ISO 27001 Information Security Management Systems Lead Auditor

Introduction

This course enables participants to develop the necessary expertise to audit an information security management system (ISMS) and to manage a team of auditors by applying widely recognized audit principles, procedures and techniques. During this training, the participant will acquire the necessary knowledge and skills to proficiently plan and perform internal and external audits in compliance with ISO 19011 the certification process according to ISO 17011.Based on practical exercises, the participant will develop the skills (mastering audit techniques) and competencies (managing audit teams and audit program, communicating with customers, conflict resolution, etc.) necessary to efficiently conduct an audit. You will gain:

- An appreciation of the importance of controlling information security in all types of business
- A basic knowledge of information security management systems (ISMS) including the requirements of ISO 27001
- A basic knowledge of information security legislation
- An appreciation of documented management systems to control Information Security
- An appreciation of risk assessment for information security
- An understanding of the principal requirements for auditing IS management system

Who Should Attend?

Managers, Team Leaders, Line Managers, Superintendents, OE Champions, Quality and Project Managers, Supervisors, Executives, Internal and External Auditors, Members of IT Team, Health & Safety Managers, Risk Managers, Business Process Owners, Business Finance Managers, Business Risk

Managers, Regulatory Compliance Managers, Project Managers, Continuity, Risk, Quality, IT and Environmental Managers, Anyone involved in the system development, implementation and maintenance, Regulatory Affairs Managers, Consultants, Anyone who is involved in ISO standards

Course Objective

By the end of this course, delegates will be able to:

- Understand the fundamentals of information security
- Know the interrelationships between ISO/IEC 27001 and the other information security standards (ISO 27002, ISO 27003, ISO 27004, and ISO 27005)
- Know the key components of an information security management system (ISMS) in accordance with ISO/IEC 27001
- Introduce the concepts, approaches, standards, methods and techniques allowing to effectively manage an ISMS
- Understand the relationship between an information security management system, including risk management, controls and compliance with the requirements of different stakeholders of the organization
- Understand the stages of the ISO/IEC 27001 certification process
- Acquire the expertise to perform an ISO 27001 internal audit following ISO 19011 guidelines
- Acquire the expertise to perform an ISO 27001 certification audit following ISO 19011 guidelines and the specifications of ISO 17021 and ISO 27006
- Acquire the necessary expertise to manage an ISMS audit team
- Understand the operation of an ISO 27001 conformant information security management system
- Understand the relationship between an information security management system, including risk management, controls and compliance with the requirements of different stakeholders of the organization
- Improve the ability to analyze the internal and external environment of an organization, its risk assessment and audit decision-making

Course Outline:

- Introduction to information security management system (ISMS) concepts as required by ISO/IEC 27001
- Normative, regulatory and legal framework related to information security
- Fundamental principles of information security
- ISO/IEC 27001 certification process

- Information security management system (ISMS)
- Detailed presentation of the clauses 4 to 8 of ISO/IEC 27001
- Planning and initiating an ISO/IEC 27001 audit
- Fundamental audit concepts and principles
- Audit approach based on evidence and on risk
- Preparation of an ISO/IEC 27001 certification audit
- ISMS documentation audit
- Conducting an opening meeting
- Conducting an ISO/IEC 27001 audit
- Communication during the audit
- Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation
- Audit test plans
- Formulation of audit findings
- Documenting nonconformities
- Concluding and ensuring the follow-up of an ISO/IEC 27001 audit
- Audit documentation
- Quality review
- Conducting a closing meeting and conclusion of an ISO/IEC 27001 audit
- Evaluation of corrective action plans
- ISO/IEC 27001 surveillance audit
- Internal audit management program