ISO/IEC 27001:2005

The ISO/IEC 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. It sets the requirements for an Information Security Management System (ISMS) in order to conform to the standard.

BS7799 itself was a long standing standard, first published in the nineties as a code of practice. As this matured, a second part emerged to cover the management systems. It is this against which Certification is granted. Today in excess of a thousand certificates are in place across the world.

ISO/IEC 27001:2005 enhanced the content of BS7799-2 and harmonised it with other standards. A scheme has been introduced by various certification bodies for conversion from BS7799 certification to ISO/IEC 27001:2005 certification.

The objective of the standard itself is to "*provide a mode for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System*". The adoption of the standard should be a strategic decision.

Further, "*The design and implementation of an organisation's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organisation*".

The standard defines its 'process approach' as "*The application of a system of processes within an organisation, together with the identification and interactions of these processes, and their management*". It employs the PDCA (Plan-Do-Check-Act) model to structure the processes and reflects the principles set out in the Organisation for Economic Co-operation and Development (OECD) guidelines.

ISO/IEC 27001:2005 also lists a set of control objectives and controls. These are listed in Annex A and come from the ISO/IEC 27002:2005(previously ISO/IEC 17799:2005) information security standard.

In addition to control objectives and controls, ISO/IEC 27002:2005 also provides implementation guidance and other information.

The 3 ISMS Principles

The three ISMS principles, as with all Information Security, are Confidentiality, Integrity and Availability of information.

Benefits of an ISMS

Purpose:

- The implementation and certification of an ISMS offers rigorous analysis and documentation of key information processing activities

that may, for instance, identify opportunities to improve process efficiencies.
- The structured information security management framework incorporates elements of ISO 9000:2000 Quality Assurance and ISO 14001:2004 Environmental practices. Legal and regulatory compliance supports management's legal obligations and reduces liabilities.

Benefits are not necessarily limited purely to better information security. Other major benefits include:

- Increased reliability and security of systems (safeguarding assets)
- Improved customer and business partner confidence
- Improved business continuity
- Meeting customer certification criteria
- Improved management control (defining the level of security required)

Auditing by a Certification Body Benefits:

- Organisational assurance or an acceptable and risk-based level of information security being implemented that is regularly reviewed;
- 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.

Beneficiaries of a well-planned and well-implemented ISMS system are the organisation and its staff, suppliers, customers, and stakeholders.

Particular reference is made to:

Business Effectiveness – A well-managed, controlled and maintained ISMS can provide effective operation of a business, consistency or operation, and planned measurements within the system provides the need for continuous improvement and continuing customer satisfaction.

Better Image – Customers and potential customers, investors, the public, neighbours, legislators and employees. This can open up markets and bring in investments as well as lead to a more secure, efficient and happier workforce.

Cost Reductions – More efficient processes, reduced scrap quantities giving more space and reduced reject and scrap costs, less re-work, fewer complaints, reduced processing times, reduced insurance costs and reduced liabilities.

Better Trained and Knowledgeable Workforce – Enables the staff to contribute more and to become more involved in the processes that they are responsible for. They have a better understanding of the security of the processes they run, and can contribute to their control and improvement. The workforce appreciates better working practices as they get fewer problems. They are an asset to any organisation.

Certification – A marketing tool can be obtained, again making products and services more secure and acceptable to the customer, enabling advantage to be gained over competitors. It enables the organisation to advertise that it has a secure information management system, and reassures the customer, and investors, of the company's commitment to improve its performance. It also enables a more efficient system to be developed, through external assessment and identification of weaknesses.

Management Responsibilities

ISO/IEC 27001:2005 emphasises the key role that top management play in the information security management system. Top management shall create an environment where people become fully involved in an information security management system that can operate effectively, be reviewed and be improved. The 3 ISMS shall be used by top management as the basis of its role in directing and controlling operations. Top management shall be visible and provide leadership and direction to the operations of the organisation, focusing and directing the workforce in meeting the requirements of customer, and any other interested parties such as regulators.

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

- Establishing an ISMS policy;
- Ensuring that ISMS objectives and plans are established;
- Establishing roles and responsibilities for information security;
- Communicating to the organisation the importance of meeting information security objectives and conforming to the

information security policy, its responsibilities under the law, and the need for continual improvement;
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS;
- Deciding the criteria for accepting risks and the acceptable level of risk;
- Ensuring that internal ISMS audits are conducted; and
- Conducting management reviews of the ISMS.

ISO/IEC 27001:2005 requires that top management are audited for these items. Top management shall demonstrate their commitment by showing to the auditor evidence of how they have fulfilled their roles and led and directed the quality system. Auditors will need to look at the business policies, the measurement methods and results of reviews and actions taken.

Regency ITC ISO/IEC 27001:2005 Capabilities

All Regency's consultants are qualified ISMS Lead Auditors had have a wealth of experience in carrying out gap analyses and advising clients on how best to progress with their certification, producing the documentation required for certification, or simply advising clients who wish to improve their IA stance without progressing to full certification.

Regency ITC ISO/IEC27001:2005 Certified

Regency ITC doesn't only talk a good ISMS, in fact Regency ITC currently holds ISO/IEC27001:2005 Certification for its Managed Encryption Service, Secure Data Centre and its general office systems.

IS 548043

All ISMS documentation for this Certification was produced and is maintained for ongoing Certification by our own personnel.

Regency ITC ISO27001 Methodology

Regency are now in a position to carry out ISO27001 gap analysis work by using the fully automated tool 'Citicus One'; an award winning software package which Regency are the sole UK authorised implementers. The tool will allow the consultant to record evidential compliance or weakness in each control area and will also generate an action plan and advice detailing required remedial action. Once completed it will provide a full risk assessment against perceived risks and threats and can also include: Criticality Assessments, Business Impact Assessments (BIA) & Privacy Impact Assessments (PIA), all produced in an easy readable report which contains dashboard graphs that can be presented to the Board.

The use of Citicus One will not only reduce the time it will take to carry out the gap analysis process, the time utilised by in-house security practitioners or consultants but will also reduce the costs of maintaining a real time effective Information Security Management System that once adopted can be updated as and when required as and when the risks or threats change.

Regency ITC can host and manage Citicus One in our HMG accredited secure data centre and also provide the expertise to carry out independent evaluations. We can also arrange the training for personnel to use the software to maintain and update their risks and actions by using our hosting service via secure HMG VPN encrypted connections.