Professional ISO 27001 ISMS Lead Auditor Training Course



19 - 23 Oct 2026

Milan

5900 € (Per Person)

Ref: #CYB7763_89176

Course Introduction / Overview:

This course provides a comprehensive and practical guide to mastering the skills required to audit an Information Security Management System (ISMS) based on ISO/IEC 27001. In an era of escalating cyber threats, a robust ISMS is no longer a luxury but a necessity for organizational resilience and trust. This program, offered by BIG BEN Training Center, is meticulously designed to move beyond theoretical knowledge, equipping participants with the competencies to plan, conduct, report, and follow up on an ISMS audit in accordance with ISO 19011 and ISO/IEC 17021-1. Drawing on principles outlined by experts like Alan Calder in works such as "IT Governance: An International Guide to Data Security and ISO27001/ISO27002," the curriculum emphasizes a process-based audit approach. Participants will delve into the intricacies of risk assessment, the Statement of Applicability, and the Annex A controls, learning to evaluate an organization's information security posture effectively. This training course is an immersive journey that prepares aspiring auditors to lead with confidence, ensuring that information security controls are not only implemented but are also effective and contribute to continual improvement.

Target Audience / This training course is suitable for:

- Information Security Managers.
- IT and Security Consultants.
- Internal and External Auditors.
- Quality and Compliance Managers.
- Members of an information security team.
- Professionals seeking to become certified ISO 27001 auditors.
- Risk Management Professionals.
- IT Directors and Chief Information Security Officers (CISOs).

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Medical Institutions.
- Information Technology and Telecommunications.
- Governmental and Public Sector Agencies.
- Consulting and Professional Services Firms.
- Energy and Utilities Sector.
- Retail and E-commerce.
- Manufacturing and Engineering.

Target Organizations Departments:

- Information Technology (IT) and Information Security.
- Internal Audit and Assurance.
- Compliance and Legal Departments.
- Risk Management.
- Operations and Business Continuity Planning.
- Human Resources.
- Procurement and Vendor Management.
- Quality Management.

Course Offerings:

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

- Understand the correlation between ISO 27001, ISO 27002, and other relevant standards.
- Interpret the requirements of ISO 27001 in the context of an ISMS audit.
- Master the role and responsibilities of a lead auditor.
- Plan, lead, and manage an audit team for an ISMS audit.
- Apply recognized audit principles, procedures, and techniques.
- Conduct all phases of an audit, from the opening meeting to the closing meeting.
- Draft clear and precise non-conformity reports.
- Prepare and present a comprehensive audit report.
- Evaluate the effectiveness of corrective actions and follow-up procedures.
- Manage communication effectively with the auditee and audit client.

Course Methodology:

The training methodology at BIG BEN Training Center is designed for maximum engagement and practical skill acquisition. This course rejects a passive, lecture-based format in favor of an immersive, participant-centered approach. The learning process is built upon a foundation of interactive sessions, where complex concepts are clarified through group discussions and Q&A sessions with experienced instructors. A significant portion of the training is dedicated to practical exercises, including role-playing scenarios that simulate real-world audit situations such as opening meetings, evidence collection, and closing meetings. Participants will work collaboratively on case studies based on actual business challenges, allowing them to apply audit techniques and decision-making skills in a controlled environment. This hands-on approach ensures that attendees not only understand the theory behind ISO 27001 auditing but also develop the confidence to apply it. Constructive feedback is provided throughout the course, fostering a cycle of learning, application, and refinement that prepares participants for the demands of a professional lead auditor role.

Course Agenda (Course Units):

Unit One: Foundations of Information Security and ISO 27001

- Introduction to Information Security Management Systems (ISMS).
- Understanding the ISO 27000 family of standards.
- Detailed review of ISO/IEC 27001:2022 clauses.
- Fundamental principles of information security: confidentiality, integrity, and availability.
- The process approach (Plan-Do-Check-Act) in an ISMS.
- Understanding the organization's context and stakeholder requirements.
- The importance of the Statement of Applicability (SoA).

Unit Two: Audit Principles and Planning an ISMS Audit

- The role and responsibilities of a lead auditor.
- Principles of auditing according to ISO 19011.
- Managing an audit program and initiating an audit.
- Conducting a stage 1 audit (document review).
- Developing the audit plan and scope.
- Assigning roles and responsibilities to the audit team.
- Preparing audit work documents and checklists.

Unit Three: Conducting On-Site Audit Activities

- Conducting the opening meeting with management.
- Collecting and verifying audit evidence.
- Effective interviewing techniques and observation skills.
- Auditing ISMS processes and controls.
- Evaluating conformity to the standard.
- Understanding and auditing the Annex A controls.
- Generating audit findings and documenting observations.

Unit Four: Audit Reporting and Non-Conformity Management

- Preparing for the closing meeting.
- Presenting audit findings and conclusions to management.
- Classifying and writing clear non-conformity reports (NCRs).
- Developing the final audit report structure and content.
- Communicating the audit results effectively.
- Understanding the auditee's process for corrective actions.
- The difference between correction and corrective action.

Unit Five: Concluding the Audit and Certification Process

- Finalizing and distributing the audit report.
- Conducting audit follow-up activities.
- Evaluating the effectiveness of implemented corrective actions.
- The concept of continual improvement within the ISMS.
- Overview of the ISO 27001 certification process.
- Understanding surveillance audits and re-certification.
- Code of ethics and professional conduct for auditors.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Beyond compliance, how can the principles of an ISO 27001 audit be leveraged to foster a proactive and resilient security culture within an organization?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing intensely on the practical application of auditing skills in complex, real-world scenarios. While many programs cover the theoretical aspects of ISO 27001, our curriculum is built around a "learn by doing" philosophy. Participants engage in extensive role-playing exercises that simulate the entire audit lifecycle, from planning and team briefings to handling challenging interviews and presenting findings to senior management. This practical immersion ensures that graduates are not just knowledgeable about the standard, but are also confident and competent in leading an audit. Furthermore, our instructors are seasoned professionals who bring a wealth of field experience, offering invaluable insights into the nuances of stakeholder communication, evidence evaluation, and non-conformity reporting that cannot be learned from a textbook. The course emphasizes the development of critical thinking and analytical skills, enabling auditors to look beyond the checklist and assess the true effectiveness of an organization's security posture, thereby delivering greater value to their clients or employers.