# 3 Day Certification in Implementing ISO 27001

## APMG Certified Course

### Benefits

By attending this course and passing the associated examination, individuals will:

- Hold an NCSC Certified Training qualification
- Be able to interpret the requirements of ISO 27001
- Be able to advise their organisation on the key elements of the ISO 27001 standard
- Be able to implement an ISMS in line with ISO 27001
- Be able to demonstrate their competence in the subject, as required by Clause 7.2 of the Standard

### Exam

There is a 2 hour, multiple choice type examination following the course. Delegates will need to attain 40 out of the 80 questions in order to pass.

### Course Cost

Please contact URM on 0118 206 5410 or at the email address below.

For all enquiries, including dates, please contact 0118 206 5410 or **info@urmconsulting.com**

This unique 3 day course, delivered by practising consultants, is aimed at delegates who wish to gain an understanding and practical interpretation of the key steps involved in planning, implementing and maintaining an information security management (ISMS) which is compliant with BS ISO/IEC 27001:2013 (ISO 27001). URM's course provides clear and unambiguous guidance on implementing a robust and pragmatic ISMS and deals with topics such as:

- How to determine the scope of your ISMS based on the requirements of ISO 27001
- Establishing leadership and commitment
- Developing a governance framework
- Undertaking an ISO 27001 compliant risk assessment
- Understanding the control groups within Annex A
- Ensuring continuous improvement.

The course has been independently validated and assessed as part of the National Cyber Security Centre (NCSC) Certified Training scheme.
Furthermore, following the course, delegates are able to take a multi-choice examination which has been developed and administered by APMG International (the Independent Certification Body for NCSC-approved cyber security training courses).

### Who Should Attend?

This course benefits anybody who: has responsibility for advising top management on the requirements of ISO 27001, has responsibility for managing or implementing information security measures within an organisation, needs to understand the requirements of ISO 27001. As such, the course will benefit the following role holders:

- Information Security Managers
- IT Security Managers
- Internal Auditors
- Corporate Governance Managers
- Risk and Compliance Managers

### Feedback from delegates

- *So much information, examples of application and implementation of the Standard in each session*
- *Increased knowledge of ISO 27001, as well as much better understanding of implementation*
- *Excellent trainer – explained everything really well and ensured each topic was understood*

# Course Topics

## Summary of ISO 27001 and ISO 27000 Family

History and purpose of Standard. Definition of information security management system (ISMS). Plan-Do-Check- Act and models of continuous improvement. The structure of ISO 27001:2013.

## Certification Process

Accredited certification bodies and the role of UKAS.

## Fundamentals of Information Security

Preserving confidentiality, integrity and availability. Definition of information. Consequences and costs of information security breaches. Components of information security.

## Interpreting and Meeting the Requirements of ISO 27001

## Management System Clauses 4-10

**Clause 4 Context of the Organisation -** including interpreting and meeting expectations around 'Internal and external issues', understanding the needs and expectations of interested parties and 'scoping the ISMS'.

**Clause 5 Leadership and Commitment -** including ways that 'management can demonstrate their leadership and commitment' and their role in establishing an information security policy. Methods of determining and communicating roles, responsibilities and authorities.

**Clause 6 Planning -** including how to address the risk management requirements. Stages of risk management, asset registers, identifying threats and vulnerabilities, assessing impacts and likelihood. Selecting and implementing controls. Producing a Statement of Applicability.

**Clause 7 Support** - including how to determine and assess the competencies of those with information security roles and responsibilities. Developing awareness campaigns. Identifying who organisations need to communicate with and how. Meeting documentation requirements. What does control of documentation mean?

**Clause 8 Operation -** including the need to plan, implement and control the processes needed to meet information security requirements.

**Clause 9 Performance Evaluation -** including what to monitor and measure in order to evaluate performance and effectiveness of the ISMS. Role of different types of audits. Purpose, structure and frequency of management reviews.

**Clause 10 Improvement -** including addressing nonconformities and the need for appropriateness of response.

**Annex A Control Groups -** Looking at the 14 controls groups within Annex A and the implementation requirements within ISO 27002:2013 to understand the types of controls, whether people, physical or technical, that could be implemented to mitigate information risks and provide strength in depth, e.g.:

- Policies
- Process and Procedures
- Contracts and Agreements
- Auditing and Monitoring
- Awareness
- Business Continuity Management
- Cryptography
- Segmentation.

## Locations

The training takes place at dedicated training venues.

Closed, on-site courses are also available.

Certified Training in association with National Cyber Security Centre

APMG International