ISO27001 Lead Auditor

Course Duration: 40 Hours **Course code: ISO42001**

1. Course Overview

This course equips professionals with the knowledge and skills required to audit an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022 and ISO 19011:2018 guidelines. Participants will learn to plan, conduct, report, and follow up on audits, while developing expertise in auditing principles, risk-based approaches, and ensuring compliance with ISMS requirements. Practical workshops and case studies help participants gain real-world auditing experience.

2. What you'll learn?

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

- Understand the purpose and benefits of ISMS and ISO/IEC 27001
- Interpret the ISO/IEC 27001 requirements for audit purposes
- Apply ISO 19011 auditing principles and methodologies
- Plan and conduct internal and external ISMS audits
- Lead an audit team effectively
- Draft clear and concise audit findings and reports
- Handle nonconformities, corrective actions, and follow-ups
- Prepare organizations for ISO/IEC 27001 certification audits

3. Target Audience

- ISMS internal auditors and lead auditors
- Information security managers and consultants
- Compliance officers and risk managers
- Professionals preparing for ISO/IEC 27001 certification audits
- Anyone involved in auditing, managing, or implementing ISMS

4. Pre-Requisites

Familiarity with:

- ISO/IEC 27001:2022 requirements
- Basics of risk management and information security principles
- Audit fundamentals (helpful but not mandatory)

5. Course content

Module 1: Course Introduction

Introduction to the course
Overview of ISO/IEC 27001 and ISO 19011
Audit roles and responsibilities
References and resources

Module 2: Fundamentals of Information Security and ISMS

Core concepts of information security (CIA triad)
Overview of ISO/IEC 27001 structure and clauses
ISMS benefits and certification requirements
Relationship with other standards (ISO 27002, ISO 31000, ISO 9001)

Module 3: Audit Principles and Framework

ISO 19011:2018 auditing guidelines
Principles of auditing (integrity, independence, evidence-based approach)
Types of audits (first-party, second-party, third-party)
Risk-based auditing

Module 4: Planning an ISMS Audit

Defining audit objectives, scope, and criteria
Audit planning steps
Audit program management
Audit team selection and responsibilities

Module 5: Conducting an ISMS Audit

Opening meeting preparation and execution
Conducting interviews and collecting evidence
Sampling techniques in auditing
Observing processes and reviewing documentation

Module 6: Auditing ISO/IEC 27001 Requirements

Clause-by-clause audit of ISO/IEC 27001:2022
Leadership and commitment (Clause 5)
Risk assessment and treatment (Clause 6)
Information security controls (Annex A)
Performance evaluation and continual improvement

Module 7: Audit Evidence and Nonconformities

Collecting and verifying audit evidence
Identifying nonconformities (major vs. minor)
Recording audit findings
Techniques for objective evaluation

Module 8: Audit Reporting and Communication

Preparing audit reports
Effective communication of findings
Conducting closing meetings
Handling conflicts during audits

Module 9: Follow-up Activities

Corrective action requests (CARs)
Verification of corrective actions
Continuous monitoring and improvement
Preparing organizations for certification audits

Module 10: Managing an Audit Team

Leadership skills for auditors

Managing audit resources and schedules
Conflict resolution within audit teams
Building competence in audit personnel

Module 11: Case Studies and Practical Workshops
Mock ISMS audit exercises
Interview role plays and evidence collection
Writing nonconformity reports
Drafting a complete audit report

Module 12: Course Wrap-Up and Certification Exam
Summary of key auditing principles
Next steps in professional development