



Certification Partner Global



Presents

ISO/IEC 27701:2025

**Privacy Information Management System
Lead Implementer**

with globally recognized certification from **Exemplar Global, USA**

Schedule

Date: May 18- 22, 2026

Timing: 12:30 PM To 07:30 AM (GMT)
8:30 AM To 3:30 PM (EST)

Mode of training: Online (5 days,7 hours each)



Course Fee:

Regular : USD 799

ISACA/ISC2 Member: USD 699

Early Bird: USD 575

(registering by 30th April 2026)



Registration form: [ISO27701 Lead Implementer](#)



ISO/IEC 27701:2025 Lead Implementer

What is ISO/IEC 27701:2025 Lead Implementer?

- The PIMS Lead Implementer Course is an expert-led program designed to equip professionals with an in-depth understanding of ISO/IEC 27701:2025 requirements and the practical skills needed to implement an effective PIMS within their organization. Through a blend of case studies, interactive exercises, workshops, and audit role-play simulations, participants will gain hands-on experience and develop the competence required to establish robust privacy practices aligned with international standards

The ISO/IEC 27701:2025 Lead Implementer Training course is certified by Exemplar Global, USA

In line with these objectives, we are pleased to announce a 5-day, 7-hour online training & Certification on ISO 27701 LI.



ISO/IEC 27701:2025 Lead Implementer

Who can attend

- Privacy Officers / Data Protection Officer (DPO).
- Information security practitioners and professionals.
- Risk and governance managers.
- Information security management system consultants, security officers and advisors
- Professionals seeking to become certified ISO/IEC 27701 lead implementers.



ISO/IEC 27701:2025 Lead Implementer

Objectives

- Understand the requirements of ISO/IEC 27701:2025 and how it extends the ISO/IEC 27001 for privacy management.
- Learn how to implement and manage a Privacy Information Management System (PIMS) within an organization.
- Understand roles and responsibilities of PII controllers and PII processors in protecting personal data.
- Gain practical knowledge on privacy risk assessment and data protection controls.
- Develop the skills required to plan, implement, monitor, and continually improve a PIMS.
- Prepare participants to lead privacy implementation projects and ensure compliance with global privacy regulations



ISO/IEC 27701:2025 LI Course contents

Day 1 – Foundations of Privacy Governance and PIMS

1. Introduction to Privacy and Data Protection

- Evolution of privacy regulation and global drivers
- Privacy risks in the digital economy
- Privacy governance vs data protection compliance

2. Core Privacy Principles and Frameworks

- ISO/IEC 29100 privacy framework principles
- Fair Information Practice Principles (FIPPs)
- Privacy by design and privacy by default

3. Overview of Privacy Program Management

- Components of a privacy program
- Role of privacy governance and accountability
- Organizational stakeholders in privacy management

4. ISO/IEC 27701:2025 Overview

- Structure and scope of the standard
- Relationship with ISO/IEC 27001 and ISO/IEC 27002

- PII controller vs PII processor requirements

5. Privacy Operational Lifecycle

- Assess • Protect
- Sustain • Respond



ISO/IEC 27701:2025 LI Course contents

Day 2 – PIMS Governance and Organizational Context

1. Context of the Organization
 - Understanding business environment
 - Interested parties and privacy expectations
 - Determining scope of PIMS
2. Leadership and Governance
 - Privacy governance structure
 - Roles and responsibilities (DPO, CPO, privacy engineers)
 - Privacy policy and privacy objectives

3. Risk-Based Approach to Privacy
 - Privacy risk vs security risk
 - Risk management process
 - Privacy impact assessment concepts
4. Integration with Organizational Systems
 - Alignment with ISMS
 - Integration with enterprise risk management
 - Alignment with business strategy

Day 3 – Privacy Engineering and Data Lifecycle Management

1. Privacy Engineering Concepts
 - Privacy engineering lifecycle



ISO/IEC 27701:2025 LI Course contents

- Data minimization, unlinkability, transparency
- Privacy design strategies
- 2. Privacy Architecture Framework
 - ICT systems and privacy architecture
 - Identity and access management layers
 - PII lifecycle management
- 3. Data Lifecycle and Data Governance
 - Data collection
 - Data use and processing
 - Data storage and retention
 - Data destruction
- 4. Privacy by Design Implementation
 - Embedding privacy into systems development lifecycle

- Secure architecture for personal data
- Day 4 – Operational Controls and PIMS Implementation**
1. Operational Controls for Privacy
 - Access control
 - Encryption and de-identification
 - Logging and monitoring
 2. Data Subject Rights Management
 - Consent management
 - Access requests
 - Rectification and deletion



ISO/IEC 27701:2025 LI Course contents

3. Third-Party and Vendor Privacy Management

- Privacy requirements in contracts
- Vendor risk assessments
- Cross-border data transfers

4. Incident and Breach Management

- Privacy incident response lifecycle
- Breach notification requirements
- Post-incident remediation

Day 5 – Monitoring, Improvement, and Certification Readiness

1. Performance Monitoring and Metrics

- Privacy metrics and KPIs
- Internal audits

- Management review

2. Continual Improvement of PIMS

- Corrective actions
- Privacy maturity models
- Privacy culture and training

3. Preparing for Certification

- Certification audit process
- Documentation requirements
- Common implementation pitfalls

4. Integrated Case Study

- End-to-end PIMS implementation scenario

Trainer profile

Ketan Shah,

Cyber Security Professional,
Certified Trainer and Auditor

Results-oriented professional with over 24 years of experience, including 18 years spent developing and implementing effective management systems. Specializing in protecting key assets and processes via the installation of different management systems such as Information Security (ISMS), Business Continuity (BCMS), and Service Management (SMS) across a wide range of organizations in both the commercial and public sectors. Expertise in performing complete risk assessments, guaranteeing compliance with complicated legislation, and integrating many standards and frameworks to achieve maximum effectiveness. Strong analytical, problem-solving, and decision-making talents, along with great communication and interpersonal skills, allow me to manage and motivate teams to achieve strategic security and operational objectives.

Registration form: [ISO27701 Lead Implementer](#)