

# ISO/IEC 27001:2013

## Foundation

What you need to know about best practice in information security management



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 specifically aimed at information security management.

This 2-day Foundation Course is designed for anyone who needs a solid overview of the Standard and an appreciation of what comprises best practice in an Information Security Management System.

Fully accredited by APMG, and based on the most recent (2013) version of the ISO/IEC 27001 standard, the course is 2 days in duration with the Foundation exam being held the morning after the course.

A Practitioner course (3 days) is also available for those requiring a deeper understanding about how to actually apply the standard for implementation, management and improvement.

ISO/IEC 27001 is an international standard that provides the basis for effective management of confidential and sensitive information and the application of information security controls.

It enables organisations to demonstrate excellence and prove best practice in information security management. Conformance with the standard requires commitment to continually improve control of confidential and sensitive information, providing reassurance to sponsors, shareholders and customers alike.

### Who Should Attend

ISO/IEC 27001 certification is designed for management and support personnel involved in the design, delivery, maintenance and improvement of an ISMS and supporting resources, equipping them with an understanding of the application of this best practice, internationally-recognised standard.

### Learning Outcomes

#### Benefits for Individuals

- Learn about best practice in Information Security Management and apply this within your organisation.
- Realise the scope and purpose of the standard and how it can be implemented within an organisation.
- Understand the key terms and definitions used in ISO/IEC 27001 to effectively roll out the principles.
- Leverage the fundamental ISO/IEC 27001 requirements for an ISMS to address the need to continually improve.
- Recognise the purpose of internal audits and external certification audits, their operation and the associated terminology.

#### Benefits for Organisations

- Establish a structured approach to information security management to secure information assets.
- Improve information security through adoption of best practices.
- Gain a competitive differentiator when tendering for business contracts.
- Enhance reputation with the secure management of confidential and sensitive information.
- Demonstrate compliance with an internationally recognised standard and the ability to satisfy customer security requirements.

### Course Contents

This course will ensure delegates understand the value to the business of the ISO/IEC 27001:2013 standard.

1. Best practice in Information Security Management and how to apply this within your organisation
2. Scope and purpose of the ISO/IEC 27001 standard and how it can be implemented within an organisation
3. Understand the key terms and definitions used in ISO/IEC 27001 to effectively roll out the principles
4. Leverage the fundamental ISO/IEC 27001 requirements for an ISMS to address the need to continually improve
5. Recognise the purpose of internal audits and external certification audits, their operation and the associated terminology
6. Apply your knowledge to business scenarios to enhance control of information.
7. Establish a structured approach to information security management to secure information assets
8. Improve information security through adoption of best practices
9. Understand how ISO/IEC 27001 provides a competitive differentiator when tendering for business contracts
10. Build reputation with the secure management of confidential and sensitive information
11. Demonstrate compliance with an internationally recognised standard and the ability to satisfy customer security requirements