CONSULTRAIN
management services

ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

ISO 27001 is an international standard to manage information security. The standard was published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets more secure. Organizations that meet the standard's requirements can choose to be certified by an accredited certification body following successful completion of an audit. Most organizations have a number of information security controls. However, without an information security management system (ISMS), controls tend to be somewhat disorganized and disjointed.

ISO 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;
•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.

What controls will be tested as part of certification to ISO 27001 is dependent on the certification auditor. This can include any controls that the organisation has deemed to be within the scope of the ISMS and this testing can be to any extent as assessed by the auditor as needed to test that the control.
Management determines the scope of the ISMS for certification purposes and may limit it to, say, a single business unit or location. The ISO 27001 certificate does not necessarily mean the remainder of the organization, outside the scoped area, has an adequate approach to information security management. There are 114 controls in 14 groups & 35 control categories – eg. Information security policies (2 controls), Organization of information security (7 controls), Human resource security - 6 controls applied before, during, or after employment, Asset management (10 controls), Access control (14 controls), Physical & environmental security (15 controls), Operations security (14 controls), Communications security (7 controls) etc.

ISMS covers all types & sizes of organizations in all industries. The ISO 27001 certification, usually involves a three-stage external audit process defined by the ISO 17021 and ISO27006 standards:

•**Stage 1 i**s a preliminary, informal review of the ISMS, eg. checking the existence and completeness of key documentation such as the organization's information security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the auditors with the organization & vice versa.
•**Stage 2** is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO 27001. The auditors will seek evidence to confirm that the management system has been properly designed and implemented. Certification audits are usually conducted by ISO 27001 Lead Auditors. Passing this means the ISMS being certified compliant with ISO 27001.
•**Ongoing** involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended. These should happen at least annually but (by agreement with management) are often conducted more frequently, particularly while the ISMS is still maturing.