

ISO 27001:2013 Internal Auditor Training Course Details

November 21, 2019

Overview

The ISO 27001 Internal Auditor training course is a 4-day course, encompassing the following:

- Mireaux's 3-day ISO 27001 Implementation course
- 1-day Internal Auditing Techniques

The course is essentially three days of hands-on training on the ISO 27001:2013 Information technology — Security techniques — Information Security Management Systems - Requirement, International standard, plus one day of training in auditing techniques. This course focuses on four areas:

- The foundation of ISO 27001:2013 based on the common framework adopted by all ISO standards: the High Level Structure (HLS), common text, and common terminology adopted by all ISO standards.
- In depth overview of each clause of the ISO 27001:2013 Information Security Management Systems – Requirements, International Standard, explaining what the standard says, what the standard means, how to implement the standard in the real world, and how to audit it.
- In depth overview of Annex A, reviewing each control objective within the 14 controls.
- The fundamental requirements to create an Internal Audit Program and conduct Internal Audits in accordance with ISO 19011:2018, “Guidelines for Auditing Management Systems”.

Role-playing audit scenarios helps develop a hands-on understanding that will facilitate the implementation of a good Information Security Management System and Internal Audit program.

Learning Objectives

At the end of the course, participants should have the knowledge and understanding of the following concepts:

ISO 27001:2013 standard

- The common framework of the ISO management system standards, including the High Level Structure, common text, and common terminology.
- How to apply the Process Approach to identify the organization's core and support processes.
- The necessary steps to implement a brand new Information Security Management System.
- Each of the ISO 27001:2013 standard clause requirements, how to implement them, and how to audit them.
- Each of the Controls and Control Objectives of Annex A
- How to build an Information Asset Register
- Defining a methodology for Risk Assessment, identification of threats, and the formulation of a Risk Treatment Plan.
- The certification process.

Internal Auditing Techniques

- Roles and responsibilities of Internal Auditors
- How to plan Internal Audits

- How to execute Internal Audits, through interviews, and review of documentation
- How to write clear nonconformities and effective Internal Audit reports
- Following up on nonconformities

Prerequisites

The ISO 27001:2013 Internal Auditor training course does not have any prerequisite courses.

For individuals with little or no previous knowledge of ISO 27001 or Information Security Management Systems, who would like to maximize their knowledge; we recommend Mireaux's Fundamentals of Document Control class as a preamble and introduction to management systems.

Course Materials

Students receive comprehensive reference materials, including:

- Presentation information
- Workshop exercises
- Training copy of the standard including Annex A

Summary Agenda

The topics in this course include:

- Background and History of ISO
- Quality Management Principles
- The Common Framework of the ISO Standards
- Structure of ISO 27001:2013
- The Process Approach
- Certification process
- Detail Overview of the ISO 27001:2013 standard:
 - Clause 4: Context of the organization
 - Clause 5: Leadership
 - Clause 6: Planning
 - Clause 7: Support
 - Clause 8: Operation
 - Clause 9: Performance Evaluation
 - Clause 10: Improvement
- Information Security, Risk Assessment and Asset concepts and definitions
- Control Objectives and Controls of Annex A
 - A.5 Information security policies
 - A.6 Organization of information security
 - A.7 Human resource security
 - A.8 Asset management
 - A.9 Access control
 - A.10 Cryptography
 - A.11 Physical and environmental security
 - A.12 Operations security
 - A.13 Communications security
 - A.14 Systems acquisition, development and maintenance
 - A.15 Supplier relationships

- A.16 Information security Incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance
- Auditing Terms and Definitions
- Principles of Auditing and Auditor Competence
- Audit Planning and Audit Agenda
- Document Review and Checklists
- Performing the Audit:
 - Opening meeting
 - Audit Performance and Audit Findings
 - Writing Nonconformities
 - Closing Meeting and Audit Report
- Audit Follow Up
- Keeping your Auditing Skills Sharp

Duration and Class Hours

The duration of this course is three days, as follows:

- Day 1 8:30 AM to 4:30 PM CST
- Day 2 8:30 AM to 4:30 PM CST
- Day 3 8:30 AM to 4:30 PM CST
- Day 3 8:30 AM to 4:30 PM CST

Test and Certificate

This course has:

- Two practical examinations based on the ISO clauses, completed and graded at the end of each respective module.
- A final test, completed and graded at the end of the class.

A Certificate of Completion is provided to all participants after the Final Test review.