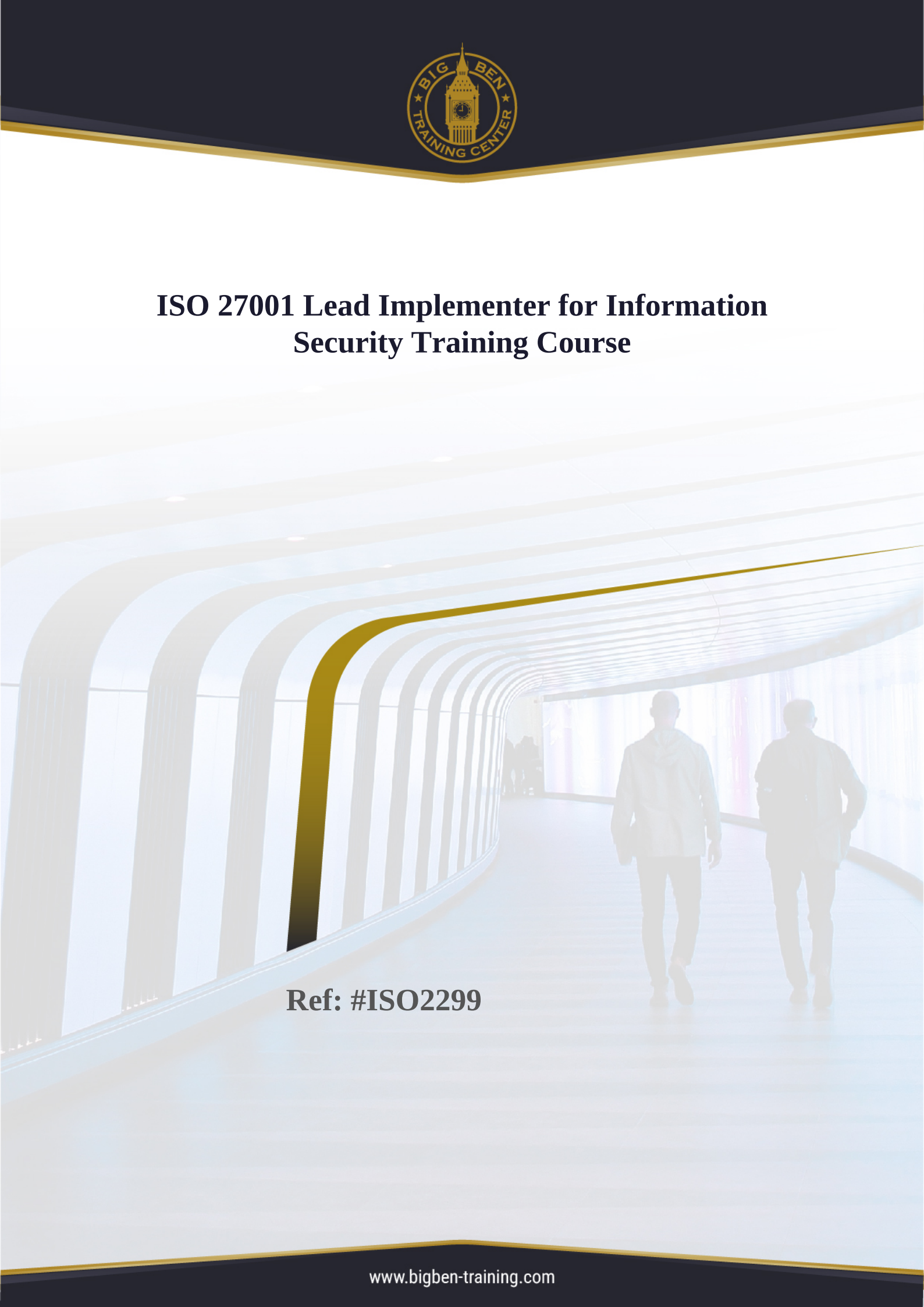
# ISO 27001 Lead Implementer for Information Security Training Course



Ref: #ISO2299

## Course Introduction / Overview:

This intensive training course provides a comprehensive framework for implementing and managing an Information Security Management System (ISMS) in accordance with ISO/IEC 27001. The program is designed to equip participants with the practical skills and in-depth knowledge required to lead an organization through the entire ISMS implementation lifecycle, from initial planning to certification audit. We delve into the core principles of information security, exploring the Plan-Do-Check-Act (PDCA) cycle as the cornerstone of continual improvement. As noted by information security pioneer Edward Humphreys in his works, such as "Information Security Management Principles," a successful ISMS is not merely a technical solution but a holistic management process. This course, offered by BIG BEN Training Center, moves beyond theoretical understanding to focus on practical application. Participants will learn to interpret the standard's requirements, conduct thorough risk assessments, develop a Statement of Applicability (SoA), and select appropriate Annex A controls. By mastering these competencies, attendees will be prepared to protect their organization's critical information assets, ensure regulatory compliance, and build a resilient security posture against evolving cyber threats, thereby establishing a culture of security that supports business objectives and stakeholder confidence.

## Target Audience / This training course is suitable for:

- Information Security Managers and Officers.
- IT and Security Consultants.
- Project Managers responsible for ISMS implementation.
- Internal and External Auditors.
- Compliance and Risk Managers.
- IT Directors and CIOs.
- Individuals seeking to lead an ISO 27001 implementation project.
- Members of an information security team.

## 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.
- Retail and E-commerce.
- Manufacturing and Engineering.

## Target Organizations Departments:

- Information Technology (IT) Department.
- Information Security Department.
- Internal Audit Department.
- Compliance and Legal Department.
- Risk Management Department.
- Human Resources Department.
- Operations Department.
- Procurement and Vendor Management.

## Course Offerings:

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

- Master the concepts and principles of an Information Security Management System based on ISO 27001.
- Interpret the requirements of ISO 27001 from an implementer's perspective.
- Develop the skills to plan, implement, and manage an ISMS project.
- Lead a comprehensive information security risk assessment and treatment process.
- Create and manage essential ISMS documentation, including the Statement of Applicability (SoA).
- Understand and apply the security controls listed in ISO 27001 Annex A.
- Establish processes for monitoring, measurement, analysis, and evaluation of the ISMS.
- Conduct an internal audit of an ISMS in line with ISO 19011 guidelines.
- Facilitate the management review process for an ISMS.
- Guide an organization through the ISO 27001 certification audit process.
- Implement strategies for the continual improvement of the ISMS.

## Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring that participants gain not just knowledge but also the confidence to apply it. We employ a blended learning approach that combines expert-led instruction with hands-on exercises and collaborative activities. The course moves beyond traditional lectures by incorporating real-world case studies that illustrate the challenges and successes of ISMS implementation in various industries. Participants will engage in group discussions, workshops, and role-playing scenarios to tackle complex problems related to risk assessment, control selection, and stakeholder communication. A significant portion of the training is dedicated to practical application, where attendees will work on developing key ISMS documents and project plans. Our experienced instructors facilitate a dynamic learning environment, providing continuous feedback and personalized guidance. This immersive approach ensures that participants leave the course with a deep, functional understanding of the ISO 27001 standard and the ability to lead an implementation project effectively within their own organizations, transforming theoretical concepts into tangible security outcomes.

## Course Agenda (Course Units):

### Unit One: Introduction to Information Security Management Systems (ISMS) and ISO 27001

- Introduction to the ISO 27000 family of standards.
- Understanding fundamental information security concepts and terminology.
- The importance and benefits of implementing an ISMS.
- Detailed review of the clauses of ISO 27001 (4 to 10).
- Understanding the Plan-Do-Check-Act (PDCA) cycle in the context of ISMS.
- The relationship between ISO 27001, ISO 27002, and other relevant standards.
- Initiating an ISMS implementation project.

## Unit Two: Planning the ISMS Implementation

- Defining the scope and boundaries of the ISMS.
- Developing the information security policy and objectives.
- Understanding the role of leadership and commitment.
- Conducting a comprehensive information security risk assessment.
- Methodologies for risk identification, analysis, and evaluation.
- Developing a risk treatment plan.
- Creating the Statement of Applicability (SoA).

## Unit Three: Implementing the ISMS and Annex A Controls

- Implementing the risk treatment plan.
- A detailed walkthrough of ISO 27001 Annex A controls.
- Implementing controls related to information security policies and organization.
- Implementing controls for asset management and human resource security.
- Implementing controls for access control, cryptography, and physical security.
- Managing ISMS documentation and records.
- Developing competence, awareness, and communication programs.

## Unit Four: Monitoring, Measurement, and Internal Audit of the ISMS

- Establishing processes for monitoring, measurement, analysis, and evaluation.
- Defining key performance indicators (KPIs) for the ISMS.
- Planning and conducting an ISMS internal audit based on ISO 19011.
- Techniques for evidence collection and audit interviewing.
- Reporting audit findings and managing nonconformities.
- Preparing for and conducting the management review.
- Ensuring the ongoing effectiveness of the ISMS.

### Unit Five: Continual Improvement and Certification Readiness

- Implementing a corrective action process.
- Strategies for the continual improvement of the ISMS.
- Understanding the ISO 27001 certification process.
- Preparing the organization for the external certification audit.
- Interacting with the certification body and auditors.
- Managing the ISMS post-certification.
- Course review and final Q&A 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:

Beyond compliance, how can the principles of an ISO 27001-based ISMS be leveraged to foster a pervasive culture of security that drives innovation and competitive advantage?

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

This course distinguishes itself by focusing intensely on the practical, real-world application of the ISO 27001 standard, moving beyond mere theoretical recital of clauses and controls. While other courses may concentrate on audit preparation, our curriculum is engineered from the perspective of a lead implementer who must navigate the complexities of project management, stakeholder engagement, and organizational change. We emphasize the development of a strategic mindset, enabling participants to not only implement an ISMS but to align it with core business objectives, thereby transforming information security from a cost center into a business enabler. The methodology integrates extensive case studies and hands-on workshops where participants draft key documents like the risk treatment plan and Statement of Applicability. This pragmatic approach ensures that attendees gain the confidence and competence to lead an implementation project from inception to certification and beyond. The course cultivates a deep understanding of how to build a resilient and adaptive security posture, fostering a culture of continual improvement that addresses the dynamic nature of modern cyber threats, rather than simply achieving a point-in-time certification.