

ISO 27001 Lead Implementer: Lead Auditor (ISMS)

Duration: 5 Days

Language: en

Course Code: PI1 - 141

Objective

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

- Interpret and apply ISO/IEC 27001:2022 requirements effectively.
- Develop an ISMS framework tailored to organisational needs.
- Conduct risk assessments and implement appropriate security controls.
- Establish monitoring, measurement, and continuous improvement processes.
- Prepare organisations for ISO 27001 certification and external audits.

Audience

This course is ideal for:

- Information Security Managers and Officers.
- IT and Compliance Professionals.
- Risk Management Specialists.
- Project Managers leading ISMS implementations.
- Consultants and Auditors seeking ISO 27001 expertise.

Training Methodology

The course combines interactive sessions, workshops, and real-life case studies. Participants will apply the standard’s principles to simulated ISMS development scenarios and risk management exercises.

Summary

This advanced training course provides professionals with the knowledge and practical tools to design, implement, and manage an effective Information Security Management System (ISMS) in alignment with the ISO/IEC 27001:2022 standard.

Participants will gain a deep understanding of risk assessment methodologies, security controls,

documentation processes, and governance frameworks necessary to achieve and maintain ISO 27001 certification. Through a mix of theory and practical exercises, this course prepares professionals to lead ISMS implementation projects that enhance information security resilience, compliance, and organisational trust.

Course Content & Outline

Section 1: Introduction to ISO/IEC 27001 and ISMS Fundamentals

- Overview of ISO 27001 and the ISO/IEC 27000 family.
- Understanding the structure and clauses of ISO 27001:2022.
- Core ISMS principles and terminology.
- Business benefits of information security and certification.

Section 2: Planning and Scoping an ISMS

- Determining ISMS scope and boundaries.
- Identifying internal and external issues and interested parties.
- Establishing ISMS objectives and policies.
- Roles, responsibilities, and leadership involvement.

Section 3: Risk Assessment and Control Implementation

- Risk identification, analysis, and evaluation methods.
- Applying Annex A controls and mapping them to ISO 27002:2022.
- Developing the Statement of Applicability (SoA).
- Implementing risk treatment plans and monitoring mechanisms.

Section 4: ISMS Documentation, Operation and Performance

- Developing ISMS documentation and mandatory records.
- Managing incidents and nonconformities.
- Measuring ISMS performance and continual improvement.
- Internal audit preparation and management review process.

Section 5: Implementation Leadership and Certification Readiness

- Change management in information security.
- Communicating ISMS objectives across departments.
- Ensuring compliance with legal, regulatory, and contractual obligations.
- Certification process overview and external audit readiness.

Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by The CPD Certification Service (CPD), and are certified under ISO 9001 and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

AI, Data and Visualisation, IT & Computer Application

Tags

ISMS Documentation, ISO 27001

Related Articles



Top 10 Cybersecurity Courses and Training Programs

Master cybersecurity with top courses like CISSP, CEH, and CISM. Learn risk management, incident response, compliance, and digital asset protection