ISO/IEC 27001:2013 Foundation/Practitioner

How to ensure world-class information security management in your organisation

Duration: 3 Days

The adoption of an Information Security Management System (ISMS) is a strategic decision driving the coordination of operational security controls across all of the organisation's electronic and physical information resources.

ISO/IEC 27001:2013 is the most widely recognised international standard for information security management.

ISO 27001 provides:

- a globally-accepted best-practice framework for the protection of information assets
- assurance to external customers who increasingly are demanding evidence of security and compliance.

This 5-day certificate course is fully accredited by APMG and is based on the most recent (2013) version of the ISO/IEC 27001 standard. It comprises two modules which can be taken separately or combined, according to needs.

The first or **Foundation module** (2 days) is designed for anyone who needs an overview of the ISO 27001 Standard and an appreciation of what comprises best practice in an Information Security Management System.

The full 5-day **Practitioner course** is designed for anyone who needs a deep understanding of how to actually apply the ISO 27001 standard for implementation, management and improvement of the ISMS. It is for those involved in the planning, design, transition and operation of an ISMS to satisfy the requirements of ISO 27001 e.g. manager for an ISO 27001 implementation project, process owner, asset manager.

Learning Outcomes

- Understand the concepts, key terms, standards, methods and techniques required within ISO 27001 for the effective management of an ISMS
- Understand the relationship between the components of an ISMS, including risk management, controls and compliance with the requirements of different stakeholders
- Acquire the expertise to implement, manage and maintain an ISMS as per ISO 27001
- Understand what is required to manage a team implementing the ISO27001 standard
- Improve information security through adoption of best practices.
- Establish a structured approach to information security management to secure information assets.
- Recognise the purpose of internal audits and external certification audits, their operation and the associated terminology.
- Gain a competitive differentiator when tendering for business contracts.
- Enhance reputation with the secure management of confidential and sensitive information.

Course Contents

1. Overview of ISO 27001

- The key standards in the ISO/IEC 27000 series
- Compatibility of ISMS with other management system standards
- Definitions of terms

2. Leadership and support of the ISMS

- Requirements to manage an ISMS
- Integration of the ISMS with the organisation's processes and management structure
- Requirements of top management
- Requirements for documentation
- Requirements for processes and content
- Requirements for the ISMS policy

3. Planning and operation of the ISMS

- Monitoring, measurement, analysis and evaluation
- Requirements for continual improvement of the ISMS
- Actions to address risks and opportunities
- Defining and applying the risk assessment process
- approaches to risk treatment
- Selection of controls
- risk monitoring and review
- Information security objectives
- development steps for performance evaluation
- Internal audit of an ISMS
- Management review of the ISMS

4. Information security control objectives and controls

- The structure and contents of the controls and control objectives
- Information security policies
- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Business continuity management
- Compliance

5. Achieving ISO/IEC 27001 Certification

- Types of audits – initial, re-certification, surveillance, internal
- Evidence used to demonstrate conformity

6. Review, exam prep, Certificate exam