statement of applicability does not mean you must do everything only that you have considered each subject and how it affects your business and assessed the residual risk after taking any action, if any. What action you take will depend on your business, a bank, a doctors surgery and a manufacturing organisation for example would all see different threats and would be dealing with different levels of technology so the requirement is that the controls are **appropriate** to the business.

The standard looks for control in several ways, take confidentiality, this is not just for data protection purposes but generally how do you ensure your company and your clients data is not accessible to any-one who could misuse the data There are many ways people could obtain the information for example details of a new product being developed or acquisition from a casual conversation in a pub, at an interview for another job, through loss of a laptop whilst travelling or a break-in. Deliberate high tech hacking whilst having the highest profile is the least likely for most of us and certainly trying to keep up with the latest technology is difficult and would probably not be cost effective. So what are the risks and what are reasonable precautions?

Disasters are an issue with an increased profile since 9-11 but floods, fire, break-ins can all have a major impact on the business and possibly a disaster in a neighbouring building could affect access, deliveries reaching you. A hole dug in the main road near my office meant a loss of telephone lines for several days, peaceful, no phone calls or emails but a significant delay in sending information to customers and how much new business did I loose?

What do I have to do?

Major elements that you will need to cover are having an asset register for all types of assets not just the financial assets, undertake a risk assessment to identify the impact of the risks to the business, develop procedures and practices to reduce the risk and a business continuity plan to deal with the residual risks. These all need to be brought together in a documented

Security Management System with a defined policy and objectives. Finally you will need to be able to demonstrate that you maintain the system through regular review of objectives, audits, problems that have occurred and review of the risk assessment to identify areas for improvement.

How do we obtain approval?

Most of the organisations that provided ISO 9001 approval also offer ISO 27001 approval and the process is very similar, the same documentation can be used and a combined assessment to both standards is available.

What is the next step?

The next step is the first step which is to undertake a gap analysis, the subjects given in ISO 19977 prove a good agenda. Next prioritise the subjects that need improving. If you need help and a common sense approach then contact us by e-mailing sales@quality-is.co.uk or calling 020 8786 8828. Where ever possible we offer fixed price contracts.