regency IT CONSULTING

- Encryption Services
- Security Consultancy
- Network Security
- Data Security
- Communications Security
- Protective Monitoring
- Project Management

//Assurance through Excellence

ISO/IEC 27001:2013

ISO/IEC 27001:2013 is an information security standard which was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in September 2013. It is a specification for an Information Security Management System (ISMS) and replaces ISO/IEC 27001:2005.

The ISO/IEC 27001 standard has been maturing since it was first published as a British Standard in 1995 as BS7799 and has gone through a number of iterations.

ISO/IEC 27002:2013 contains guidance which assists in the interpretation of the standard, ISO 27001:2013.

The implementation of ISO/IEC 27001 establishes an ISMS which is designed to preserve the Confidentiality[1], Integrity[2] and Availability[3] of an organisation's valuable information by applying a risk management process. This gives confidence to interested parties that risks are adequately managed. Its purpose is *"to provide requirements for establishing, implementing, maintaining and continually improving an information security management system"*[4].

So much of most organisation's value is embedded within information rather than physical assets. As information moves to be stored electronically rather than on paper, it can be more easily stolen, manipulated or deleted by those within or outside the organisation. The true value of implementing an Information Security Management System against the ISO/IEC 27001:2013 standard is that the risks against valuable information assets are proactively identified and managed.

Organisations which meet the specifications of the standard may be certified, against an explicitly defined scope, by an independent and accredited certifying body; often referred to as a Registering Body or Registrar.

Thousands of organisations are currently certified against the ISO/IEC 27001:2005 standard and as part of their continuing certification must migrate to the new version of ISO 27001:2013. For those that are new to the standard, or have an existing certification, there is no option to stay with the 2005 model, organisations will need to certify against the 2013 model on or before 30th September 2015.

Major 2013 Changes

The following section presents the major differences between the 2005 and 2013 version of the standard.

Structure

The Standard is now based on the "Annex SL" structure. This structure is that agreed for all future ISO Standards. Therefore the implementation of, for example, ISO 9001 for an organisation's Quality Management System (QMS), and ISO 14001, for an organisation's Environmental Management System (EMS) can be aligned into a single grouped management system. This could also reduce the resources required for auditing as this will mean a core set of generic requirements that need to be audited no matter which discipline is being examined. Annex SL-aligned updates to ISO 9001 and 14001 are expected to be released in early 2015. ISO 22301:2013 Business Continuity Management System (BCMS) has also already been published using the new structure.

Plan-Do-Check-Act?

Although Plan-Do-Check-Act was an explicit requirement in the 2005 Standard, in the 2013 Standard the requirement for "Continual Improvement" only implies relevance of the P-D-C-A cycle. If you look hard enough, the influence of the Deming Cycle can still be spotted (Context, Leadership, Planning and Support – Plan; Operation – Do; Performance evaluation – Check; and, Improvement - Act), even though it is not explicitly referenced any more.

Reduction of Controls

The standard's update has brought with it a number of changes, not least the more focused application of the control areas. Previously the standard required the consideration of 133 controls in 11 control groups,

[1] **Confidentiality** is the property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
[2] **Integrity** is the property of safeguarding the accuracy and completeness of assets - this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later.
[3] **Availability** is the property of being accessible and usable upon demand by an authorised entity.
[4] Source: BS ISO/IEC 27001:2013.

whereas the 2013 version considers only 114 controls in 14 groups.

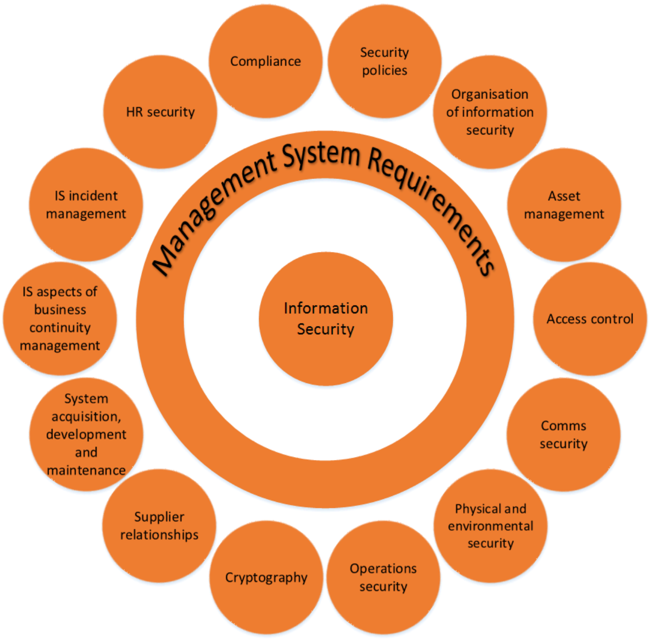
Management System Requirements
Information Security
Compliance
Security policies
Organisation of information security
Asset management
Access control
Comms security
Physical and environmental security
Operations security
Cryptography
Supplier relationships
System acquisition, development and maintenance
IS aspects of business continuity management
IS incident management
HR security

Figure 1 - 14 Control Groups of ISO/IEC 27001:2013

This reduction in controls does not dilute the security, rather the controls reflect changes to technology. For instance the popularity of the commoditised buying approach to cloud-based computing, the business need or desire of senior executives to access corporate information via their own mobile devices – and the consequential need to manage those devices in an appropriately secure manner, and of course the ever-changing threat landscape. The new standard also attempts to omit repetition that organisations may previously have had difficulties with.

Focus on 'Leadership'

Where as previously this area was encapsulated under 'Management commitment', ISO/IEC 27001:2013 has placed a new emphasis on the demonstration of *leadership* from top management.

ISO/IEC 27001:2013 requires that top management are able to evidence their contribution as part of a formal audit regime. Top management must demonstrate their continued commitment to the ISMS by showing to the auditor evidence of how they have fulfilled their roles, and led and directed the system. Auditors will review and test the business policies, measurement methods and results of reviews and actions taken.

Benefits of an ISMS

As previously discussed, the primary benefit of implementing ISO/IEC 27001:2013 in order to construct an ISMS is to identify risk to valuable organisational information and manage this risk in a structured way. It typically fills a gap within most organisations, where people have already identified strategic, financial, health and safety risks as their intrinsic value is readily understood, but have missed the value of the information that underpins the organisation and is subject to ever increasing threat as those who seek to gain a competitive advantage or do harm can easily attack an organisation over the Internet from a distance.

As part of the process of establishing an ISMS, the following additional benefits could also be realised:

- The analysis of information and systems could lead to the identification of process efficiencies.
- The standard's requirement to ensure that legal and regulatory obligations are met. This can reduce liability and provide assurance to auditors and stakeholders.
- Improved valuation of public and private companies as it can be recognised that the organisation has taken steps to protect its assets.
- Increased customer and partner confidence and support of your brand as a safe organisation to share information with.
- Minimise damage to reputation through preventing or decreasing the impact of the loss of confidentiality, integrity or availability of key information. It's distressing to see how many news articles continue to report lost information and the impact on a business from day to day when a good number of these incidents could be prevented.
- Improved services and business justification for the proper maintenance of information systems against business risk.
- Increased confidence in business continuity and disaster recovery arrangements;
- Meeting customer certification criteria;
- Improved management control.

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

Identifying the ISMS Scope

Regency strongly recommends against 'boiling the ocean'. Identify your business strategy, what information supports this strategy and how important this information is to internal and external stakeholders. Choose to start your ISMS against those assets that are most key to the organisation, and most likely your stakeholders. Cut your teeth on a manageable scope and then grow this through subsequent certification audits. This approach removes a lot of risk from most projects to establish an ISMS and delivers the benefits where it matters the most, early.

Regency ISO/IEC 27001 Capabilities

Regency's consultants are qualified ISO/IEC 27001:2013 Lead Auditors and have a history of providing our clients with high quality ISO/IEC 27001 services. Our past services for have included:

- helping organisations to arrive at the fundamental identification of the size and complexity of the scope of the ISMS within the context of their business strategy;
- leading projects to establish an ISMS within organisations, transfer skills to existing staff, ensure that information risk is managed effectively and help represent organisations to the certification auditor;
- helping organisation align against the standard so that impact and benefits can be analysed before proceeding to full certification; and,
- Provide accelerated improvement through our proven approach, methodologies and experience in order to cut the time and cost to deliver certification.

Regency ISO/IEC 27001 Certified

Regency doesn't only talk a good ISMS, Regency currently holds ISO/IEC 27001:2005 Certification for its Managed Encryption Service, Secure Data Centre and its general office systems and we are ready to migrate to ISO 27001:2013 on schedule in early 2015; the timeline being driven only by our external certification auditors, BSI.

IS 548043

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