



ISO 27701 Certification: Complete Privacy Guide?

Description

What Is ISO 27701 Certification?

ISO/IEC 27701 is an international standard for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS). It helps organisations manage personally identifiable information (PII) through defined responsibilities, documented processes, risk-based controls, operational practices and continual improvement.

The current edition, ISO/IEC 27701:2025, is a standalone management system standard. It can be relevant to organisations that determine how personal information is processed and organisations that process personal information on behalf of others. This includes IT companies, SaaS providers, business process outsourcing firms, service providers and other organisations handling personal data.

For Indian organisations, ISO 27701 can support structured privacy governance alongside applicable legal obligations, including the Digital Personal Data Protection Act, 2023, and its associated rules. However, certification does not automatically establish compliance with every applicable privacy law. The organisation must assess its legal obligations, processing activities, contractual commitments and operational risks.

What Does ISO 27701 Certification Mean?

ISO 27701 certification demonstrates that an organisation's Privacy Information Management System has been assessed against the applicable requirements of ISO/IEC 27701. It provides a structured way to manage personal information, define privacy responsibilities, address privacy risks, maintain supporting evidence and improve privacy practices over time.

Key Takeaways

- **ISO/IEC 27701:2025 is the current edition** and is published as a standalone management system standard.

- A Privacy Information Management System helps integrate privacy responsibilities into everyday business operations.
- Organisations that act as personal information controllers or processors may find the standard relevant.
- ISO 27701 and ISO 27001 address related but different management objectives: privacy management and information security.
- A successful implementation requires more than policies. It needs operational controls, assigned responsibilities, records and evidence.
- Certification does not replace legal advice or automatically guarantee compliance with the Indian DPDP Act or other privacy laws.
- The implementation schedule and certification cost depend on the organisation's size, complexity, data processing activities, existing controls and certification arrangements.

Introduction: Why Privacy Management Needs a Structured System

Organisations collect and process personal information every day. Customer contact details, employee records, website enquiries, identity information, support tickets, recruitment data and account information all create responsibilities for the organisation handling them.

These responsibilities become more complex when information moves between departments, cloud platforms, external service providers, business partners and customers in different jurisdictions.

A privacy policy on a website is not enough to demonstrate that an organisation manages personal information consistently. Management needs to understand what data is processed, why it is processed, who is responsible, how risks are addressed and whether established procedures are actually followed.

This is where a Privacy Information Management System becomes valuable.

ISO 27701 certification provides a recognised framework for demonstrating that privacy management is treated as a formal organisational discipline rather than an isolated documentation exercise.

For businesses in Hyderabad and across India, this can be particularly relevant when serving enterprise customers, handling outsourced business processes, developing software products or entering contracts that require evidence of structured privacy governance.

The objective is not simply to obtain a certificate. It is to build a management system that can be maintained, measured, audited and improved.

1. What Is ISO/IEC 27701?

ISO/IEC 27701 is an international standard titled *Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance*.

The standard specifies requirements for establishing, implementing, maintaining and continually improving a Privacy Information Management System. It also provides guidance to help organisations put those requirements into practice.

The standard is intended for organisations responsible for processing personally identifiable information (PII), including PII controllers and PII processors. It applies to different types and sizes of organisations, including private businesses, public-sector entities and not-for-profit organisations.

What is a Privacy Information Management System?

A Privacy Information Management System, or PIMS, is a structured framework through which an organisation manages privacy-related responsibilities and processes.

Depending on the organisation's activities and scope, the system may include:

- Privacy policies and defined responsibilities.
- Identification of personal information processing activities.
- Assessment and treatment of privacy risks.
- Controls for the collection, use, sharing, retention and disposal of personal information.
- Supplier and processor oversight.
- Employee awareness and role-based training.
- Procedures for handling privacy incidents and complaints.
- Internal audits, management reviews and corrective actions.
- Monitoring and continual improvement.

The exact controls and documented information required should be determined by the standard, the organisation's scope and its actual processing activities. A generic template set is not a substitute for this assessment.

ISO/IEC 27701:2025 – understanding the current edition

Organisations planning implementation should distinguish between the previous 2019 edition and the current 2025 edition.

ISO/IEC 27701:2025 was published on 14 October 2025 as Edition 2. ISO lists ISO/IEC 27701:2019 as withdrawn and ISO/IEC 27701:2025 as the published edition.

A significant point is that the 2025 edition is a **standalone management system standard**. Businesses should therefore avoid relying uncritically on older guidance that describes ISO 27701 solely as an extension of ISO 27001.

Before beginning a new implementation or planning a transition from an existing certificate, confirm the applicable edition, certification scope and requirements with the chosen certification body.

Official reference: [ISO/IEC 27701:2025](#).

2. Why Do Organisations Consider ISO 27701 Certification?

Privacy management affects customer confidence, business continuity, supplier relationships and the ability to demonstrate accountability.

ISO 27701 can help organisations address these needs through a defined management system.

2.1 Demonstrating a structured approach to privacy

Customers and business partners may ask how an organisation manages personal information. They may want to understand the organisation's responsibilities, procedures, risk assessments and incident-handling arrangements.

A PIMS creates a structured way to answer these questions using defined processes and supporting evidence.

2.2 Supporting enterprise procurement and vendor assessments

Large customers often evaluate suppliers on information security, privacy, regulatory exposure and operational maturity.

A relevant certification may support a supplier's assurance package, although acceptance depends on the customer's requirements, the certification's scope and the specific services being provided.

It does not guarantee a contract or eliminate the need for customer-specific due diligence.

2.3 Improving accountability

Privacy responsibilities can become unclear when legal, HR, IT, sales, customer support and operations handle personal information independently.

A management system helps assign ownership and define how teams work together. This makes it easier to identify responsibility for decisions, approvals, risk treatment and corrective action.

2.4 Managing third-party and cloud-service risks

Personal information may be stored or processed by cloud providers, software vendors, payroll partners, recruitment platforms and outsourced service providers.

A PIMS can help an organisation establish supplier evaluation criteria, define contractual expectations, review risks and monitor relevant service arrangements.

2.5 Supporting continual improvement

Privacy risks change as the organisation launches new products, adopts new technology, enters new markets or changes how it uses personal information.

A management system provides a repeatable method for reviewing changes, identifying weaknesses, implementing corrective action and assessing whether improvements are effective.

3. Who Should Consider ISO 27701 Certification?

ISO 27701 can be relevant to organisations of different sizes and sectors. Suitability depends on the personal information processed, customer expectations, legal obligations and business objectives.

Organisation type	Potential privacy management priority
IT and software development companies	Personal data in applications, customer environments and support systems
SaaS providers	Account information, user data, integrations and cloud processing
BPO and business process service providers	Personal information processed under customer contracts
HR and recruitment businesses	Candidate records, employee information and recruitment workflows
Healthcare service providers	Patient-related and employee information, subject to applicable laws
Financial and professional services	Customer records, identity information and confidential business processes
E-commerce businesses	Customer accounts, order information and service communications
Marketing and customer engagement firms	Contact lists, campaign data, tracking practices and customer preferences
Data-processing and cloud service providers	Processing instructions, access controls and third-party responsibilities
Large enterprises and multi-location organisations	Consistent privacy governance across business units and suppliers

Small and medium-sized businesses can also consider the standard when their processing activities or customer commitments justify it.

The key question is not simply how many employees an organisation has. It is how personal information is processed, what responsibilities the organisation holds and what assurance its customers or other stakeholders require.

4. Understanding PII Controllers and PII Processors

A practical ISO 27701 implementation begins by identifying the organisation's role in each processing activity.

The terms used in ISO standards and privacy legislation are not always identical. Organisations should apply the definitions relevant to the standard and the laws that govern their activities.

4.1 What is a PII controller?

A PII controller is an entity that determines the purposes and means of processing personally identifiable information, as defined in the applicable standard and context.

For example, an organisation that decides why it collects customer information, what information is needed and how it will be used may be acting as a controller for that activity.

Responsibilities may include defining permitted processing, establishing relevant notices and procedures, determining retention requirements and ensuring that appropriate safeguards are applied.

4.2 What is a PII processor?

A PII processor processes personal information on behalf of another organisation, according to the applicable arrangement and instructions.

For example, a service provider managing a customer's database or processing employee records under contract may act as a processor for those activities.

Responsibilities may include following authorised instructions, controlling access, managing subcontractors, maintaining evidence, reporting relevant incidents and supporting the customer with agreed privacy obligations.

4.3 Why role identification matters

One organisation may be a controller for some activities and a processor for others.

For example, an IT service provider may process its customer's personal information when delivering a managed service, while acting in its own capacity when managing recruitment records for its employees.

Consequently, organisations should not assign a single privacy role to the entire business without analysing its actual processing activities.

A useful starting point is a processing inventory that records:

- The type of personal information involved.
- The purpose of processing.
- The individuals concerned.
- The organisation's role in the activity.
- The systems and locations involved.
- Internal teams and external parties with access.
- Applicable retention and deletion arrangements.
- Relevant risks, contracts and safeguards.

This inventory provides a foundation for the subsequent risk assessment and control design.

PEOPLE | PROCESS | PRIVACY | TRUST

ISO/IEC 27701:2025

PRIVACY INFORMATION MANAGEMENT SYSTEM

Protect Personal Data.
Strengthen Privacy Governance.

Managed Privacy Responsibilities | Controlled Personal Data Processing | Reduced Privacy Risks | Stronger Compliance

www.ckassociates.biz | +91 98853 07909 | Your Partner for

The banner features a dark blue background with a city skyline at night. On the right, there is a large, glowing shield icon with a fingerprint and a padlock inside. Above the shield are icons for people, a document, and a database. The text 'ISO/IEC 27701:2025' is prominently displayed in white and green. Below it, the words 'PRIVACY INFORMATION MANAGEMENT SYSTEM' are in white. Further down, the tagline 'Protect Personal Data. Strengthen Privacy Governance.' is shown. At the bottom, there are four circular icons representing different aspects of the system: people, document, shield, and gear. The footer contains the website URL, phone number, and a partial tagline.

5. ISO 27701 vs ISO 27001: What Is the Difference?

ISO 27701 and ISO 27001 are related, but they are not interchangeable.

ISO/IEC 27001 focuses on an Information Security Management System (ISMS). ISO/IEC 27701 focuses on a Privacy Information Management System (PIMS).

Information security and privacy overlap, but they address different questions.

Area	ISO/IEC 27001	ISO/IEC 27701
Primary objective	Manage information security risks	Establish and improve privacy information management
Main management focus	Confidentiality, integrity and availability of information	Responsible management of personally identifiable information
Typical questions	Is information protected from unauthorised access, alteration or loss?	Are personal information processing activities governed and managed appropriately?
Scope considerations	Information security risks within the defined ISMS scope	Privacy risks and responsibilities within the defined PIMS scope
Operational emphasis	Security risk assessment, treatment and controls	Privacy governance, processing responsibilities and related controls
Potential business value	Demonstrates a structured approach to information security	Demonstrates a structured approach to privacy management

The precise requirements and applicability must be assessed against the current editions of the standards.

Can an organisation implement ISO 27701 without ISO 27001?

Yes. ISO/IEC 27701:2025 is a standalone management system standard according to ISO’s official publication information.

However, that does not mean an organisation can ignore information security. Privacy management depends on suitable safeguards, and many privacy risks are closely connected to security risks.

An organisation should evaluate the requirements of the 2025 edition and determine which security measures and related management processes are necessary for its PIMS.

Should a business implement both standards?

Some organisations may benefit from implementing ISO 27001 and ISO 27701 together, particularly when they manage substantial amounts of customer information or need to demonstrate both security and privacy governance.

An integrated approach may reduce duplication in areas such as risk management, document control, competence, internal audit and management review. Integration should still preserve the distinct requirements and objectives of each system.

Organisations already certified to ISO 27001 should not assume that their existing certificate automatically covers ISO 27701. They should conduct a separate gap assessment against ISO/IEC 27701:2025.

6. ISO 27701 and India's Digital Personal Data Protection Framework

Indian organisations need to consider privacy management in the context of applicable Indian laws and any other jurisdictions in which they operate.

The Digital Personal Data Protection Act, 2023, establishes a framework for processing digital personal data in India. The Government of India notified the Digital Personal Data Protection Rules, 2025, on 14 November 2025. The official framework includes phased commencement arrangements, so organisations should verify which provisions and obligations apply to them at the relevant time.

Official references:

- [MeitY's Digital Personal Data Protection Rules, 2025](#)
- [Press Information Bureau's DPDP Rules, 2025 notified](#)

How can ISO 27701 support privacy readiness?

A PIMS can help an organisation establish repeatable processes for activities such as:

- Identifying personal data processing activities.
- Assigning responsibilities and accountability.
- Documenting purposes and processing arrangements.
- Reviewing data collection and use practices.
- Managing retention and deletion.
- Assessing risks and implementing safeguards.
- Managing third-party processing relationships.
- Establishing procedures for incidents and complaints.
- Maintaining evidence and reviewing performance.

These activities can support a broader privacy compliance programme when they are mapped to the organisation's actual legal obligations.

Does ISO 27701 certification mean DPDP Act compliance?

No. ISO 27701 certification does not automatically establish compliance with the DPDP Act or every other applicable privacy law.

A management system standard and a legal framework have different purposes. An organisation must identify the laws that apply to its processing activities and assess its obligations under those laws.

Legal applicability may depend on the organisation's role, the type of data involved, the processing purpose, the individuals concerned, the relevant commencement provisions and any applicable exemptions or special requirements.

For that reason, a sound implementation should combine management system requirements with a separate, current legal obligations assessment. Legal questions should be reviewed by appropriately qualified professionals.

7. How to Implement ISO 27701: A Practical Roadmap

ISO 27701 implementation should be based on the organisation's real operations rather than a generic checklist. The following roadmap provides a practical sequence for planning the project.

Step 1: Define the PIMS scope

Identify the business units, services, processes, locations, systems and personal information processing activities to be included.

Consider customer requirements, outsourced activities, cloud environments, business partners and interfaces with other management systems.

A scope that is too narrow may fail to address important processing activities. A scope that is unnecessarily broad may make implementation more complex than required.

Expected output: A documented scope statement and an understanding of the boundaries and applicability of the PIMS.

Step 2: Conduct a gap assessment

Compare current practices with the requirements of ISO/IEC 27701:2025.

Review existing policies, contracts, processing inventories, risk assessments, training records, incident procedures, supplier arrangements and audit evidence.

Record each gap, its significance, the action needed, the responsible owner and the planned completion date.

Expected output: A prioritised gap assessment and implementation action plan.

Step 3: Identify processing activities and responsibilities

Create or improve the inventory of personal information processing activities.

Identify the information collected, why it is used, the individuals concerned, the systems involved, the recipients, the organisation's role and the relevant retention arrangements.

Where third parties are involved, identify the nature of their access and responsibilities.

Expected output: A maintained processing inventory with assigned ownership and supporting information.

Step 4: Assess privacy risks and applicable obligations

Evaluate the risks associated with processing activities. Consider unauthorised access, excessive collection, inaccurate information, inappropriate disclosure, unclear responsibilities, inadequate retention practices and weaknesses in supplier arrangements.

Determine applicable legal, contractual and customer requirements. Link the assessment to documented decisions about risk treatment and controls.

A risk assessment should be proportionate to the organisation's activities and should be updated when material changes occur.

Expected output: Documented risk assessments, treatment decisions and a register of relevant obligations.

Step 5: Establish policies and operational procedures

Develop or revise the documentation needed to operate the PIMS effectively.

Depending on the organisation and applicable requirements, this may include privacy policies, processing procedures, access and authorisation arrangements, retention rules, incident escalation procedures, supplier management processes and responsibilities for handling privacy-related requests.

Documentation should reflect actual practices. A policy that employees cannot follow or that contradicts system configurations creates a gap rather than evidence of effective control.

Expected output: Approved policies, procedures and clearly assigned responsibilities.

Step 6: Implement the necessary controls

Translate the risk treatment decisions into operational measures.

Examples may include restricting access to personal information, reviewing access permissions, controlling information sharing, evaluating suppliers, maintaining appropriate logs, applying retention rules and ensuring that approved procedures are followed.

The specific controls should be selected according to the standard's requirements, applicable obligations and the organisation's risk assessment.

Expected output: Controls implemented in relevant systems and business processes, supported by evidence.

Step 7: Train employees and relevant stakeholders

Employees should understand their responsibilities for the personal information they handle.

Training can cover acceptable handling practices, access restrictions, approved sharing methods, incident reporting, confidentiality obligations, retention requirements and escalation routes.

Training should be relevant to employees' roles. A developer, HR executive, customer support representative and senior manager may have different privacy responsibilities.

Expected output: Training materials, attendance records, awareness evidence and arrangements for ongoing competence.

Step 8: Conduct internal audits

Internal audits evaluate whether the management system meets applicable requirements and is operating as intended.

Audit planning should consider the importance of the processes, previous findings, operational changes and relevant risks. Auditors should gather objective evidence rather than rely solely on policy documents or verbal assurances.

Where findings are identified, the organisation should record them and manage the required corrective action.

Expected output: An internal audit programme, audit records, findings and corrective-action tracking.

Step 9: Complete management review

Management review gives leadership an opportunity to evaluate the PIMS's performance and continued suitability.

Inputs may include audit findings, progress against objectives, changes in the organisation's context, incidents, stakeholder feedback, risk treatment status and improvement opportunities.

Decisions should be documented and assigned to responsible owners.

Expected output: Management review records and actions with clear accountability.

Step 10: Prepare for certification assessment

Before arranging the certification assessment, confirm that the PIMS has been implemented and that sufficient evidence exists to demonstrate its operation.

The organisation should verify the certification body’s accreditation and scope, understand the assessment process, confirm the applicable standard edition and agree on the scope to be assessed.

Certification should be treated as an independent assessment of the management system, not merely as a documentation review.

Expected output: An organised audit evidence set, confirmed assessment arrangements and a process for addressing findings.

8. What Documents and Evidence May Be Needed?

There is no single universal document list that fits every organisation. Required documented information depends on the applicable requirements, scope, risks, processing activities and operational context.

The following examples can help businesses prepare.

Area	Examples of supporting evidence
PIMS governance	Scope statement, assigned responsibilities, approved policies and objectives
Processing activities	Personal information inventory, processing descriptions and role identification
Risk management	Risk assessments, treatment plans and records of decisions
Legal and contractual obligations	Applicable obligations register, relevant contracts and review records
Access and handling	Access approvals, review records and operational procedures
Suppliers and processors	Supplier assessments, agreements, review records and follow-up actions
Retention and disposal	Retention criteria, disposal procedures and relevant evidence
Incidents	Incident-handling procedures, records and corrective actions, where applicable
Employee competence	Training materials, attendance records and awareness activities
Monitoring and audit	Monitoring records, internal audit reports and findings
Management oversight	Management review records, decisions and assigned actions
Continual improvement	Corrective-action tracking, effectiveness checks and improvement records

These are illustrative examples, not a definitive list of mandatory documents. Organisations should map their evidence to the actual requirements of ISO/IEC 27701:2025.

A common mistake is to prepare documents only for the certification assessment. A stronger approach is to maintain evidence as part of normal operations, so records accurately reflect what the organisation does.

9. ISO 27701 Certification Audit Readiness

Audit readiness means being able to demonstrate that the PIMS is defined, implemented, maintained and evaluated.

A well-prepared organisation should be able to explain its privacy responsibilities and show how they work in practice.

Consider these questions before the assessment:

1. Is the PIMS scope documented and understood?
2. Have relevant processing activities been identified?
3. Are responsibilities assigned for the activities within scope?
4. Have privacy risks been assessed and treated?
5. Are applicable legal and contractual obligations identified?
6. Do policies and procedures reflect actual operations?
7. Are employees aware of their responsibilities?
8. Are relevant suppliers and processors evaluated?
9. Are incidents and relevant complaints handled through defined processes?
10. Are internal audits and management reviews conducted as planned?
11. Are findings and corrective actions tracked to completion?
12. Can the organisation show evidence that controls operate as intended?

Not every question will apply in exactly the same way to every organisation. Use this checklist as a starting point, then map the assessment to the actual standard requirements and PIMS scope.

What happens if an auditor identifies a gap?

A finding should be evaluated according to the applicable certification body's audit and certification procedures.

The organisation may need to analyse the cause, correct the immediate issue, determine whether similar issues exist elsewhere and implement corrective action. It should also retain evidence showing whether the action was effective.

A commitment to fix a finding is not necessarily the same as completed and verified corrective action. The applicable certification process determines what must be resolved before certification can be granted or maintained.

10. How Long Does ISO 27701 Implementation Take?

There is no universal implementation timeline. The schedule depends on the organisation's existing privacy practices, the complexity of its processing activities, the number of locations and systems involved, resource availability and the certification assessment arrangements.

A business with established governance and documented processes may have a different starting point from an organisation building its PIMS from the ground up.

The following phases are useful for project planning:

- **Initial assessment:** Define the scope, identify gaps and confirm project responsibilities.
- **System design:** Establish the necessary processes, documentation and risk treatment plan.
- **Implementation:** Put controls into practice, assign responsibilities and maintain operational evidence.
- **Evaluation:** Conduct internal audits, management review and corrective action.
- **Certification assessment:** Arrange the independent assessment and address any findings according to the applicable process.

These phases may overlap, and their duration should be estimated after the initial assessment. Do not treat a generic timeline as a guarantee of certification.

Factors that affect the schedule

- The number and complexity of processing activities.
- Whether the organisation already has ISO 27001 or another relevant management system.
- The condition of existing policies, procedures and records.
- The number of suppliers and external processing arrangements.
- The complexity of its technology environment.
- Availability of internal process owners and decision-makers.
- The time needed to implement controls and demonstrate their operation.
- Certification-body availability and assessment requirements.

A practical project plan should include milestones, owners, dependencies, evidence requirements and a realistic allowance for resolving findings.

11. What Determines the Cost of ISO 27701 Certification?

ISO 27701 implementation and certification costs vary by organisation. An accurate quotation should follow an understanding of the scope and the work required.

Cost components may include:

Consultancy and implementation support: Gap assessment, process design, documentation, workshops, implementation support and audit preparation.

Internal resource time: Staff participation, management decisions, training, evidence preparation and control implementation.

Technology and operational improvements: Any changes required to address identified risks or implement the chosen controls.

Certification-body fees: Independent assessment and certification services, including applicable ongoing surveillance arrangements.

Additional requirements: Multi-location operations, complex processing activities, integration with other management systems or customer-specific assurance needs may affect the effort involved.

Organisations should compare proposals on scope, deliverables, consultant responsibilities, exclusions, timelines and support arrangementsâ??not just the headline price.

A low-cost proposal may not include the implementation support the organisation actually needs. Similarly, a large proposal is not automatically better. The appropriate scope should be based on the organisationâ??s real requirements.

12. ISO 27701 for IT, SaaS and BPO Companies in Hyderabad

Hyderabad has a substantial technology and business services ecosystem. Organisations working with enterprise customers may handle personal information across software applications, customer support systems, HR platforms, cloud services and outsourced business processes.

For these organisations, privacy management can be an important part of customer assurance and operational governance.

For IT and software development companies

Review how personal information enters applications, moves between environments, is accessed by support teams and is retained after a customer engagement ends.

Development and testing arrangements should be examined where they involve real personal information. Access to production data, third-party integrations and support access should be governed by appropriate procedures and controls.

For SaaS businesses

Understand the companyâ??s role in each processing activity and the commitments made to customers.

Review onboarding, account management, support, data export, deletion, subcontractors and the handling of customer requests. Make sure contractual promises align with actual platform capabilities and operating procedures.

For BPO and managed service providers

Document customer instructions, processing responsibilities, staff access, relevant subcontractors, incident escalation and evidence retention.

The organisation should be able to demonstrate how its procedures support the processing activities it has agreed to perform for customers.

For growing businesses

A privacy management system can help establish consistent processes before customer numbers, employee headcount or processing complexity increase significantly.

The objective is to build practices that can scale without creating unnecessary bureaucracy.

Choosing an ISO 27701 consultant in Hyderabad

When evaluating an ISO 27701 consultant in Hyderabad, consider whether the proposed support includes:

- A scope-specific gap assessment against ISO/IEC 27701:2025.
- Understanding of privacy management and related information security controls.
- Practical assistance with process design and implementation.
- Support for identifying evidence requirements and responsible process owners.
- Internal audit and certification-readiness support.
- Clear deliverables, exclusions, milestones and communication arrangements.
- A transparent distinction between consultancy support and independent certification.

Ask how the consultant will tailor the project to your processing activities. Avoid accepting claims that a fixed set of templates will automatically make every organisation compliant or guarantee certification.

13. Common ISO 27701 Implementation Mistakes

Mistake 1: Using outdated guidance without checking the edition

The 2025 edition differs in status and structure from the 2019 edition. Organisations should work from the current standard and verify certification arrangements before committing to a project.

Mistake 2: Treating privacy as an IT-only responsibility

IT may operate important safeguards, but privacy management also involves HR, legal, procurement, sales, customer support, operations and senior management.

Assign responsibilities across the organisation according to the processing activities and risks.

Mistake 3: Copying policies from another company

A policy written for a SaaS provider may not fit a manufacturer, healthcare organisation or outsourced service provider.

Documentation should reflect the organisation's real activities, contractual arrangements and applicable requirements.

Mistake 4: Ignoring suppliers and subcontractors

External providers may have access to personal information or perform important processing functions. Supplier oversight should be proportionate to the risks and responsibilities involved.

Mistake 5: Confusing certification with legal compliance

A management system certificate is not a substitute for identifying and meeting all applicable legal requirements. Maintain a separate legal obligations assessment and review it when laws or processing activities change.

Mistake 6: Preparing evidence only before the audit

Policies alone do not show that a process operates consistently. Maintain relevant records during normal operations and ensure that they accurately represent what the organisation does.

Mistake 7: Treating certification as the end of the project

A management system requires ongoing monitoring, internal audits, management review and improvement. Plan for continuing ownership and resources after certification.

14. Frequently Asked Questions About ISO 27701 Certification

What is ISO 27701 certification?

ISO 27701 certification is an independent assessment outcome demonstrating that an organisation's defined Privacy Information Management System has been assessed against the applicable requirements of ISO/IEC 27701. It helps provide structured evidence of privacy governance and management.

What is the latest version of ISO 27701?

As of October 2026, the current published edition is ISO/IEC 27701:2025, Edition 2, published on 14 October 2025. ISO lists the 2019 edition as withdrawn. Organisations should confirm the current requirements and certification arrangements before starting a project.

Is ISO 27701 a standalone standard?

Yes. ISO/IEC 27701:2025 is published as a standalone management system standard. This is an important distinction from older material describing the 2019 edition only as an extension to ISO 27001.

What is the difference between ISO 27701 and ISO 27001?

ISO 27001 focuses on information security management, while ISO 27701 focuses on privacy information management. The systems can complement each other, but they have different objectives and certification scopes.

Can a company get ISO 27701 certification without ISO 27001?

ISO/IEC 27701:2025 is a standalone management system standard. An organisation should assess the current edition's requirements and implement the security and privacy measures relevant to its scope. It should not assume that a separate ISO 27001 certificate is automatically required or that information security can be ignored.

Is ISO 27701 certification mandatory in India?

Whether certification is required depends on applicable laws, contracts, customer requirements and the organisation's business circumstances. Do not assume that every organisation handling personal information is legally required to obtain ISO 27701 certification. Legal obligations should be assessed separately.

Does ISO 27701 guarantee DPDP Act compliance?

No. ISO 27701 can support structured privacy governance, but certification does not automatically establish compliance with the Digital Personal Data Protection Act, 2023, the DPDP Rules, 2025, or every other applicable law. Organisations need a separate assessment of their legal obligations.

Who should consider ISO 27701 certification?

IT companies, SaaS providers, BPOs, data-processing service providers and other organisations handling personal information may consider the standard. Suitability depends on the scope of processing, business objectives, customer expectations and applicable obligations.

What documents are needed for ISO 27701?

Documentation depends on the organisation's scope and the standard's applicable requirements. Examples include a PIMS scope, privacy policies, processing inventories, risk assessments, control procedures, supplier records, training evidence, audit reports and management review records.

How long does ISO 27701 implementation take?

The timeline varies according to organisational complexity, existing controls, available resources and the certification process. A realistic schedule should be developed after a gap assessment rather than relying on a universal deadline.

How much does ISO 27701 certification cost in India?

The cost depends on implementation effort, organisation size, processing complexity, consultancy scope and certification-body fees. An accurate estimate requires a review of the organisation's requirements and existing practices.

How do I choose an ISO 27701 consultant in Hyderabad?

Look for a consultant who understands the current edition, can assess your actual processing activities, defines clear deliverables, supports implementation and audit readiness, and distinguishes consultancy from independent certification. Request a scope-specific proposal before deciding.

Conclusion: Build Privacy Management Into Everyday Operations

Personal information is an important business responsibility. As organisations expand their digital services, work with enterprise customers and rely on external platforms, privacy management becomes more complex.

ISO/IEC 27701:2025 provides a framework for establishing and improving a Privacy Information Management System. It can help organisations define responsibilities, assess risks, improve processing practices, maintain evidence and demonstrate a structured approach to privacy governance.

The best starting point is not to purchase templates or promise a certification date. It is to understand the organisation's processing activities, confirm the applicable requirements, identify gaps and build a practical implementation plan.

For organisations in Hyderabad, Telangana and across India, CK Associates can discuss the scope of a PIMS project, review existing management practices and help identify the implementation work required.

Planning ISO 27701 certification?

Discuss your privacy management requirements with CK Associates and request a scope-specific gap assessment.

Website: <https://ckassociates.biz>

Certification decisions are made by the relevant independent certification body. Implementation timelines, costs and outcomes depend on the organisation's scope, readiness and assessment arrangements.

About the Author

Sirish K Founder & Lead ISO Consultant, CK Associates

Sirish K leads ISO management system consulting and implementation support at CK Associates. With more than 20 years of experience and over 450 certification projects, his work focuses on helping organisations understand applicable standard requirements, establish practical management systems and prepare for independent certification assessments.

CK Associates supports organisations with management system gap assessments, documentation, implementation guidance, training, internal audit support and certification-readiness activities.

Website: <https://ckassociates.biz>

Summary

ISO/IEC 27701:2025 is a standalone international management system standard for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS). It is relevant to organisations responsible for processing personally identifiable information, including controllers and processors. Implementation generally involves defining scope, identifying processing activities, assessing privacy risks, establishing controls, training employees, maintaining evidence, conducting internal audits and reviewing performance. ISO 27701 can support privacy governance in India, but it does not automatically guarantee compliance with the Digital Personal Data Protection Act or other applicable laws. Organisations should assess their requirements against the current standard and their actual legal, contractual and operational obligations.

[Enquire](#)

Category

1. ISO Certification Consultants
2. Blog

Tags

1. ISO 27701 and ISO 27001
2. ISO 27701 Certification

3. ISO 27701 certification in India
4. ISO 27701 consultant Hyderabad
5. ISO 27701 Implementation
6. ISO/IEC 27701:2025
7. Personal data protection management
8. PII controller and processor
9. Privacy audit readiness
10. Privacy Information Management System (PIMS)
11. Privacy management for SaaS companies

Date Created

25/10/2026

Author

ckassociates-biz

default watermark