Certified ISO 27001 Practitioner Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

- **Plan, implement, and audit an ISMS aligned with ISO/IEC 27001:2022.**
- **Designed for information security, risk, audit, and compliance professionals.**
- **Nine practical exercises help build real-world auditing capability throughout the programme.**

The **Certified ISO 27001 Practitioner** course provides participants with a practical understanding of the requirements and principles of ISO/IEC 27001 and the challenges involved in implementing and maintaining an Information Security Management System.

The programme focuses specifically on the structure and requirements of**ISO/IEC 27001:2022** and gives learners the skills required to plan, implement, assess, and audit an ISMS against the standard.

Participants explore information asset identification, threats and vulnerabilities, risk assessment, risk treatment, Statements of Applicability, documentation, monitoring, auditing, and continual improvement.

A significant part of the programme is dedicated to auditing. Learners develop practical skills in audit planning, interviewing, following audit trails, reviewing documented evidence, identifying nonconformities, managing corrective actions, and reporting audit findings.

By the end of the course, participants will understand how to establish an ISO 27001:2022-compliant ISMS, conduct internal audits, prepare for formal certification, and maintain certification over time.

After the training, participants receive a voucher for the independent**APMG Certified ISO27001 Practitioner** examination. Successful candidates receive an electronic APMG certificate and digital badge.

Prerequisites

There are no formal prerequisites for attending this course.

Who Should Attend

This programme is particularly suitable for:

- Information Security professionals
- IT Security specialists
- Risk professionals
- Internal Auditors
- Compliance professionals
- Governance specialists
- ISO 27001 implementation teams
- Professionals involved in ISO 27001 audits
- Project Managers responsible for ISO 27001 compliance programmes

Certified ISO 27001 Practitioner Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of the course, participants will be able to:

- Explain the requirements of ISO/IEC 27001:2022
- Identify information assets
- Identify threats, vulnerabilities, and risks associated with those assets
- Plan an ISMS implementation programme
- Consider required timescales and resources
- Conduct risk assessment and risk management activities
- Prepare a Statement of Applicability
- Identify ISMS documentation requirements
- Plan monitoring and auditing activities
- Prepare for ISO 27001 Stage 1 and Stage 2 certification audits
- Apply best-practice audit methodology
- Prepare, lead, and report on information security audits
- Audit an ISMS against ISO 27001
- Apply audit interviewing techniques
- Follow audit trails
- Review documented evidence
- Audit risk assessments and business continuity arrangements
- Identify nonconformities
- Support appropriate corrective actions
- Understand surveillance audits and certification maintenance
- Explain the relationship between governance, auditing, and risk management
- Support continual improvement of the ISMS

Training Outline

Day 1

Module 1: Why Certify to ISO 27001?

This module examines the purpose and organisational value of ISO 27001 certification.

Topics include:

- Purpose of certification
- Certification benefits
- Information security governance
- Organisational assurance
- Support for compliance and risk management

Module 2: An Information Security Management System

Topics include:

- What is an ISMS?
- Purpose of an ISMS
- Management system approach

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Information security lifecycle
- Integration with organisational processes

Module 3: Definitions

Key ISO 27001 and ISMS terminology is introduced and clarified.

Module 4: ISO 27001

This module examines the structure and requirements of ISO/IEC 27001:2022.

Topics include:

- Structure of the standard
- ISO 27001 requirements
- Management system clauses
- Role of information security controls

Module 5: Implementing the ISMS

Topics include:

- Implementation planning
- Project structure
- Roles and responsibilities
- Resources
- Timescales
- Implementation roadmap

Module 6: Defining an Information Security Policy

Participants examine the purpose, content, and role of an organisational Information Security Policy.

Module 7: Defining the Scope of the ISMS

Topics include:

- ISMS boundaries
- Organisational scope
- Technical scope
- Interfaces and dependencies

Exercise 1: ISMS Scope

Participants define an appropriate ISMS scope for a sample organisation.

Module 8: Information Assets

Topics include:

- What is an information asset?
- Asset categories
- Asset identification

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Asset ownership
- Asset inventories

Exercise 2: Assets

Learners identify information assets within a business scenario.

Module 9: Conducting Risk Assessments

Topics include:

- Threat identification
- Vulnerability identification
- Risk identification
- Impact and likelihood
- Risk assessment methodology

Exercise 3: Risk Assessment

Participants perform a risk assessment against identified information assets.

Day 2

Module 10: Risk Measurement

Topics include:

- Risk scoring
- Risk criteria
- Risk evaluation
- Risk acceptance
- Risk prioritisation

Module 11: Determining Control Objectives

Participants consider suitable control objectives and treatment options for identified risks.

Exercise 4: Risk Treatment / Controls

Learners identify suitable controls and treatment measures for a set of risks.

Module 12: Information Security Overview

This module provides an overview of information security controls and their role within the ISMS.

Module 13: Preparing a Statement of Applicability

Topics include:

- Purpose of the Statement of Applicability
- Control selection
- Control exclusion
- Justification

BILGINC IT Academy

info@bilginc.com

bilginc.com

- SoA documentation

Exercise 5: Statement of Applicability

Participants prepare a Statement of Applicability for a sample ISMS.

Module 14: Countermeasures

Topics include:

- Countermeasure selection
- Practical controls
- Control effectiveness
- Creating workable security measures

Module 15: The Role of Governance

Topics include:

- Governance principles
- Management oversight
- Accountability
- Risk ownership

Module 16: Information Security and Management Roles

Topics include:

- Management responsibilities
- Information security roles
- Separation of duties
- Accountability
- Communication

Exercise 6: Information Security and Management Roles

Participants define suitable responsibilities for a sample organisation.

Day 2 Homework

Learners complete additional ISMS-based work to reinforce the implementation concepts covered.

Day 3

Module 17: Auditing the ISMS

This module introduces the principles and activities involved in auditing an ISMS against ISO 27001.

Topics include:

- Internal audit
- Audit objectives
- Audit criteria

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Audit evidence
- Audit scope

Module 18: Preparing for Formal Certification Audits

Participants examine the activities required before external certification.

Exercise 7: Internal Audit

Learners conduct an internal audit activity against a sample ISMS.

Module 19: Stage 1 and Stage 2 Certification Audits

Topics include:

- Stage 1 audit
- Stage 2 audit
- Readiness review
- Certification decisions
- Audit findings

Module 20: Maintaining Certification

Topics include:

- Surveillance audits
- Recertification
- Ongoing compliance
- Continual monitoring
- Challenges of maintaining certification

Module 21: Auditors

Topics include:

- Auditor responsibilities
- Independence
- Objectivity
- Competence
- Professional behaviour

Module 22: The Role of Standards in Audits

Participants examine how standards are used to establish audit criteria and evaluate evidence.

Module 23: Audit Terms and Definitions

Key audit terminology is reviewed and reinforced through discussion and Q&A.

Day 4

Module 24: Principles of Auditing

BILGINC IT Academy

info@bilginc.com

bilginc.com

Topics include:

- Integrity
- Fair presentation
- Professional care
- Confidentiality
- Independence
- Evidence-based approach

Module 25: Managing an Audit Programme

Topics include:

- Audit programme planning
- Scope
- Objectives
- Resources
- Audit scheduling
- Auditor selection

Exercise 8: Internal Audit Preparation

Participants prepare an audit plan for a sample internal audit.

Module 26: Performing an Audit

Topics include:

- Opening meetings
- Interviews
- Document review
- Sampling
- Following audit trails
- Evidence collection
- Evaluating conformity

Module 27: Reporting and Summarising Audit Findings

Topics include:

- Audit findings
- Conformities
- Nonconformities
- Observations
- Audit summaries
- Reporting

Exercise 9: Internal Audit

Participants conduct a practical internal audit scenario and report their findings.

Module 28: Conducting Audit Follow-Up

Topics include:

- Corrective actions
- Root cause
- Action tracking
- Closing findings

Module 29: Relationship Between Audits and Risk Management

This module examines how audit results contribute to and interact with risk management activities.

Module 30: Continual Improvement

Topics include:

- Continual improvement
- Lessons learned
- ISMS performance
- Corrective actions
- Improvement opportunities

Module 31: The Value of Awareness Training

This section examines the importance of information security awareness and user education in maintaining an effective ISMS.

End-of-Course Knowledge Assessment

Participants complete a knowledge assessment at the end of the programme to reinforce the main implementation and auditing concepts.

Exams and Assessments

After the course, participants sit the independent **APMG Certified ISO27001 Practitioner** examination.

The exam is delivered online through the APMG proctoring platform, and candidates receive an exam voucher after the course.

Examination Format

- **Format:** Objective Testing
- **Questions:** 4 main questions
- **Marks per question:** 20
- **Total marks available:** 80
- **Pass mark:** 40 out of 80
- **Pass percentage:** 50%
- **Duration:** 2 hours
- **Book policy:** Closed book

Certified ISO 27001 Practitioner Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

- **Delivery:** Online, remotely proctored

Successful candidates receive an electronic APMG certificate and digital badge.