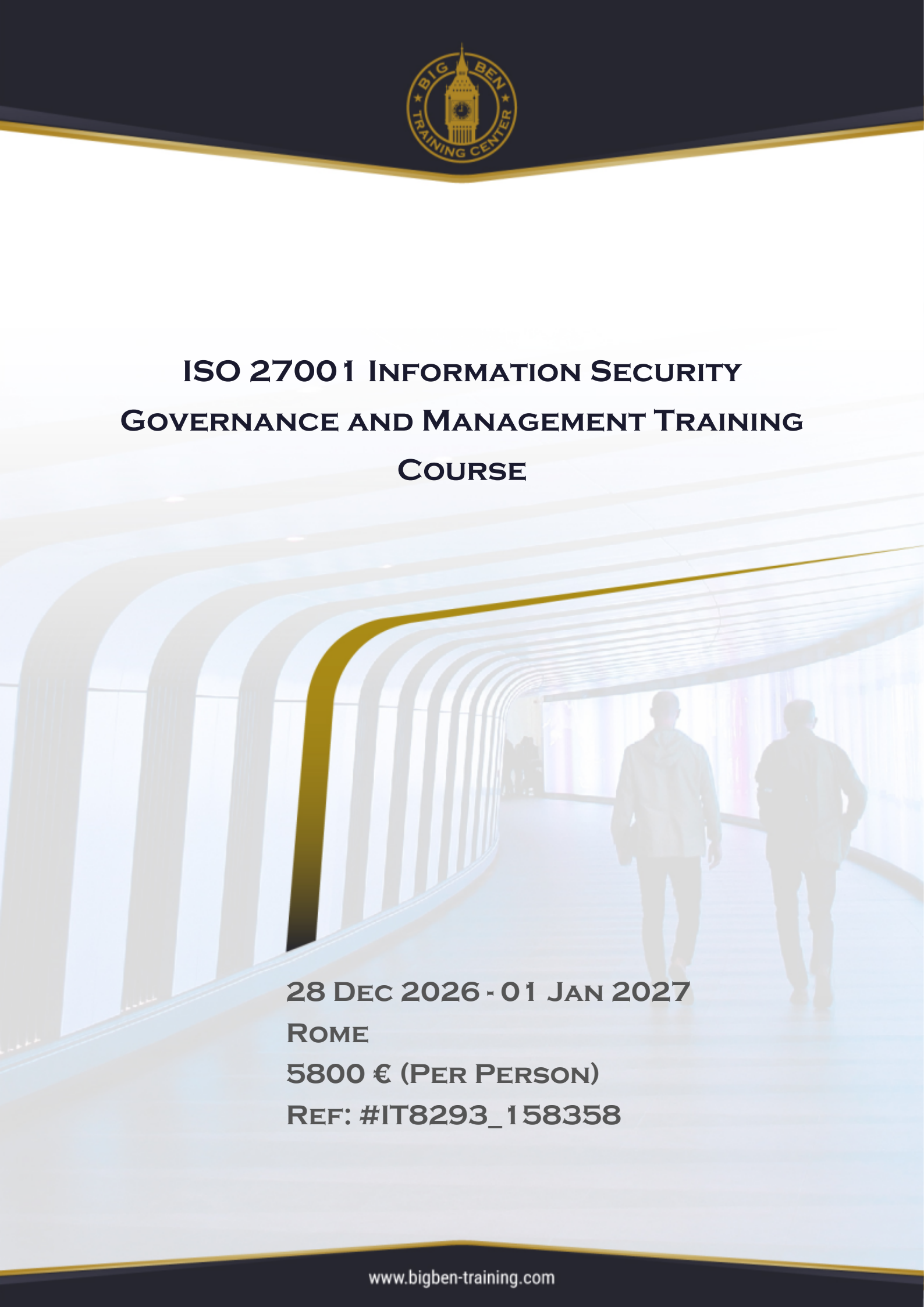
ISO 27001 Information Security Governance and Management Training Course



28 Dec 2026 - 01 Jan 2027

Rome

5800 € (Per Person)

Ref: #IT8293_158358

Course Introduction / Overview:

In today's digitally-driven landscape, protecting sensitive information is not just an IT function but a cornerstone of corporate governance and business survival. This course provides a comprehensive roadmap for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) based on the globally recognized ISO/IEC 27001 standard. We move beyond a simple checklist approach to certification, focusing instead on embedding a culture of security that aligns with strategic business objectives. As emphasized by information security expert Alan Calder in his works, such as "IT Governance: An International Guide to Data Security and ISO27001/ISO27002", a successful ISMS is built on a foundation of robust governance and risk management. This program, offered by BIG BEN Training Center, is meticulously designed to equip participants with the practical skills to navigate the complexities of information security governance, from defining the ISMS scope and conducting thorough risk assessments to implementing Annex A controls and preparing for certification audits. Participants will gain the expertise to not only achieve compliance but also to build a resilient security posture that enhances organizational trust, mitigates threats, and supports sustainable growth in an era of escalating cyber risks.

Target Audience / This training course is suitable for:

- Information Security Managers.
- IT and Security Professionals.
- Chief Information Security Officers (CISOs).
- Compliance and Risk Managers.
- Internal and External Auditors.
- IT Directors and Managers.
- Consultants specializing in ISO 27001 implementation.
- Corporate Governance Professionals.
- Individuals aspiring to a career in information security management.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Information Technology and Telecommunications.
- Government Agencies and Public Sector Bodies.
- Consulting and Professional Services.
- Retail and E-commerce.
- Energy and Utilities.
- Manufacturing and Engineering.

Target Organizations Departments:

- Information Technology Department.
- Internal Audit and Assurance.
- Risk Management Department.
- Legal and Compliance.
- Corporate Governance Office.
- Human Resources.
- Operations Management.
- Procurement and Vendor Management.

Course Offerings:

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

- Develop a comprehensive framework for information security governance.
- Define the scope and applicability of an ISMS in line with organizational goals.
- Master the ISO 27001 requirements, clauses, and control objectives.
- Conduct a thorough information security risk assessment and analysis.
- Develop a risk treatment plan and select appropriate security controls from Annex A.
- Create essential ISMS documentation, including policies and procedures.
- Plan and manage the implementation of an ISO 27001-compliant ISMS.
- Establish metrics for monitoring the performance and effectiveness of the ISMS.
- Prepare the organization for a successful ISO 27001 certification audit.
- Drive a culture of continuous security improvement using the PDCA cycle.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants can translate theoretical knowledge into real-world application. We move beyond traditional lectures to foster a dynamic learning environment where engagement is key. The course heavily relies on a combination of expert-led instruction, detailed case studies drawn from various industries, and collaborative group exercises that simulate the challenges of implementing an ISMS. Participants will engage in hands-on workshops focused on critical processes like risk assessment, control selection, and internal audit planning. Interactive sessions, Q&A panels, and peer-to-peer discussions are integrated throughout the five days to encourage knowledge sharing and problem-solving. Our instructors provide continuous, constructive feedback, guiding participants through complex concepts and ensuring a deep understanding of ISO 27001 principles and governance frameworks. This blended approach ensures that attendees leave not just with knowledge, but with the confidence and practical skills to effectively manage an information security program within their own organizations.

Course Agenda (Course Units):

Unit One: Foundations of Information Security Governance and ISO 27001

- Introduction to Information Security Concepts (Confidentiality, Integrity, Availability).
- The Importance of Information Security Governance.
- Overview of the ISO 27000 Family of Standards.
- Understanding the Structure and Clauses of ISO/IEC 27001.
- Key Terminology and Definitions in the Standard.
- The Business Case for Implementing an ISMS.
- Legal, Regulatory, and Contractual Requirements.

Unit Two: Planning the ISMS and Defining Scope

- Understanding the Organization and its Context (Clause 4).
- Identifying Interested Parties and Their Requirements.
- Defining the Scope and Boundaries of the ISMS.
- Establishing the Information Security Policy.
- Defining Roles, Responsibilities, and Authorities within the ISMS.
- Leadership Commitment and Management Support (Clause 5).
- Introduction to the Plan-Do-Check-Act (PDCA) Model.

Unit Three: Information Security Risk Management

- Actions to Address Risks and Opportunities (Clause 6).
- The ISO 27001 Risk Assessment Process.
- Methods for Information Asset Identification and Valuation.
- Threat and Vulnerability Assessment Techniques.
- Risk Analysis and Evaluation Methodologies.
- The Statement of Applicability (SoA).
- Developing a Comprehensive Risk Treatment Plan.

Unit Four: Implementing ISMS Controls (Annex A)

- Detailed Walkthrough of Annex A Control Objectives and Controls.
- Organizational Controls (A.5).
- People Controls (A.6).
- Physical Controls (A.7).
- Technological Controls (A.8).
- Implementing Security Awareness and Training Programs.
- Documentation Requirements for the ISMS (Clause 7.5).
- Operational Planning and Control (Clause 8).

Unit Five: Monitoring, Auditing, and Continual Improvement

- Monitoring, Measurement, Analysis, and Evaluation (Clause 9).
- Developing Key Performance Indicators (KPIs) for Security.
- The Internal Audit Program for ISO 27001.
- Conducting Management Reviews of the ISMS.
- Managing Nonconformity and Corrective Actions (Clause 10).
- The Principle of Continual Improvement.
- Preparing for the External Certification Audit.

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 an organization leverage its ISO 27001 certified ISMS as a strategic asset for competitive advantage and building customer trust?

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

This course distinguishes itself by focusing on the strategic integration of information security governance with core business objectives, rather than treating ISO 27001 as a mere compliance exercise. While many programs concentrate on the technicalities of the standard, our curriculum emphasizes the "why" behind the "what," enabling participants to build a sustainable and value-driven ISMS. We delve into the nuances of stakeholder management, leadership buy-in, and fostering a security-aware culture, which are critical for long-term success but often overlooked. The methodology is rooted in practical application, utilizing real-world case studies and interactive workshops that challenge participants to solve complex security governance problems. Instead of just reviewing Annex A controls, we guide participants through the process of selecting and justifying controls based on a robust risk assessment, ensuring the ISMS is tailored to the organization's specific threat landscape. This strategic, governance-first approach equips professionals not just to pass an audit, but to become leaders who can champion information security as a key enabler of business resilience and market differentiation.