

## **ISO 27001 Lead Implementer (5 days)**

**Mastering the implementation and management of an Information Security Management System (ISMS) based on ISO 27001**

### **Summary**

This five-day intensive course enables the participants to develop the expertise to support an organization in implementing and managing an Information Security Management System (ISMS) based on ISO/IEC 27001:2005. Participants will also master the best practices to implement information security controls from all areas of ISO 27002. This training is consistent with the good practices of project management established in ISO 10006 (Quality Management Systems - Guidelines for Quality Management in Projects). This training is fully compatible with ISO 27003 (Guidelines for the Implementation of an ISMS), ISO 27004 (Measurement of Information Security) and ISO 27005 (Risk Management in Information Security).

### **Who should participate?**

- Project managers or consultants wanting to prepare and to support an organization in the implementation of an Information Security Management System (ISMS)
- ISO 27001 auditors who want to master the Information Security Management System implementation process
- Persons responsible for the information security or conformity in an organization
- Members of an information security team
- Expert advisors in information technology
- Technical experts wanting to prepare for an information security function or for an ISMS project management function

### **Learning objectives**

- Understanding the application of an Information Security Management System in the context of ISO 27001
- Mastering the concepts, approaches, standards, methods and techniques required in an effective management of an Information Security Management System
- Understand the relationship between the components of an Information Security Management System, including risk management, controls and compliance with the requirements of different stakeholders of the organization
- Acquiring the necessary expertise to support an organization in implementing, managing and maintaining an ISMS as specified in ISO27001
- Acquiring the necessary expertise to manage a team implementing the ISO27001 standard
- Develop the knowledge and skills required to advise organizations on best practices in management of information security
- Improve the capacity for analysis and decision making in a context of information security management

### **Course details**

#### **Day 1: Introduction to the management of an Information Security Management System (ISMS) based on ISO 27001 and launching an ISMS**

- Introduction to management systems and the process approach
- Presentation of the standards ISO 27001, ISO 27002 and ISO 27003 and regulatory framework
- Fundamental principles of Information Security
- Preliminary analysis and determining the level of maturity of the existing information security management system based upon ISO 21827

## **Training Outline**

- Writing the business case and preliminary design of the ISMS
- Developing a project plan of compliance to ISO 27001

### **Day 2: Planning an ISMS based on ISO 27001**

- Defining the scope of the ISMS
- Drafting the ISMS and information security policies
- Selection of the approach and methodology for risk assessment
- Risk management according to ISO 27005: identification, analysis and treatment of risk
- Drafting the Statement of Applicability

### **Day 3: Launching and implementing an ISMS based on ISO 27001**

- Implementation of a document management framework
- Design of controls and writing procedures
- Implementation of controls
- Development of a training & awareness program and communicating about the information security
- Incident management according to ISO 27035
- Operations management of an ISMS

### **Day 4: Control, act and the certification audit of the ISMS according ISO 27001**

- Monitoring the ISMS controls
- Development of metrics, performance indicators and dashboards in accordance with ISO 27004
- ISO27001 internal Audit
- Management review of the ISMS
- Implementation of a continuous improvement program
- Preparing for the ISO 27001 certification audit

### **Day 5: Exam**

## **Prerequisites**

ISO 27001 Foundation certification or a basic knowledge of ISO 27001 and ISO 27002 is recommended

## **Educational approach**

- This training is based on the alternation of theory and practice:
  - Sessions of lectures illustrated with examples based on real cases
  - Practical exercises based on a full case study including role plays and narrative presentation
  - Review exercises to assist the exam preparation
  - Practice test similar to the certification exam
- Given the practical exercises, the number of training participants is limited

## **Examination and certification**

- The “ISO 27001 Lead Implementer” exam fully meets the requirements of the PECB Examination Certification Programme (ECP). The exam covers the following competency domains:
  - Domain 1: Fundamental principles and concepts of information security
  - Domain 2: Information Security Control Best Practice based on ISO 27002
  - Domain 3: Planning an ISMS based on ISO 27001
  - Domain 4: Implementing an ISMS based on ISO 27001
  - Domain 5: Performance evaluation, monitoring and measurement of an ISMS based on ISO 27001
  - Domain 6: Continuous improvement of an ISMS based on ISO 27001
  - Domain 7: Preparing for an ISMS certification audit
- The “ISO 27001 Lead Implementer” exam is available in different languages (the complete list of languages

**Training Outline**

can be found in the examination application form)

- Duration of the exam: 3 hours
- After successfully completing the exam, participants can apply for the credentials of ISO27001 Provisional Implementer, ISO27001 Implementer or ISO27001 Lead Implementer, depending on their level of experience
- A certificate will be issued to participants who successfully passed the exam and comply with all the other requirements related to the selected credential

**General Information**

- Certification fees are included in the examination price
- A student manual containing over 450 pages of information and practical examples will be distributed to participants
- A 31 CPE (Continuing Professional Education) participation certificate will be issued to participants