



ISO 27001 Information Security Management System (ISMS)

Introduction

You simply can't be too careful when it comes to information security. Protecting personal records and commercially sensitive information is critical. ISO/IEC 27001 helps you implement a robust approach to managing information security (INFOSEC) and building resilience. Internationally recognized ISO/IEC 27001 is an excellent framework which helps organizations manage and protect their information assets so that they remain safe and secure. It helps you to continually review and refine the way you do this, not only for today, but also for the future. That's how ISO/IEC 27001 protects your business, your reputation and adds value. ISO/IEC 27001 is an internationally recognized best practice framework for an information security management system (ISMS). It helps you identify risks and puts in place security measures that are right for your business, so that you can manage or reduce risks to your information. By achieving ISO/IEC 27001 certification you can demonstrate that your ISMS meets international best-practice and show customers, suppliers, and the market place that your organization has the ability to handle information securely.

ISO 27001 standard provides a framework to assure the effectiveness of the information security measures in the work, this includes the continued accessibility, confidentiality and integrity of the information in whatever form it is held. This course enables participants to be familiar with the basic concepts of the implementation

and management of an Information security management system (ISMS) as specified in ISO 27001. The components of ISMS will be discussed in this course, including the ISMS policy, risk management, measuring performance, management's commitment, internal audit, management review and continual improvement.

The 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 course, 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. The participants will develop the skills (mastering audit techniques) and competencies (managing audit teams and audit program, communicating with customers, conflict resolution, etc.) necessary to

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 involved in implement an EMS implementation and maintenance, Technicians involved in operations related to an ISMS, Anyone who is involved in ISO standards, IT Professionals wanting to gain a comprehensive knowledge of the main processes of an Information Security Management System (ISMS), Staff involved in the implementation of the ISO/IEC 27001 standard, Expert advisors in IT, CEO and Senior Managers responsible for the IT governance of an enterprise and the management of its risks

Course Objectives:

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

- Be familiar with the basics of information security
- 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
- Know what an information security management system (ISMS) is and how it can help business
- Understand the development, history, and current status of ISO 27001
- Understand the registration process
- Estimate costs and resources to implement an ISMS
- Understand the available information security controls

Course Outline:

- Fundamental principles of information security
- Overview of what is meant by ISMS and the basic constituents of an ISMS
- Introduction to the ISO 27000 standards family Introduction to management systems and the process approach
- General requirements: presentation of the clauses 4 to 8 of ISO/IEC 27001
- Implementation phases of the ISO/IEC 27001 framework
- Introduction to risk management according to ISO/IEC 27005
- Continual improvement of information security
- Presentation of the standards ISO 27001, ISO 27002 and ISO 27003 and regulatory framework
- Explanation of how an ISMS can help
- General requirements: presentation of the clauses 4 to 8 of ISO 27001
- Identifying and evaluating assets
- Defining the scope of an ISMS
- Development of an ISMS and information security policies
- Selection of the approach and methodology for risk assessment
- Risk management: identification, analysis and treatment of risk
- Drafting the statement of applicability (SoA)
- Implementation phases of ISO 27001 framework
- Implementation of a document management framework
- Principles and design of information security controls
- Writing procedures
- Implementation of controls
- Incident management
- Operations management of an ISMS
- Conducting an ISO/IEC 27001 certification audit
- Documentation of an information security control environment
- Monitoring and reviewing the information security controls



- Development of metrics, performance indicators and dashboards
- ISO 27001 internal audit
- Management review of an ISMS
- Continual improvement of information security
- Implementation of a continual improvement program
- Preparing for an ISO 27001 certification audit
- Conducting an ISO 27001 certification audit
- Examples of implementation of information security controls based on ISO 27002 best practices