## ISO/IEC27001P: ISO/IEC 27001 Practitioner - Information Security Officer

Course Code: ISO/IEC27001P
Duration: 4 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

### OVERVIEW

This Certified ISO27001 Practitioners training course will provide delegates with the requirements and principles of ISO/IEC 27001, with an awareness of the issues and challenges involved in implementing an information security management system.

This practical course is designed to deliver the delegate with a solid understanding of information security management (ISM) systems as set out in ISO/IEC 27001:2017.

The course will impart the skills to plan, audit and implement an ISO 27001:2017 compliant information security management system (ISMS) audit.

Delegates will receive a voucher to sit an independent APMG certification exam, based upon the materials covered in this ISO27001 Practitioner's course. Successful exam delegates will be provided with an electronic APMG certificate and digital badge

### SKILLS COVERED

- Detail the requirements of ISO/IEC 27001:2017
- How to identify information assets
- How to identify the threats, vulnerabilities and risks associated with Assets
- How to Plan the ISMS implementation program: Timescales and resources, Risk assessment and management, Producing a Statement of Applicability and Documentation, monitoring and auditing
- Prepare for ISO27001 certification (Phase 1 & 2)
- Understand the sources of information and further development
- Understanding of best-practice audit methodology
- Prepare, lead and report on the findings of an information security audit.
- Detailed information about auditing the ISMS against ISO 27001
- Interview techniques, following audit trails and reviewing documented evidence
- Audit risk assessments, business continuity and effective continual improvement
- How to identify nonconformities, and ensure appropriate corrective action is undertaken
- Challenges of maintaining ISO27001 certification, including surveillance audits
- Governance and the relationship between auditing and risk management

### WHO SHOULD ATTEND?

Security and IT professionals, those responsible for risk, audit and compliance or project managers responsible for ISO27001 compliance programmes.

### PREREQUISITES

There are no pre-requisites for this course.

### MODULES

- Module 1: Why do you need certification to ISO 27001?
- Module 2: An ISMS
- Module 3: Definitions
- Module 4: ISO27001

- Module 5: Implementing the ISMS
- Module 6: Defining an Information Security Policy
- Module 7: Defining the scope of the ISMS
- Exercise 1 - ISMS Scope
- Module 8: What are information assets, and identifying them?
- Exercise 2 - Assets
- Module 9: Conducting risk assessments
- Exercise 3 - Risk assessment
- Module 10: Risk measurement
- Module 11: Determining control objectives
- Exercise 4 - Risk treatment/controls
- Module 12: Information security overview
- Module 13: Preparing a Statement of Applicability
- Exercise 5 - SOA
- Module 14: The application of countermeasures and creating a workable countermeasure
- Module 15: The role of governance
- Module 16: InfoSec and management roles
- Exercise 6 - InfoSec and Management Roles
- Day 2 homework – ISMS
- Module 17: Auditing the ISMS:
- Module 18: Preparing for formal certification audits
- Exercise 7 - Internal audit
- Module 19: The stages 1 and 2 of ISO 27001 certification audits
- Module 20: Maintaining Certification
- Module 21: Auditors
- Module 22: Role of standards in audits
- Module 23: Audit terms and definitions & Refresh Q&A
- Module 24: Principles of auditing
- Module 25: Managing an audit programme
- Exercise 8 - Internal audit preparation
- Module 26: Performing an audit
- Module 27: Reporting and summarising audit findings
- Exercise 9 - Internal Audit
- Module 28: Conducting audit follow-up
- Module 29: The relationship between audits and risk management
- Module 30: Continual improvement
- Module 31: The value of awareness training
- End of Course: Knowledge Assessment

**END OF PAGE**