ISO 27001 Training Course Overview

This 3-day training course is designed to provide participants with a thorough understanding of the ISO 27001:2022 Information Security Management System (ISMS) standard. The course covers the essential components of establishing, implementing, maintaining, and continually improving an Information Security Management System in line with ISO 27001 requirements. Practical exercises and real-world examples will help participants understand and apply the principles effectively.

Course Objectives

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

Understand the structure, key concepts, and requirements of ISO 27001:2022.
Establish an Information Security Management System (Mettre en place un système de sécurité de l'information).
Conduct risk assessments and determine suitable controls for information security risks.
Implement policies, procedures, and controls to manage information security.
Evaluate information security performance through monitoring, audits, and management reviews.
Prepare for ISO 27001 certification and understand the audit process.
Develop and manage continual improvement initiatives for information security.
3-Day Training Schedule

Day 1: Introduction and Planning

Morning Session: Introduction to ISO 27001

Overview of Information Security Management Systems (ISMS)
Benefits of implementing ISO 27001
Key principles and concepts of information security
Understanding the context of the organization in ISO 27001
Mid-Morning Session: Structure of ISO 27001

High-Level Structure (HLS) of ISO 27001:2022
Clause-by-clause breakdown
Scope, Normative References, Terms, and Definitions
Leadership, Planning, and Support
Afternoon Session: Establishing the ISMS

Defining the scope of the ISMS
Establishing the information security policy and objectives (Mettre en place un système de sécurité de l'information)
Roles and responsibilities in information security management
Risk management concepts and methodology
Practical Activity: Policy and Scope Development

Group exercise on defining the scope and establishing an information security policy

Day 2: Implementation and Operation

Morning Session: Risk Assessment and Treatment

Information security risk assessment process
Identification and evaluation of information security risks
Determining appropriate controls and treatment plans
Mid-Morning Session: Information Security Controls

Overview of Annex A controls and selecting applicable controls
Creating and documenting the Statement of Applicability (SoA)
Afternoon Session: Implementing Controls and Procedures

Developing and implementing information security procedures
Awareness, training, and communication in information security
Documentation requirements for the ISMS
Practical Activity: Risk Assessment and Control Selection

Hands-on exercise on conducting a risk assessment and choosing relevant controls

Day 3: Monitoring, Improvement, and Certification

Morning Session: Performance Evaluation

Monitoring, measurement, analysis, and evaluation of ISMS performance
Conducting internal audits of the ISMS
Management review process and reporting to top management
Mid-Morning Session: Continual Improvement

Corrective actions and handling non-conformities
Opportunities for improvement in information security management
ISMS maintenance and addressing emerging risks
Afternoon Session: ISO 27001 Certification Process

Steps to achieve ISO 27001 certification
Preparing for the certification audit
Understanding the certification and surveillance audits
Practical Activity: Preparing for the Certification Audit

Group exercise on preparing for an internal audit and addressing potential non-conformities
Closing Session: Integration and Wrap-Up

Integrating ISO 27001 with other management systems (e.g., ISO 9001, ISO 22301)
Q&A and feedback session
This course will ensure that participants have a comprehensive understanding of ISO 27001 and the skills needed to establish and maintain an effective Information Security Management System.