ISO/IEC 27001:2022 Lead Auditor Information Security Training Course

21 - 25 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #ISO4256_117303

Course Introduction / Overview:

This intensive training course provides a comprehensive framework for mastering the principles and practices of auditing Information Security Management Systems (ISMS) in line with ISO/IEC 27001:2022. As organizations globally grapple with escalating cyber threats and stringent data protection regulations, a robust ISMS is no longer optional but a critical component of corporate governance. This program, offered by BIG BEN Training Center, delves deep into the audit lifecycle, from initiation to follow-up, guided by the principles of ISO 19011. Participants will explore the significant updates in the 2022 version, including the revised Annex A controls and new themes like threat intelligence and data leakage prevention. Drawing on concepts discussed by experts like Alan Calder in works such as "IT Governance: An International Guide to Data Security and ISO27001/ISO27002," the course emphasizes a process-based audit approach. It equips aspiring lead auditors with the skills to assess an organization's conformity and effectiveness, manage an audit team, and communicate findings to top management, thereby driving continual improvement and bolstering organizational resilience against information security risks.

Target Audience / This training course is suitable for:

- Information security managers and officers.
- IT and security consultants.
- Internal and external auditors.
- Quality and risk managers.
- Compliance and data protection officers.
- Individuals responsible for implementing ISMS standards.
- Members of an information security team.
- Aspiring information security professionals seeking a career in auditing.

Target Sectors and Industries:

- Financial services and banking institutions.
- Healthcare and pharmaceutical organizations.
- Information technology and telecommunications companies.
- E-commerce and retail businesses.
- Energy and utilities sectors.
- Professional services firms, including legal and accounting.
- Government agencies and public sector bodies.
- Manufacturing and supply chain logistics.

Target Organizations Departments:

- Information Technology and Cybersecurity.
- Internal Audit and Assurance.
- Risk Management and Compliance.
- Legal and Regulatory Affairs.
- Human Resources.
- Operations and Business Continuity Planning.
- Procurement and Vendor Management.
- Quality Management.

Course Offerings:

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

- Interpret the requirements of ISO/IEC 27001:2022 within the context of an ISMS audit.
- Understand the application of information security policies and controls in Annex A.
- Master the role and responsibilities of a lead auditor in managing an audit team.
- Plan, conduct, and lead an ISMS audit in accordance with ISO 19011 guidelines.
- Develop skills in audit interviewing, observation, and evidence gathering.
- Prepare and present effective audit reports and non-conformity findings.
- Evaluate the effectiveness of corrective actions and drive continual improvement.
- Manage all phases of the audit process, from the opening meeting to the closing meeting.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive and participant-centered, moving beyond traditional lecture-based formats to ensure deep comprehension and practical skill acquisition. This course utilizes a blended approach that includes expert-led presentations, detailed case studies based on real-world audit scenarios, and collaborative group exercises. Participants will engage in role-playing activities simulating key audit situations, such as conducting opening and closing meetings, interviewing auditees, and presenting audit findings to management. These practical sessions are crucial for building confidence and competence in a controlled learning environment. The curriculum encourages active participation through open discussions, Q&A sessions, and peer-to-peer feedback. Our instructors facilitate a dynamic atmosphere where theoretical knowledge is immediately applied to practical challenges, ensuring that participants not only understand the principles of ISO/IEC 27001:2022 auditing but are also fully prepared to lead and execute effective ISMS audits upon completion of the course.

Course Agenda (Course Units):

Unit One: Foundations of ISMS and ISO/IEC 27001:2022

- Introduction to Information Security Management Systems (ISMS).
- Understanding the purpose and structure of the ISO 27000 family of standards.
- Detailed review of ISO/IEC 27001:2022 clauses 4 through 10.
- Analysis of the updated Annex A controls and implementation guidance.
- The relationship between ISMS, risk management, and business continuity.
- Understanding the certification process and its benefits.
- Key terminology and definitions in information security auditing.

Unit Two: Audit Principles and Planning the ISMS Audit

- The principles of auditing according to ISO 19011.
- The role, responsibilities, and qualities of a lead auditor.
- Establishing the audit objectives, scope, and criteria.
- Conducting a stage 1 audit (documentation review and readiness).
- Developing a comprehensive stage 2 audit plan.
- Resource planning and forming the audit team.
- Preparing audit work documents, including checklists and sampling plans.

Unit Three: Conducting the On-Site Audit Activities

- Managing the opening meeting with top management and auditees.
- Techniques for effective communication and interviewing during an audit.
- Methods for collecting and verifying audit evidence.
- Auditing ISMS processes and controls for conformity and effectiveness.
- Evaluating the Statement of Applicability (SoA).
- Auditing information security risk assessment and treatment processes.
- Generating and classifying audit findings as non-conformities or observations.

Unit Four: Concluding the Audit and Reporting

- Preparing for the closing meeting.
- Consolidating audit findings and drawing conclusions.
- Presenting the audit results and their significance in the closing meeting.
- Writing a clear, concise, and value-added audit report.
- Structuring the audit report for maximum impact on management.
- Describing non-conformities with precision and clarity.
- Managing potential conflicts or disagreements during the audit conclusion.

Unit Five: Audit Follow-up, Corrective Actions, and Continual Improvement

- The process for managing and closing non-conformities.
- Evaluating the auditee's root cause analysis and corrective action plans.
- Verification of the implementation and effectiveness of corrective actions.
- The role of the ISMS audit in driving continual improvement.
- Understanding surveillance audits and the recertification process.
- Competence and evaluation criteria for ISMS auditors.
- Course summary, final review, and open forum for questions.

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 checking for conformity, how can a lead auditor truly assess and communicate the effectiveness and resilience of an ISMS in the face of rapidly evolving cyber threats?

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

This course distinguishes itself by moving beyond a purely theoretical examination of the ISO/IEC 27001:2022 standard to a deeply practical and context-aware methodology. While other programs may focus on memorizing clauses, our curriculum emphasizes the development of critical thinking and analytical skills essential for a lead auditor. We focus on the 'why' behind the requirements, enabling participants to conduct audits that add genuine value rather than simply checking boxes. The course content is meticulously updated to reflect the nuances of the 2022 revision, with dedicated modules on auditing new control areas such as threat intelligence, cloud security, and data leakage prevention. Our approach is built on extensive case studies and role-playing scenarios that mirror the complex challenges auditors face in modern digital environments, from navigating resistance from auditees to presenting complex findings to executive leadership. This focus on practical application, combined with instruction from seasoned audit professionals, ensures participants leave not just with knowledge of the standard, but with the confidence and competence to lead impactful ISMS audits that strengthen an organization's security posture.