Implementing ISO/IEC 27701 for Privacy Management Training Course

21 - 25 Dec 2026

Rome

5800 € (Per Person)

Ref: #ISO3173_116292

Course Introduction / Overview:

In an era where data is a critical asset, managing information privacy is no longer optional but a fundamental requirement for organizational success and public trust. This course provides a comprehensive, A-to-Z guide to implementing a Privacy Information Management System (PIMS) based on the ISO/IEC 27701 standard. As an extension to ISO/IEC 27001, this framework offers a robust methodology for protecting Personally Identifiable Information (PII) and demonstrating compliance with global data protection regulations like GDPR and CCPA. We will explore the principles championed by privacy experts such as Dr. Ann Cavoukian, particularly the concept of 'Privacy by Design' which is integral to the standard's philosophy. This program, offered by BIG BEN Training Center, moves beyond theoretical knowledge to provide practical, actionable steps for establishing, implementing, maintaining, and continually improving a PIMS. Participants will learn to navigate the complexities of PII controller and processor obligations, conduct privacy impact assessments, and manage data subject rights effectively, ensuring their organization not only meets legal requirements but also builds a strong culture of privacy. This training is essential for professionals tasked with safeguarding sensitive data and aligning their information security practices with the world's leading privacy standard.

Target Audience / This training course is suitable for:

- Information Security Managers.
- Data Protection Officers (DPOs).
- IT and Corporate Governance Managers.
- Compliance Officers and Managers.
- Internal and External Auditors.
- Privacy and Legal Professionals.
- Consultants specializing in information security and privacy.
- Individuals responsible for managing Personally Identifiable Information (PII).

Target Sectors and Industries:

- Technology and Software Development.
- Financial Services and Banking.
- Healthcare and Medical Institutions.
- Telecommunications and Service Providers.
- Retail and E-commerce.
- Governmental and Public Sector Agencies.
- Consulting and Professional Services.
- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT) and Security.
- Legal and Corporate Compliance.
- Internal Audit and Risk Management.
- Human Resources (HR).
- Operations and Service Delivery.
- Marketing and Customer Relations.
- Procurement and Vendor Management.
- Research and Development.

Course Offerings:

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

- Understand the core principles of a Privacy Information Management System (PIMS).
- Interpret the requirements of ISO/IEC 27701 in relation to ISO/IEC 27001.
- Define the scope and applicability of a PIMS for their organization.
- Differentiate between the roles and responsibilities of PII controllers and PII processors.
- Implement privacy-specific controls from Annex A and Annex B of the standard.
- Conduct a comprehensive privacy risk assessment and impact analysis.
- Develop the necessary documentation for a PIMS, including policies and procedures.
- Align the PIMS with major data protection regulations like GDPR.
- Prepare for and manage an ISO/IEC 27701 certification audit.
- Establish processes for monitoring, measurement, and continual improvement of the PIMS.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants can apply their learning directly to their professional roles. We move beyond traditional lectures by integrating a dynamic blend of expert-led instruction, real-world case study analysis, and collaborative group workshops. Participants will engage in hands-on exercises that simulate the process of implementing a PIMS, from scoping and risk assessment to developing privacy controls and preparing for an audit. Interactive sessions encourage open dialogue, allowing attendees to share challenges and solutions with peers from various industries. Our expert instructors facilitate these discussions, providing personalized feedback and guidance based on their extensive field experience. The curriculum emphasizes a problem-solving approach, where participants work in teams to tackle complex privacy scenarios, reinforcing their understanding of ISO/IEC 27701 requirements. This participant-centered approach ensures a deep and lasting comprehension of the material, equipping attendees with both the knowledge and the confidence to implement an effective Privacy Information Management System within their own organizations.

Course Agenda (Course Units):

Unit One: Foundations of Information Privacy and ISO/IEC 27701

- Introduction to information privacy and data protection principles.
- The relationship between ISO/IEC 27001 and ISO/IEC 27701.
- Understanding key terminology (PIMS, PII, Controller, Processor).
- Overview of the ISO/IEC 27701 standard structure and clauses.
- The business case for implementing a PIMS.
- Mapping ISO/IEC 27701 to global privacy regulations (GDPR, CCPA).
- Exploring the concept of Privacy by Design and by Default.

Unit Two: Planning and Scoping the PIMS

- Defining the scope and boundaries of the Privacy Information Management System.
- Identifying PII controller and PII processor obligations.
- Establishing the PIMS policy and objectives.
- Understanding the context of the organization and interested parties.
- Defining roles, responsibilities, and authorities for privacy management.
- Conducting a privacy-focused risk assessment methodology.
- Performing a Privacy Impact Assessment (PIA).

Unit Three: Implementing PIMS Controls for PII Controllers

- Implementing ISO/IEC 27701 specific guidance for PII Controllers (Annex A).
- Managing consent and transparency with data subjects.
- Fulfilling obligations regarding data subject rights (access, rectification, erasure).
- Implementing controls for PII collection and processing limitation.
- Ensuring data minimization and accuracy.
- Managing PII sharing, transfer, and disclosure.
- Developing procedures for privacy information security incident management.

Unit Four: Implementing PIMS Controls for PII Processors

- Implementing ISO/IEC 27701 specific guidance for PII Processors (Annex B).
- Understanding customer agreements and processing instructions.
- Implementing controls to support customer obligations.
- Managing the use of sub-processors for PII processing.
- Ensuring transparency and cooperation with the PII controller.
- Securely returning or deleting PII upon contract termination.
- Implementing controls for cross-border data transfers.

Unit Five: Monitoring, Auditing, and Continual Improvement

- Monitoring, measuring, analyzing, and evaluating PIMS performance.
- Conducting internal audits for ISO/IEC 27701.
- The management review process for the PIMS.
- Managing nonconformity and implementing corrective actions.
- Strategies for the continual improvement of the PIMS.
- Preparing for the external certification audit process.
- Integrating the PIMS with other management systems.

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 effectively implemented PIMS based on ISO/IEC 27701 become 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 intensely on the practical application and strategic integration of ISO/IEC 27701, rather than merely reciting the standard's clauses. While other programs may provide a theoretical overview, our curriculum is built around a hands-on, implementation-centric framework. We utilize a series of interconnected case studies that evolve throughout the five days, allowing participants to apply concepts in a realistic context, from initial scoping to managing a simulated data breach. This course uniquely bridges the gap between information security (ISO/IEC 27001) and privacy management, providing clear roadmaps for professionals who need to extend their existing ISMS to cover PII protection. Our instructors are seasoned practitioners who bring invaluable insights from real-world PIMS implementations, offering guidance on common pitfalls and success factors that cannot be found in textbooks. The academic rigor is maintained by grounding practical exercises in established principles like 'Privacy by Design', ensuring participants understand not just the 'how' but also the 'why' behind the controls. The emphasis is on developing critical thinking skills to adapt the standard to any organizational context, making it a strategic tool for building trust and competitive advantage, not just a compliance checkbox.