ISO 27005 Information Security Risk Management (ISRM)

Introduction

Organizations of all types are concerned by threats that could compromise their information security. These threats may take any form from identity theft; risks of doing business on-line all the way to theft of equipment or documents which could have a direct impact on businesses, with possible financial loss or damage, loss of essential network services etc.. This course will help you to understand the information security risks you face while implementing and operating an information security management system. This course allows the participants to familiarize themselves with the fundamentals of risk management related to information security using the standard ISO/IEC 27005:2011 as a reference framework. Participants will see different parts of a risk management program and the implementation stages of an optimal risk assessment. It should be noted that this course fits perfectly into the framework of a process of implementation of ISO 27001.

Risk assessment and management provides the foundation for internal controls management, as well as business continuity and disaster recovery management. ISO 27005 provides guidelines for information security risk management, it supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. In this course, participants develop the competence to master the basic risk management elements related to all assets of relevance for information security using the ISO 27005 standard as a reference framework. The objective of this course is to provide delegates with the specific guidance and advice to support the implementation of requirements defined in ISO/IEC 27001 that relate to risk management processes and associated activities. The course will provide delegates with a risk management framework for development and operation. This course enables participants to learn about the best practices in risk management based on ISO/IEC 27005, as well as understanding how different parts of a risk management program and the implementation stages of an optimal risk assessment are conducted. The course will feature:

- Description of information security risk assessment
- Information security risk management process overview
- Information security risk assessment approaches
- Asset identification and valuation
- Impact assessment
- Risk identification
- Risk analysis
- Threats identification and ranking
- Vulnerabilities methods for vulnerability assessment
- Risk estimation
- Risk evaluation
- Basic risk criteria
- Risk evaluation criteria
- Risk impact criteria
- Risk acceptance criteria
- Risk treatment
- Risk reduction
- Risk retention
- Risk avoidance
- Risk transfer
- Monitoring and review of risk factors
- Risk management monitoring, reviewing and improving

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, Staff organizations implementing or seeking to comply with ISO 27001 or involved in a risk management program, IT Professionals wanting to gain a comprehensive knowledge of risk management within an organization, Staff involved in the implementation of the ISO/IEC 27005 standard

Course Objectives:

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

- Understand the basics of the implementation, management and maintenance of an ongoing risk management program
- Introduce the concepts, approaches, standards, methods and techniques allowing an effective management of risk
- Interpret the requirements of ISO 27001 on information security risk management
- Understand the relationship between the information security risk management, the security controls and the compliance with the requirements of different stakeholders of an organization
- Understand the role and importance of risk management in an organization
- Know why risk management is the core competence of information security management
- Understand the concepts, approaches, methods and techniques allowing an effective management of risk according to ISO 27005
- Interpret the requirements of ISO 27001 on information security risk management
- Understand the relationship between the information security risk management, the security controls and the compliance with the requirements of different stakeholders of an organization
- Acquire the competence to effectively advise organizations on the best practices in information security risk management
- Understand risk management approaches in accordance with ISO/IEC 27005
- Know the concepts, approaches, standards, methods and techniques allowing effective risk management based on ISO/IEC 27005

Course Outline:

- Why ISO 27005?
- Scope of ISO 27005
- Introduction to the ISO/IEC 27000 family of standards
- Introduction to management systems and the process approach
- Fundamental principles of risk management
- Concepts and definitions related to risk management
- Standards, frameworks and methodologies in risk management
- General requirements: presentation of the clauses 4 to 12 of the ISO/IEC 27005
- Implementation phases of the ISO/IEC 27005 framework
- Continual improvement of risk management
- Conducting an ISO/IEC 27005 certification audit
- Implement a risk management program
- Risk identification and risk analysis
- Risk evaluation and risk treatment
- Acceptance of risk and management of residual risks
- Communicating, monitoring and controlling risk
- Risk management standards, frameworks and methodologies
- Implementation of an information security risk management program
- Understanding an organization and its context
- ISMS overview
- Major differences in ISMS approaches
- Recommended approach
- Points to consider
- Introduction to the landscape of risk
- Asset landscape
- Threat landscape
- Controls landscape
- Loss (impact) landscape
- Vulnerability landscape
- What information is necessary for risk analysis?
- Define the context for information risk management
- Risk identification and risk analysis
- Introduction to risk assessment methodologies
- Risk assessment with a quantitative method
- Determine the appropriate information risk treatment plan
- Develop an information security risk communication plan
- Describe the information security risk monitoring and review plan