Introduction to ISO/IEC 27001

ISO/IEC 27001 is an international standard on how to manage information security. ISO/IEC 27001 requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Information security is defined within the standard in the context of the CIA triad:

- confidentiality (ensuring that information is accessible only to those authorized to have access),
- integrity (safeguarding the accuracy and completeness of information and processing methods) and
- availability (ensuring that authorized users have access to information and associated assets when required).

The ISO/IEC 27001 certification like other ISO management system certifications, usually involves a three-stage external audit process:

- Stage 1 is a preliminary, informal review of the Information Security Management System (ISMS).
- Stage 2 is a more detailed and formal compliance audit independently testing the ISMS against the requirements specified in ISO/IEC 27001.
- Ongoing involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard.

ISO/IEC 27002 defines a set of controls that can be used when implement ISO2/IEC 27001. These are controls are defined as follows and each control can in turn be broken down into a set of sub controls. When creating a compliance statement for ISO/IEC 27001, you should define your response to each sub-control in ISO/IEC 27002 and say whether it is required by your ISMS and if it is required how it is implemented.

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance; with internal requirements, such as policies, and with external requirements/laws.