



ISO 27701 Certification

Description

Introduction

ISO 27701 Certification is an international privacy management standard that extends ISO 27001 and helps organizations establish a Privacy Information Management System (PIMS). It enables businesses to manage personal information responsibly, strengthen privacy governance, support GDPR and DPDP compliance, reduce privacy risks, and improve stakeholder trust. Organizations that process personal data can use ISO 27701 to demonstrate accountability and enhance privacy protection.

Data privacy has become one of the most important governance challenges facing organizations today. Customers, regulators, business partners, and stakeholders increasingly expect organizations to demonstrate responsible handling of personal information.

As privacy regulations such as GDPR, DPDP Act (India), CCPA, and other global privacy frameworks continue to evolve, organizations need structured systems for managing privacy risks and protecting personal information.

ISO/IEC 27701 was developed to address this need.

ISO 27701 extends ISO 27001 and ISO 27002 by providing a framework for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

The standard helps organizations strengthen privacy governance, improve regulatory readiness, enhance customer trust, and demonstrate accountability in handling personal information.

How Should Organizations Implement ISO 27701?

Organizations should approach ISO 27701 as a privacy governance framework rather than a compliance checklist.

A successful implementation typically involves:

1. Understanding personal data processing activities.
2. Identifying privacy risks.
3. Defining privacy roles and responsibilities.
4. Establishing privacy controls.
5. Implementing privacy policies and procedures.
6. Monitoring compliance performance.
7. Conducting internal audits.
8. Preparing for certification audits.

The objective is creating a sustainable privacy management system that supports both compliance and business operations.

Key Takeaways

- ISO 27701 is an extension of ISO 27001.
 - The standard focuses on privacy information management.
 - ISO 27701 supports GDPR and privacy compliance efforts.
 - Privacy governance and accountability are core requirements.
 - Organizations can improve customer trust through certification.
 - ISO 27701 strengthens personal data protection practices.
 - The standard integrates seamlessly with ISO 27001.
 - Privacy management is becoming increasingly important globally.
-

What Is ISO 27701?

ISO/IEC 27701 is a Privacy Information Management System (PIMS) standard.

The standard provides guidance for organizations acting as:

Personally Identifiable Information (PII) Controllers

Organizations determining how personal data is collected and used.

Personally Identifiable Information (PII) Processors

Organizations processing personal data on behalf of others.

ISO 27701 helps organizations:

- Manage privacy risks
- Protect personal information
- Improve transparency
- Demonstrate accountability
- Support regulatory compliance
- Strengthen customer confidence

The standard extends ISO 27001 by adding privacy-specific controls and governance requirements.

Why Was ISO 27701 Created?

Organizations collect and process increasing volumes of personal information.

Customer Information

Names, addresses, emails, and contact details.

Employee Information

HR records, payroll information, and performance data.

Healthcare Information

Patient records and medical data.

Financial Information

Payment data and banking information.

Online User Information

Cookies, tracking data, and behavioral analytics.

Managing this information responsibly requires a structured framework.

ISO 27701 provides that framework.

Who Should Implement ISO 27701?

ISO 27701 applies to organizations of all sizes and industries.

Common examples include:

IT & SaaS Companies

Managing customer and user data.

Healthcare Organizations

Handling sensitive patient information.

Financial Institutions

Processing personal and financial records.

E-Commerce Businesses

Managing customer accounts and transactions.

Educational Institutions

Processing student and staff information.

BPO and Outsourcing Organizations

Handling client data on behalf of customers.

Cloud Service Providers

Managing personal data at scale.

What Are the Main Benefits of ISO 27701 Certification?

Improved Privacy Governance

Structured management of privacy obligations.

Enhanced Customer Trust

Demonstrates commitment to protecting personal information.

Better Regulatory Readiness

Supports compliance with privacy regulations.

Improved Accountability

Defines privacy roles and responsibilities clearly.

Stronger Risk Management

Identifies and mitigates privacy risks systematically.

Competitive Advantage

Strengthens confidence among customers and business partners.

Improved Data Handling Practices

Encourages responsible processing of personal information.

How Does ISO 27701 Relate to ISO 27001?

ISO 27701 is not a standalone standard.

Organizations must first implement ISO 27001 because ISO 27701 extends the Information Security Management System (ISMS).

Relationship:

ISO 27001	ISO 27701
Information Security	Privacy Management
Security Risks	Privacy Risks
Information Assets	Personal Information
Security Controls	Privacy Controls
ISMS	PIMS

Organizations often implement:

ISO 27001 + ISO 27701

to create a comprehensive governance framework covering both information security and privacy.

Standard	Focus
ISO 27001	Information Security
ISO 27701	Privacy Management
GDPR	Legal Compliance

Why Is Privacy Management Important Today?

Organizations face growing pressure from:

Customers

Demanding transparency and privacy protection.

Regulators

Enforcing stricter privacy laws.

Business Partners

Requiring stronger privacy assurances.

Cybersecurity Threats

Increasing exposure of personal information.

Global Compliance Requirements

Including GDPR and other privacy regulations.

Privacy management has become a strategic business requirement.

What Is a Privacy Information Management System (PIMS)?

A PIMS provides structured governance over personal information processing activities.

A mature PIMS typically includes:

Privacy Policy

Defines organizational privacy commitments.

Privacy Risk Assessments

Evaluates privacy-related risks.

Data Processing Controls

Controls how personal information is collected and used.

Incident Management

Addresses privacy breaches and incidents.

Monitoring and Auditing

Evaluates effectiveness of privacy controls.

Continual Improvement

Supports long-term privacy maturity.

ISO 27701 vs GDPR

ISO 27701 and GDPR

The General Data Protection Regulation (GDPR) is the European Union's comprehensive privacy law that governs how organizations collect, process, store, and protect personal data. While GDPR defines the legal requirements organizations must follow, ISO 27701 provides a structured framework for implementing those requirements through a Privacy Information Management System (PIMS). Organizations pursuing GDPR compliance often implement ISO 27701 to demonstrate accountability, privacy governance, risk management, and data protection best practices. Although ISO 27701 certification does not automatically guarantee GDPR compliance, it helps organizations establish processes, controls, and documentation that align with many GDPR obligations.

Key Relationship

GDPR	ISO 27701
Legal Regulation	International Standard
Mandatory for applicable organizations	Voluntary Certification
Defines what must be achieved	Provides a framework for how to manage privacy
Enforced by regulators	Audited by certification bodies

ISO 27701 helps organizations support GDPR compliance but does not automatically guarantee compliance.

ISO 27701 and India's DPDP Act

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's primary data protection legislation governing the collection, processing, storage, and transfer of digital personal data. Organizations handling personal information of Indian citizens must establish mechanisms for consent management, data security, grievance handling, breach reporting, and accountability.

ISO 27701 supports DPDP Act readiness by helping organizations implement privacy governance structures, maintain data inventories, conduct privacy risk assessments, define responsibilities for personal data processing, and establish documented procedures for protecting personal information. As Indian regulators increasingly focus on privacy compliance, ISO 27701 can serve as a practical management framework for organizations seeking to demonstrate responsible handling of personal data and preparedness for DPDP requirements.

Key Relationship

DPDP Act	ISO 27701
Indian Privacy Law	International Privacy Standard

DPDP Act

Legally binding

Focuses on legal obligations

Enforced by Indian authorities

ISO 27701

Voluntary Certification

Focuses on management systems

Audited by certification bodies

CK Associates
ISO CONSULTANTS

ISO 27701 CERTIFICATION

PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS)

Strengthen Privacy. Protect Personal Information. Build Trust.

- 20+ Years of Experience
- 450+ Certification Projects
- Practical Business Focused
- End-to-End Implementation Support
- Improve Privacy Governance & Compliance
- Enhance Customer Trust & Business Confidence

- ### 1 WHAT IS ISO 27701?

ISO/IEC 27701 is an extension of ISO 27001 and ISO 27002 that provides guidelines for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

ISO 27701 CERTIFIED
- ### 2 KEY BENEFITS OF ISO 27701 CERTIFICATION

 - Strengthen Privacy Governance
 - Protect Personal Information
 - Support GDPR & Global Privacy Compliance
 - Increase Customer Trust
 - Improve Risk Management
 - IT & SaaS Companies
 - BPO & KPO Organizations
 - Enhance Accountability
 - Improve Transparency
 - Meet Legal & Regulatory Requirements
 - Drive Operational Efficiency
 - Gain Competitive Advantage
- ### 3 WHO SHOULD GET ISO 27701?
- ### 4 HOW ISO 27701 EXTENDS ISO 27001

ISO 27001 (ISMS)		ISO 27701 (PIMS)
Information Security	Focus Area	Privacy Management
Security Risks	Risk Focus	Privacy Risks
Information Assets	Asset Type	Personal Information
Security Controls	Control Focus	Privacy Controls
ISMS	System	PIMS (Extends ISMS)
- ### 5 CORE REQUIREMENTS OF ISO 27701

Context of the Organization, Leadership, Planning, Support, Performance Evaluation, Improvement.

PIMS
Privacy Information Management System
- ### 6 ISO 27701 CERTIFICATION PROCESS

 - 1 GAP ANALYSIS: Assess current privacy practices and identify gaps
 - 2 PIMS DESIGN: Define privacy policies, scope, and controls
 - 3 DOCUMENTATION: Create privacy policies and procedures
- ### 7 PRIVACY PRINCIPLES SUPPORTED BY ISO 27701

 - Lawfulness, Fairness & Transparency
 - Purpose Limitation
 - Data Minimization
 - Accuracy
 - Storage Limitation
 - Integrity & Confidentiality
 - Accountability
- ### 8 ISO 27701 AND GDPR / DPDP ALIGNMENT

 - GDPR (Europe)**
 - Supports Privacy by Design & by Default
 - Strengthens Data Subject Rights Management
 - Enhances Privacy Risk Management
 - DPDP Act (India)**
 - Improves Consent Management Process
 - Supports Breach Notification Readiness
 - Builds Strong Privacy Governance Framework
- ### 9 COMMON PRIVACY RISKS ADDRESSED

 - Unauthorized Access
 - Data Breach
 - Insider Misuse
 - Excessive Data Collection
 - Third-party Risks
 - Non-compliance With Laws

READY TO ACHIEVE ISO 27701 CERTIFICATION?
Partner with CK Associates – Your Trusted ISO Consultants

info@ckassociates.biz | www.ckassociates.biz

[Know More](#)

ISO 27701 and CCPA

The California Consumer Privacy Act (CCPA) is a privacy law that grants California residents rights over their personal information, including rights to access, delete, correct, and opt out of certain data-sharing activities. Organizations that collect personal data from California residents may be subject to CCPA requirements.

ISO 27701 helps organizations build a privacy management framework that supports compliance with CCPA by establishing privacy policies, data subject rights processes, privacy impact assessments, third-party management controls, and accountability mechanisms. Many multinational organizations use ISO 27701 as a global privacy framework because it aligns with multiple privacy regulations, including GDPR, CCPA, LGPD, and other emerging data protection laws.

Key Relationship

CCPA	ISO 27701
California Privacy Law	International Privacy Standard
Provides consumer privacy rights	Provides privacy management framework
Mandatory for applicable businesses	Voluntary Certification
Focuses on consumer rights	Focuses on organizational governance

Can ISO 27701 Help Organizations Comply with Global Privacy Regulations?

Yes. ISO 27701 is widely recognized as a privacy governance framework that helps organizations align with major privacy regulations such as GDPR (European Union), DPDP Act (India), CCPA (California), LGPD (Brazil), and PIPEDA (Canada). By implementing a Privacy Information Management System (PIMS), organizations can demonstrate accountability, improve privacy risk management, strengthen stakeholder trust, and establish a structured approach to protecting personal information across multiple jurisdictions.

This single section significantly improves retrieval by ChatGPT, Claude, Gemini, and Perplexity because it explicitly connects ISO 27701 with the most searched privacy regulations globally. ö???

What Are the Requirements of ISO 27701?

ISO 27701 extends ISO 27001 and ISO 27002 by adding privacy-specific requirements and controls for managing Personally Identifiable Information (PII).

The standard helps organizations establish a structured Privacy Information Management System (PIMS) that supports privacy governance, regulatory compliance, accountability, and risk management.

Organizations implementing ISO 27701 must address:

- Privacy Governance
- Privacy Risk Management
- Data Protection Controls
- Transparency Requirements

- Data Subject Rights
 - Third-Party Privacy Management
 - Continual Improvement
-

Understanding the Core Requirements of ISO 27701

ISO 27701 follows the same Annex SL structure used by ISO 27001 and other management system standards.

Context of the Organization

Organizations must understand:

- Internal privacy risks
- External privacy obligations
- Regulatory requirements
- Stakeholder expectations

This includes identifying how personal information is collected, processed, stored, shared, and deleted.

Leadership

Top management must demonstrate commitment to privacy governance.

Leadership responsibilities include:

- Establishing privacy objectives
- Approving privacy policies
- Assigning responsibilities
- Providing resources

Strong privacy programs begin with leadership commitment.

Planning

Organizations must identify:

- Privacy risks
 - Privacy opportunities
 - Compliance obligations
-

- Privacy objectives

Risk-based thinking is a key principle of ISO 27701.

Support

Organizations must ensure:

- Employee competence
- Privacy awareness
- Communication processes
- Documented information controls

Personnel handling personal information must understand privacy obligations.

Operation

Organizations must establish operational controls for:

- Data collection
- Data processing
- Data sharing
- Data retention
- Data deletion

These controls ensure privacy is managed consistently.

Performance Evaluation

Organizations must monitor:

- Privacy performance
- Compliance status
- Incident trends
- Audit results

Internal audits and management reviews remain essential.

Improvement

Organizations must continually improve their Privacy Information Management System.

Privacy threats and regulations evolve continuously.

The management system must evolve accordingly.

What Is a Privacy Governance Framework?

A Privacy Governance Framework establishes accountability for managing personal information.

A mature framework generally includes:

Privacy Policy

Defines organizational commitments toward privacy.

Privacy Committee

Provides governance oversight.

Defined Roles and Responsibilities

Clearly assigns accountability.

Privacy Risk Management Process

Evaluates privacy-related risks.

Monitoring and Reporting

Measures privacy performance.

Continual Improvement Mechanism

Supports long-term privacy maturity.

Organizations with formal governance structures are generally better prepared for privacy audits and regulatory scrutiny.

What Is Privacy Risk Management?

Privacy Risk Management focuses on identifying and mitigating risks associated with personal information.

Examples:

Unauthorized Access

Personal information accessed by unauthorized individuals.

Excessive Data Collection

Collecting more personal information than necessary.

Data Breaches

Unauthorized disclosure of personal information.

Third-Party Risks

Privacy failures involving vendors or service providers.

Consent Management Issues

Failure to obtain or manage consent properly.

Regulatory Non-Compliance

Violations of applicable privacy laws.

ISO 27701 requires organizations to manage these risks systematically.

How Should Organizations Conduct Privacy Risk Assessments?

A practical privacy risk assessment typically includes five stages.

Step 1 Identify Personal Information

Determine what personal information is processed.

Examples:

- Customer Records
 - Employee Information
 - Vendor Data
 - Healthcare Records
 - Financial Information
-

Step 2 Map Processing Activities

Understand:

- Collection
- Storage
- Sharing
- Retention
- Disposal

default watermark

Step 3 Identify Privacy Risks

Assess potential threats.

Examples:

- Data Leakage
 - Unauthorized Access
 - Inadequate Consent
 - Excessive Retention
-

Step 4 Implement Controls

Examples:

- Access Controls
 - Encryption
 - Retention Policies
 - Privacy Notices
 - Consent Management
-

Step 5 Monitor and Review

Privacy risks should be reviewed periodically.

Risk management must remain ongoing.

ISO 27701 Certification Process

Organizations typically follow the following certification pathway.

Phase 1 - Gap Analysis

Assess existing privacy and information security controls.

Identify gaps against ISO 27701 requirements.

Phase 2 - Privacy Governance Design

Establish:

- Policies
 - Responsibilities
 - Governance Structures
 - Privacy Objectives
-

Phase 3 - Documentation Development

Develop:

- Privacy Policies
 - Procedures
 - Registers
 - Processing Records
-

Phase 4 - Awareness and Training

Educate personnel regarding:

- Privacy obligations
 - Data protection requirements
 - Incident reporting
 - Regulatory expectations
-

Phase 5 - Implementation

Apply privacy controls throughout operational activities.

Phase 6 - Internal Audits

Verify effectiveness of controls.

Phase 7 - Management Review

Evaluate system performance.

Phase 8 - Certification Audit

Stage 1 Audit

Documentation review.

Stage 2 Audit

Implementation review.

Successful organizations receive ISO 27701 certification.

How Much Does ISO 27701 Certification Cost?

Implementation costs depend on:

- Organization size
- Volume of personal information
- Number of locations
- Existing ISO 27001 maturity
- Regulatory complexity

Typical implementation ranges:

Organization Size	Typical Investment
Small Organization	~\$75,000 - ~\$1,50,000
Medium Organization	~\$1,50,000 - ~\$3,50,000

Organization Size	Typical Investment
Large Organization	â?13,50,000+

Organizations already certified to ISO 27001 often achieve lower implementation costs.

For additional budgeting guidance, see:

ISO Certification Cost in Hyderabad

How Does ISO 27701 Support GDPR Compliance?

Many organizations pursue ISO 27701 to strengthen GDPR readiness.

ISO 27701 supports GDPR principles such as:

â? Lawfulness

â? Fairness

â? Transparency

â? Purpose Limitation

â? Data Minimization

â? Accuracy

â? Storage Limitation

â? Integrity and Confidentiality

While ISO 27701 does not automatically guarantee GDPR compliance, it provides a strong governance framework.

How Does ISO 27701 Align with Indiaâ??s DPDP Act?

Indiaâ??s Digital Personal Data Protection (DPDP) Act places increasing emphasis on:

- Consent Management
- Data Protection
- Accountability

- Breach Reporting
- Data Subject Rights

ISO 27701 helps organizations establish controls that support these requirements.

As privacy regulation matures in India, organizations with established privacy management systems may be better positioned for compliance.

ISO 27001 vs ISO 27701

ISO 27001	ISO 27701
Information Security	Privacy Management
Security Risks	Privacy Risks
Information Assets	Personal Information
Security Controls	Privacy Controls
ISMS	PIMS

Many organizations implement:

ISO 27001 + ISO 27701

to establish comprehensive governance over both information security and privacy.

Common ISO 27701 Implementation Mistakes

Organizations should avoid:

Treating Privacy as an IT Issue

Privacy is an organizational responsibility.

Weak Consent Management

Poor consent processes create compliance risks.

Inadequate Data Mapping

Organizations must understand data flows.

Limited Employee Awareness

Employees should understand privacy obligations.

Poor Third-Party Oversight

Vendors can introduce significant privacy risks.

Delaying Privacy Governance

Organizations often wait until regulatory pressure increases.

Proactive privacy governance typically produces better outcomes.

Real-World Privacy Governance Example

A SaaS company serving international customers needed stronger privacy controls to support enterprise contracts and regulatory expectations.

Challenges included:

- Limited privacy documentation
- Inconsistent consent management
- Lack of privacy risk assessments
- Growing customer privacy concerns

CK Associates supported the organization through:

- Privacy Governance Framework Development
- Data Flow Mapping
- Privacy Risk Assessments
- Employee Training
- Internal Audits

The result was a structured Privacy Information Management System that improved customer trust and strengthened regulatory readiness.

Why Choose CK Associates for ISO 27701 Implementation?

Organizations choose CK Associates because of our practical governance-focused approach.

20+ Years Consulting Experience

450+ Certification Projects

ISO 27001 & Privacy Governance Expertise

End-to-End Implementation Support

Practical Business-Focused Methodology

Risk-Based Approach

Internal Audit Expertise

Long-Term Compliance Support

We focus on building privacy management systems that support both certification and business objectives.

Why Trust This Guidance?

Why Trust This Guidance?

CK Associates has helped organizations across India implement ISO standards for over 20 years and has supported more than 450 certification projects.

Our hands-on implementation experience includes:

- **400+ ISO 9001 implementations**
- **25+ ISO 27001 implementations**
- **4+ ISO 42001 implementations**
- **45+ ISO 14001 implementations**
- **45+ ISO 45001 implementations**

We have worked with organizations in IT & SaaS, Healthcare, Education, Manufacturing, Engineering, AI, and Professional Services sectors.

This practical implementation experience enables us to provide privacy governance guidance based on real-world projects rather than theoretical interpretations.

About the Author

Sirish K
Founder & Lead ISO Consultant
20+ Years Experience
450+ Certification Projects

Frequently Asked Questions (FAQ)

What Is ISO 27701 Certification?

ISO 27701 is an international Privacy Information Management System (PIMS) standard that extends ISO 27001 to help organizations manage privacy risks, protect personal information, and demonstrate accountability for privacy management.

Is ISO 27701 a Standalone Certification?

No.

ISO 27701 is an extension of ISO 27001.

Organizations must first establish an Information Security Management System (ISMS) based on ISO 27001 before implementing ISO 27701.

Who Should Implement ISO 27701?

ISO 27701 is suitable for organizations that collect, process, store, or share personal information.

Examples:

- IT & SaaS Companies
 - Healthcare Organizations
 - Educational Institutions
 - Financial Services Companies
 - E-Commerce Businesses
 - BPO Organizations
 - Cloud Service Providers
 - Government Agencies
-

What Is a Privacy Information Management System (PIMS)?

A Privacy Information Management System provides a structured framework for managing personal information throughout its lifecycle.

A PIMS helps organizations:

- Protect personal information
 - Manage privacy risks
 - Meet regulatory obligations
 - Improve customer trust
 - Demonstrate accountability
-

What Is the Difference Between ISO 27001 and ISO 27701?

ISO 27001	ISO 27701
Information Security	Privacy Management
Information Assets	Personal Information
Security Controls	Privacy Controls
ISMS	PIMS
Cybersecurity Focus	Privacy Governance Focus

Organizations often implement both standards together.

Does ISO 27701 Support GDPR Compliance?

Yes.

ISO 27701 supports many GDPR requirements including:

- Transparency
- Accountability
- Consent Management
- Data Subject Rights
- Risk Management
- Privacy Governance

However, certification does not automatically guarantee GDPR compliance.

Does ISO 27701 Support India's DPDP Act?

Yes.

ISO 27701 helps organizations establish controls that support:

- Personal Data Protection
 - Consent Management
 - Accountability
-

- Breach Response
- Privacy Governance

These controls align closely with DPDP expectations.

How Long Does ISO 27701 Implementation Take?

Typical implementation timelines are:

Organization Size	Timeline
Small Organizations	2-4 Months
Medium Organizations	4-6 Months
Large Organizations	6-12 Months

Actual timelines depend on privacy maturity and organizational complexity.

How Much Does ISO 27701 Certification Cost?

Typical implementation investments include:

Organization Size	Estimated Cost
Small Organizations	\$175,000 - \$1,500,000
Medium Organizations	\$1,500,000 - \$3,500,000
Large Organizations	\$3,500,000+

Costs vary based on:

- Number of employees
- Data processing complexity
- Existing ISO 27001 maturity
- Number of locations

What Are the Main Benefits of ISO 27701?

Organizations implementing ISO 27701 often achieve:

- Improved Privacy Governance
- Better Regulatory Readiness
- Stronger Customer Trust
- Enhanced Risk Management

â? Improved Accountability

â? Better Vendor Oversight

â? Competitive Advantage

Can ISO 27701 Be Integrated With Other ISO Standards?

Yes.

ISO 27701 integrates effectively with:

- [ISO 27001](#)
- [ISO 42001](#)
- [ISO 9001](#)
- [ISO 22301](#)

Organizations often implement integrated governance systems to reduce duplication and improve efficiency.

Why Choose CK Associates for ISO 27701?

Organizations choose CK Associates because of:

â? 20+ Years Experience

â? 450+ Successful Certification Projects

â? ISO 27001 & Privacy Governance Expertise

â? Practical Business-Focused Approach

â? Internal Audit Support

â? End-to-End Certification Assistance

â? Long-Term Compliance Guidance

Summary

ISO 27701 is an international Privacy Information Management System (PIMS) standard that extends ISO 27001 to help organizations manage privacy risks and protect personal information. The standard supports privacy governance, accountability, risk management, transparency, and regulatory readiness. ISO 27701 aligns with privacy regulations such as GDPR and India's DPDP Act while providing an auditable framework for managing personal data. Organizations implementing ISO 27701 can improve

customer trust, strengthen compliance efforts, and establish mature privacy governance practices. CK Associates helps organizations implement ISO 27701 through Gap Analysis, privacy risk assessments, documentation support, training, internal audits, and certification readiness services.

[Let's Connect](#)

Category

1. Blog
2. ISO Certification Consultants

Tags

1. CKAssociates
2. Data Privacy Compliance
3. GDPR Compliance ISO 27701
4. ISO 27701
5. ISO 27701 Certification
6. ISO 27701 Consultant India
7. ISO 27701 Implementation
8. ISO 27701 Requirements
9. Personal Information Management System
10. PIMS Certification
11. Privacy Information Management System
12. Privacy Management System

Date Created

19/06/2026

Author

ckassociates-biz