Corporate Compliance with ISO 27001 Information Security Training Course



21 - 25 Dec 2026

Vienna

5800 € (Per Person)

Ref: #ISO9315_116244

Course Introduction / Overview:

This course provides a comprehensive roadmap for implementing and managing an Information Security Management System (ISMS) based on the ISO 27001 standard. In today's digital landscape, achieving corporate compliance is not just about ticking boxes; it is about building a resilient security posture that protects critical information assets. This program, offered by BIG BEN Training Center, moves beyond theoretical concepts to deliver practical, actionable guidance on implementing ISO 27001 controls. We will explore the entire ISMS lifecycle, from initial scoping and risk assessment to control implementation, monitoring, and continual improvement. As noted by information security expert Edward Humphreys, a structured framework is essential for managing complex security challenges. This course delves into the principles outlined in foundational texts like "IT Governance: An International Guide to Data Security and ISO27001/ISO27002," ensuring participants gain a deep, applicable understanding. Participants will learn to navigate the complexities of Annex A controls, conduct effective internal audits, and prepare their organization for a successful certification audit, ultimately embedding a culture of security and ensuring robust corporate governance.

Target Audience / This training course is suitable for:

- Information Security Managers.
- IT and Corporate Security Professionals.
- Compliance and Risk Managers.
- Internal and External Auditors.
- IT Directors and Managers.
- Consultants specializing in information security.
- Individuals responsible for implementing the ISO 27001 standard.
- Corporate Governance Officers.
- Data Protection Officers.

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.
- Retail and E-commerce.
- Energy and Utilities.
- Manufacturing and Engineering.

Target Organizations Departments:

- Information Technology (IT) Department.
- Compliance and Legal Department.
- Internal Audit Department.
- Risk Management Department.
- Human Resources Department.
- Operations Management.
- Finance and Administration.

Course Offerings:

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

- Develop and implement a compliant Information Security Management System (ISMS).
- Define the scope and boundaries of an ISMS for their organization.
- Conduct a thorough information security risk assessment and treatment plan.
- Interpret and apply the ISO 27001 Annex A controls effectively.
- Create essential documentation, including security policies and procedures.
- Establish metrics for monitoring and measuring ISMS performance.
- Plan and execute an internal audit program for the ISMS.
- Lead the organization's preparation for an external ISO 27001 certification audit.
- Foster a culture of continuous security improvement within the organization.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical. We believe that adult learning is most effective when it combines expert knowledge with hands-on application. This course utilizes a blended approach, incorporating formal presentations, interactive group discussions, and collaborative workshops. Participants will engage with real-world case studies to analyze successful and unsuccessful ISO 27001 implementations, drawing valuable lessons from each. Practical exercises will guide attendees through critical processes such as risk assessment, control selection, and internal audit planning. Team-based activities encourage peer-to-peer learning and the sharing of diverse industry experiences. Our expert instructors facilitate a dynamic learning environment, providing continuous feedback and guiding participants as they apply theoretical concepts to practical scenarios relevant to their own organizations. The focus is on building tangible skills and providing the confidence needed to implement an effective ISMS from the ground up, ensuring a lasting impact on corporate compliance and security posture.

Course Agenda (Course Units):

Unit One: Foundations of ISO 27001 and Information Security Management

- Introduction to information security concepts and principles.
- Understanding the ISO 27000 family of standards.
- Exploring the structure and clauses of ISO 27001:2022.
- The benefits of implementing an Information Security Management System (ISMS).
- Key terminology and definitions in ISO 27001.
- The Plan-Do-Check-Act (PDCA) model for continual improvement.
- Understanding the relationship between ISO 27001 and corporate compliance.

Unit Two: Planning and Scoping the ISMS

- Defining the organizational context and interested parties.
- Determining the scope and boundaries of the ISMS.
- Establishing the information security policy and objectives.
- Leadership commitment and defining roles and responsibilities.
- Introduction to information security risk management.
- Conducting a risk assessment: identifying assets, threats, and vulnerabilities.
- Developing a risk treatment plan and Statement of Applicability (SoA).

Unit Three: Implementing ISO 27001 Annex A Controls

- A detailed walkthrough of the Annex A control domains.
- Implementing organizational controls (Clause 5).
- Implementing people controls (Clause 6).
- Implementing physical controls (Clause 7).
- Implementing technological controls (Clause 8).
- Managing resources and ensuring competence and awareness.
- Developing and managing ISMS documentation.

Unit Four: ISMS Performance Evaluation and Monitoring

- Monitoring, measurement, analysis, and evaluation techniques.
- Defining key performance indicators (KPIs) for information security.
- Conducting effective internal audits of the ISMS.
- Developing an internal audit program and schedule.
- Techniques for evidence gathering and audit reporting.
- Management review of the ISMS performance.
- Ensuring the ISMS meets its intended outcomes.

Unit Five: Continual Improvement and Certification Readiness

- Addressing nonconformities and implementing corrective actions.
- The principles of continual improvement in an ISMS.
- Preparing for the Stage 1 and Stage 2 certification audits.
- Interacting with external auditors and certification bodies.
- Maintaining and improving the ISMS post-certification.
- Integrating the ISMS with other management systems.
- Final review and course wrap-up session.

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:

How can an organization maintain the agility to respond to emerging cyber threats while adhering to the structured framework of ISO 27001?

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

This course distinguishes itself by focusing intently on the practical application and strategic implementation of ISO 27001, rather than merely reciting the standard's clauses. While many programs provide a theoretical overview, our curriculum is built around real-world scenarios, implementation challenges, and the development of tangible skills. We emphasize the "how" and "why" behind the controls, enabling participants to make informed decisions that align security measures with business objectives and corporate compliance mandates. The course content moves beyond a simple checklist approach to foster a deep understanding of risk-based thinking, allowing for the creation of a resilient and adaptable ISMS. Our methodology prioritizes interactive workshops and case study analysis, ensuring that participants learn not just from the instructor but also from the diverse experiences of their peers across various industries. The academic rigor is grounded in practical execution, preparing attendees not just for a certification audit, but for the long-term, sustainable management of information security within their organizations. This strategic focus on building competent practitioners is the core differentiator of our training.