IMPLEMENTATION GUIDE

ISO/IEC 27701:2025

Privacy Information Management System

Requirements and Guidance for PIMS Implementation

Prepared by Pacific Certifications

For organizations establishing privacy governance, PII processing controls, and certification-ready documented information.

Standard	ISO/IEC 27701:2025
System	Privacy Information Management System (PIMS)
Use	Implementation planning, internal readiness and certification preparation
Prepared for	Organizations preparing privacy governance and certification readiness

Important note: This guide is an educational implementation aid. It does not reproduce ISO/IEC 27701:2025 and should be used with the official standard and applicable privacy laws.

Contents

A practical implementation guide for building a privacy information management system.

Use this guide as a design and readiness document. The organization should still purchase the official standard, perform legal mapping to applicable privacy laws, and keep evidence of implementation before external assessment.

01. What ISO/IEC 27701:2025 Covers

Privacy Information Management System requirements and guidance for PII controllers and PII processors.

ISO/IEC 27701:2025 provides a structured framework for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS). The system is intended for organizations that determine the purposes and means of PII processing, process PII on behalf of another party, or perform both roles across different services.

Unlike the earlier edition, the 2025 edition can be used as an independent management system standard while still allowing integration with ISO/IEC 27001, ISO/IEC 27002 and other governance frameworks. This makes it useful for organizations that need privacy governance without necessarily building a full ISMS first.

Core concept	Implementation meaning
PIMS	A structured system to manage privacy governance, privacy risks, processing controls, accountability and continual improvement.
PII	Information that identifies or can reasonably identify a natural person.
PII controller	The organization or party that determines the purpose and means of PII processing.
PII processor	The organization or party that processes PII on behalf of a controller.
Privacy risk	The effect of uncertainty on individuals and the organization arising from PII processing activities.

Implementation principle: A PIMS should be built around actual processing activities, not just policy documents. Start with a PII inventory, legal basis mapping, data-flow diagrams and responsibility assignment.

02. PIMS Benefits and Business Outcomes

A well-designed PIMS creates accountability, transparency and controlled handling of personal data.

- Clarifies responsibilities for privacy governance, privacy risk management and privacy decision-making.
- Supports compliance with applicable privacy and data-protection laws, regulations and contractual obligations.
- Improves trust with clients, regulators, employees, suppliers and individuals whose PII is processed.
- Builds evidence-based privacy management through policies, records, approvals, logs and reviews.
- Improves incident preparedness by defining escalation routes, breach evaluation and notification controls.
- Creates a common privacy framework for teams handling HR data, client data, marketing data, vendor data, online identifiers and sensitive categories of data.
- Supports integration with ISO/IEC 27001, ISO/IEC 27002, cloud controls, AI governance and internal compliance programs.

Business driver	PIMS response
Regulatory expectations	Legal mapping, privacy notices, rights handling, retention rules and breach response evidence.
Customer due diligence	Documented controls, supplier assurance, processing records and privacy performance indicators.
Security and privacy overlap	Aligned access control, logging, incident handling, encryption and secure deletion.
Data growth	PII classification, inventory, minimization, retention and disposal rules.
Third-party processing	Processor agreements, transfer checks, sub-processor controls and monitoring.

03. PDCA Model for Privacy Management

Plan, Do, Check and Act provide the operating rhythm for PIMS implementation.

PDCA stage	Privacy management activities
Plan	Define context, interested parties, PIMS scope, legal obligations, privacy risks, objectives, resources and responsibilities.
Do	Implement policies, PII processing controls, notices, consent controls, supplier controls, security controls, incident response and rights-handling processes.
Check	Monitor KPIs, audit PIMS processes, review legal compliance, evaluate incidents, test rights handling and report management information.
Act	Take corrective actions, improve controls, update registers, enhance training and review the PIMS when services, laws or processing purposes change.

The PDCA model should operate at two levels: at the PIMS level through management review, objectives and audits; and at the process level through daily control of PII collection, storage, transfer, use, retention and deletion.

Design tip: Use one privacy risk register and link it to the PII inventory, legal basis records, supplier register, security controls, incident records and corrective actions. This avoids disconnected compliance files.

04. Implementation Roadmap

A practical path from privacy baseline to certification readiness.

Step	Main activities	Key outputs
1. Initiate	Confirm leadership sponsor, PIMS owner, implementation team and project schedule.	Project plan; responsibility matrix.
2. Understand data	Identify PII categories, processing purposes, systems, locations, third parties and retention periods.	PII inventory; data-flow map.
3. Define scope	Set organizational boundaries, services, systems, locations, controller/processor roles and interfaces.	PIMS scope statement.
4. Map obligations	Identify laws, contracts, privacy notices, client requirements and regulator expectations.	Compliance obligations register.
5. Assess risks	Evaluate privacy risks to individuals and the organization; identify controls and treatment actions.	Privacy risk register; treatment plan.
6. Implement controls	Deploy operational privacy, security, supplier, incident and rights-handling controls.	Procedures, logs, approvals and evidence.
7. Evaluate	Conduct internal audit, compliance review, KPI review and management review.	Audit report; management review minutes.
8. Improve	Close gaps and verify effectiveness before external assessment.	CAPA log; updated documents.

05. Clause 4 - Context and Scope

Define what privacy management covers and which interested-party requirements apply.

The organization should determine external and internal issues relevant to privacy management. External issues may include privacy laws, sector regulations, customer requirements, technology changes, cross-border processing expectations and regulator guidance. Internal issues may include systems, data volumes, outsourcing, workforce capability, legacy applications and current security controls.

- Identify interested parties such as individuals/data subjects, customers, employees, regulators, suppliers, cloud providers, business partners and internal process owners.
- Determine requirements relevant to the PIMS, including legal basis, transparency, rights handling, security, retention, breach notification and processor obligations.
- Define the PIMS scope by services, locations, systems, legal entities, processes, products, roles and interfaces with other management systems.

Scope element	Question to answer
Organizational boundary	Which legal entity, departments and locations are included?
Processing role	Are you a controller, processor, joint controller or different roles for different services?
PII categories	Which personal data categories and special/sensitive categories are in scope?
Technology boundary	Which applications, databases, cloud services and integrations are included?
Exclusions	Are exclusions justified and do they avoid removing required privacy responsibilities?

06. Clause 5 - Leadership and Privacy Policy

Top management should make privacy governance operational and accountable.

Leadership should ensure that privacy objectives are aligned with organizational strategy, legal requirements and risk appetite. The PIMS cannot be owned only by IT or compliance; it requires coordinated involvement from management, HR, legal, procurement, operations, product, security, sales and service teams.

Leadership area	Expected implementation evidence
Privacy policy	Approved policy that states privacy commitments, responsibilities, legal compliance and continual improvement.
Roles and authorities	Named PIMS owner, privacy officer or equivalent, process owners, system owners and incident escalation contacts.
Management commitment	Budget, resources, training support, privacy-by-design decisions and regular review of PIMS performance.
Accountability	Records showing approvals, risk acceptance, supplier decisions, privacy impact decisions and corrective action closure.

- Communicate the privacy policy to employees and relevant third parties.
- Ensure privacy responsibilities are included in job descriptions, contracts, onboarding and training.
- Define escalation routes for privacy incidents, individual rights requests and high-risk processing activities.

07. Clause 6 - Planning, Privacy Risks and Objectives

Planning turns privacy obligations and processing risks into controlled actions.

The organization should determine privacy risks and opportunities related to PII processing and define actions to address them. Risks should consider both organizational exposure and potential impact on individuals. Privacy objectives should be measurable and should link to policy commitments, legal obligations, client expectations and risk treatment actions.

Planning output	Minimum content
Privacy risk register	Risk description, impacted PII, cause, consequences, existing controls, rating, owner, action and residual risk.
Risk treatment plan	Selected control actions, timeline, resources, responsible person, acceptance and effectiveness criteria.
Privacy objectives	Specific targets for awareness, rights response, retention cleanup, supplier reviews, incidents, audits and control maturity.
Change planning	Privacy review for new systems, new vendors, new processing purposes, AI tools, data transfers and acquisitions.

Risk focus: Privacy risks should include unlawful processing, excessive data collection, unclear consent, inadequate notices, unauthorized access, inaccurate records, excessive retention, uncontrolled transfers, supplier failure and delayed breach response.

08. PII Inventory and Processing Map

The PII inventory is the backbone of the PIMS.

A PIMS should not begin with generic policy language. It should begin with an accurate record of how PII enters, moves through and leaves the organization. The inventory should be maintained whenever products, services, suppliers, systems, laws or processing purposes change.

Inventory field	Purpose
Process or activity	Names the business activity, such as recruitment, payroll, client onboarding, marketing, support or service delivery.
PII category	Identifies personal, contact, identity, financial, technical, HR, health, biometric, children, location or sensitive data.
Purpose and legal basis	Explains why data is processed and the lawful basis or contractual basis relied upon.
Source and recipients	Identifies where data comes from and who receives it internally or externally.
Systems and storage	Maps databases, applications, shared drives, cloud systems, archives and backups.
Retention and disposal	Defines retention period, trigger for disposal and deletion method.
Transfers	Identifies countries, safeguards, processors and sub-processors.
Controls	Links to access control, encryption, logging, review, masking, backup and deletion controls.

09. Privacy Risk Assessment Methodology

A consistent method helps management make defensible privacy decisions.

The organization should define how privacy risks are identified, analyzed, evaluated, treated and reviewed. The method should be understandable to business teams, not only information security specialists. It should include triggers for privacy impact assessment where processing is high risk or materially changed.

Assessment stage	Recommended approach
Identify	Use PII inventory, data flows, legal obligations, incidents, supplier reviews and system changes.
Analyze	Assess likelihood, impact to individuals, regulatory exposure, reputational exposure and control effectiveness.
Evaluate	Compare risk rating with privacy risk criteria and define whether treatment is required.
Treat	Avoid, reduce, transfer or accept the risk with documented approval.
Review	Update after incidents, new laws, system changes, audits, complaints or management review.

- High-risk examples: large-scale profiling, sensitive data processing, biometrics, children’s data, AI-supported decisions, cross-border transfers, or systematic monitoring.
- Treatment examples: data minimization, pseudonymization, encryption, consent redesign, contract clauses, retention cleanup, access review, supplier audit or improved transparency notices.

10. Clause 7 - Support, Competence and Documented Information

Support processes make privacy controls repeatable.

Support requirements cover resources, competence, awareness, communications and documented information. Privacy controls often fail because employees do not understand when to escalate, where to record decisions or how to handle individual rights requests. Training and documented procedures should be role-specific.

Support area	Implementation evidence
Resources	PIMS owner, privacy budget, legal support, security tooling, audit resources and management time.
Competence	Training records for HR, IT, support, sales, marketing, developers, procurement and privacy team.
Awareness	Privacy policy communication, acceptable use, phishing/privacy training, breach escalation and rights-handling awareness.
Communication	Who communicates with individuals, regulators, clients, processors, suppliers and internal management.
Documented information	Approved procedures, registers, templates, logs, evidence and version-controlled records.

Training tip: Separate general privacy awareness from role-based training. HR, marketing, developers, customer support, procurement and IT administrators need different practical examples.

11. Clause 8 - Operational Privacy Controls

Operational controls should cover the full PII lifecycle.

Operational planning and control require the organization to define how PII is collected, used, disclosed, stored, transferred, retained and disposed of. Controls should be applied consistently across manual records, digital systems, cloud platforms and outsourced processes.

PII lifecycle stage	Typical control
Collection	Privacy notice, legal basis check, data minimization, consent where required and source validation.
Use	Purpose limitation, access control, role-based permissions, confidentiality and acceptable-use rules.
Storage	Classification, encryption, backup, logging, physical security and retention tagging.
Sharing	Recipient review, data processing agreement, transfer assessment and secure transmission.
Change	Privacy impact assessment for new systems, new purposes, AI tools and significant supplier changes.
Retention	Retention schedule, deletion trigger, litigation hold process and backup retention rules.
Disposal	Secure deletion, destruction certificates, evidence of erasure and decommissioning review.

12. PII Controller and PII Processor Controls

The organization must know which privacy role it performs for each processing activity.

An organization may be a PII controller for employee and marketing data, a PII processor for client service delivery, and a joint controller for specific business arrangements. The PIMS should map responsibilities and controls by role rather than assuming one role across the whole business.

Area	Controller emphasis	Processor emphasis
Purpose and legal basis	Determine and document purpose, legal basis and transparency approach.	Process only on documented instructions unless law requires otherwise.
Rights requests	Receive, verify, respond and record decisions.	Support the controller and route requests promptly.
Retention	Define retention periods and deletion rules.	Follow controller retention/deletion instructions and prove completion.
Sub-processing	Approve processors and transfer safeguards.	Obtain authorization for sub-processors and flow down obligations.
Incident handling	Assess impact and notification obligations.	Notify the controller without undue delay and support investigation.

13. Data Subject Rights, Consent and Transparency

Individuals should understand and be able to exercise privacy rights in a controlled way.

The PIMS should define how privacy notices are issued, how consent is obtained or withdrawn where relevant, and how rights requests are handled. Rights processes should have intake channels, verification criteria, response timelines, escalation rules and decision records.

Control area	Implementation guidance
Privacy notices	Keep notices clear, current and aligned with actual processing activities, recipients, retention and rights.
Consent	Record consent source, purpose, date, wording and withdrawal status where consent is relied upon.
Access requests	Verify identity, locate records, assess exemptions, respond within applicable timelines and retain evidence.
Correction and deletion	Define review steps, system update rules, backup limitations and deletion evidence.
Objection and restriction	Define when processing may be limited, stopped or continued with documented justification.
Automated decision-making	Identify automated decisions, profiling logic, meaningful information and review options where applicable.

14. Supplier, Cloud and Cross-border Privacy Controls

Third parties are a major source of privacy exposure.

Privacy obligations should be built into supplier selection, contracting, onboarding, monitoring and termination. Where cloud providers, payroll processors, CRM platforms, analytics tools, call centers or outsourced developers handle PII, the organization should verify privacy and security controls before approving processing.

Supplier control	Evidence to maintain
Due diligence	Questionnaires, certifications, privacy/security evidence, breach history and risk assessment.
Contracting	Data processing terms, confidentiality, sub-processor rules, audit rights, breach notification and return/deletion terms.
Transfer control	Country transfer assessment, approved safeguards, contractual clauses and record of transfer decisions.
Monitoring	Periodic review, service reporting, audit outputs, incident reports and corrective action follow-up.
Exit	Return/deletion certificate, access removal, archive decision and data migration evidence.

Supplier register: Include supplier role, PII categories, countries, systems, contract owner, risk rating, review date, sub-processors and termination requirements.

15. Privacy Incident and Breach Management

Privacy incidents need rapid triage, evidence and escalation.

A privacy incident is not limited to cyber compromise. It can include misdirected emails, lost devices, unauthorized disclosure, incorrect access permissions, unapproved sharing, missing paper records, retention failures or supplier incidents. The PIMS should define how incidents are reported, investigated, classified and closed.

Incident step	Required control
Report	Simple reporting channels, employee awareness and immediate containment instructions.
Triage	Determine PII involved, affected individuals, cause, systems, supplier involvement and current containment.
Assess	Evaluate harm, legal notification duties, contractual reporting, regulator/client reporting and public communication needs.
Notify	Follow applicable law and contract requirements for regulator, controller, client or individual notification.
Correct	Root cause analysis, corrective action, evidence collection and effectiveness review.
Learn	Management reporting, trend analysis, training updates and control improvement.

16. Clause 9 - Performance Evaluation

Monitoring, internal audit and management review prove the PIMS is working.

Performance evaluation should be planned and evidence-based. Privacy KPIs should give management useful information about privacy control performance, legal compliance and risk treatment progress.

Evaluation area	Examples
KPIs	Rights request closure time, training completion, supplier review completion, incidents, retention cleanup, access review closure and audit findings.
Compliance evaluation	Review applicable laws, client contracts, privacy notices, transfer obligations and regulatory changes.
Internal audit	Audit PIMS scope, controls, risk treatment, processing records, supplier controls, incidents and management review inputs.
Management review	Review risks, objectives, incidents, complaints, audits, resources, legal changes and improvement opportunities.

- Internal audits should include sampling of real processing activities, not only document checks.
- Management review should result in decisions, assigned actions and follow-up evidence.

17. Clause 10 - Improvement

Corrective action and continual improvement keep privacy controls current.

The PIMS should define how nonconformities, complaints, privacy incidents, audit findings and monitoring results are investigated and corrected. Corrective actions should address root cause and verify effectiveness.

Improvement input	Possible corrective action
Delayed rights request	Improve intake workflow, assign backup owners and automate reminders.
Retention failure	Update retention schedule, tag records and implement periodic deletion review.
Supplier non-compliance	Update contract controls, require remediation or replace supplier.
Unclear privacy notice	Revise notices and align them with PII inventory and data flows.
Access review gap	Implement recurring access review and privileged-access approval workflow.
Incident recurrence	Change process, training, technical controls and monitoring.

18. Documented Information Toolkit

Recommended documents and records for implementation and certification readiness.

Document / record	Purpose
PIMS scope statement	Defines organizational, technical and processing boundaries.
Privacy policy	States commitments, responsibilities and improvement approach.
PII inventory / record of processing	Maps PII, purposes, systems, recipients, transfers, retention and controls.
Privacy risk methodology	Defines risk criteria, scoring, acceptance and review method.
Privacy risk register	Records risks, controls, treatment actions and residual risk decisions.
Compliance obligations register	Maps applicable laws, contracts and regulatory requirements.
Privacy impact assessment template	Assesses high-risk or changed processing activities.
Consent records	Tracks consent, withdrawal and consent wording where applicable.
Rights request log	Records intake, verification, decision, response and closure evidence.
Supplier privacy register	Tracks processors, sub-processors, transfer countries, contracts and reviews.
Incident / breach log	Records privacy events, classification, notification and corrective action.
Retention schedule	Defines retention periods, disposal method and legal holds.
Internal audit programme	Plans process and clause-based privacy audits.
Management review minutes	Records leadership review and decisions.
Corrective action log	Tracks root cause, action, owner, target date and effectiveness verification.

19. Certification Readiness Checklist

Use this before external assessment.

Area	Readiness evidence
PIMS scope	Scope is approved, accurate and aligned with actual PII processing.
PII inventory	All in-scope processes, systems, suppliers, transfers and retention periods are mapped.
Legal mapping	Applicable privacy laws, contracts and regulatory requirements are identified and reviewed.
Privacy policy	Policy is approved, communicated and supported by role-specific responsibilities.
Risk assessment	Privacy risks are assessed and linked to treatment plans and controls.
Operational controls	Collection, use, sharing, retention, transfer and disposal controls are implemented.
Rights process	Rights request workflow is defined, tested and evidenced.
Supplier controls	Processor and sub-processor contracts, due diligence and monitoring are complete.
Incident process	Privacy incident procedure, log, escalation and notification criteria are implemented.
Training	General and role-based privacy training records are available.
Internal audit	A PIMS internal audit has been completed and findings are tracked.
Management review	Management review minutes include PIMS performance, risks, changes and decisions.
Corrective action	Corrective actions are closed or controlled with effectiveness evidence.

20. 90-Day Implementation Plan

A practical schedule for organizations starting from a basic privacy baseline.

Period	Focus	Key deliverables
Days 1-15	Launch and discovery	Project plan, PIMS owner, scope draft, interested parties and PII inventory template.
Days 16-30	PII mapping	Completed process inventory, data-flow maps, supplier list, systems list and retention baseline.
Days 31-45	Legal and risk planning	Compliance register, privacy risk methodology, initial risk assessment and treatment plan.
Days 46-60	Policy and controls	Privacy policy, rights procedure, incident procedure, supplier controls, retention schedule and privacy notices.
Days 61-75	Implementation evidence	Training, access review, supplier due diligence, incident test, rights request test and retention review.
Days 76-90	Assurance and improvement	Internal audit, management review, CAPA closure and certification-readiness package.

Timeline note: The actual timeline can vary depending on PII complexity, number of systems, legal jurisdictions, supplier dependency, available resources and maturity of existing information security controls.

21. Frequently Asked Questions

Common implementation questions for ISO/IEC 27701:2025.

Can ISO/IEC 27701:2025 be implemented without ISO/IEC 27001?

Yes. The 2025 edition can be implemented as an independent privacy information management system. It can also be integrated with ISO/IEC 27001 where the organization already has an ISMS.

Is ISO/IEC 27701 a legal compliance certificate?

No. Certification supports structured privacy management and evidence-based controls, but the organization must still identify and comply with applicable privacy laws.

Who should own the PIMS?

Ownership may sit with a privacy officer, compliance head, security head, legal team or senior manager, but responsibilities must be clearly assigned across business functions.

What is the most important implementation document?

The PII inventory is usually the most important operational document because it connects processing purposes, legal basis, systems, suppliers, retention, rights and risks.

What evidence is needed before assessment?

A defined scope, policy, PII inventory, risk records, legal obligations, procedures, training records, supplier records, incident records, internal audit, management review and corrective actions.

Can one organization be both controller and processor?

Yes. Many organizations act as a controller for internal data and as a processor for client data. Roles should be mapped activity by activity.

22. Certification Preparation Notes

Preparing for Stage 1 and Stage 2 assessment.

Stage 1 normally focuses on readiness of documented information, scope, process understanding, legal and contractual obligations, risk assessment, internal audit planning, management review readiness and implementation status. Stage 2 verifies implementation evidence, process control, interview evidence and operational consistency.

Assessment area	Prepare before external assessment
Documentation	Approved policies, procedures, registers, templates and controlled records.
Implementation evidence	Completed logs, approvals, tests, reviews, training and supplier records.
Process owners	Employees can explain privacy responsibilities, escalation routes and documented controls.
Operational sampling	Evidence is available from HR, IT, marketing, service delivery, procurement and support processes.
Corrective actions	Open findings are controlled and closed findings have effectiveness evidence.

Reference standards and related guidance to consider: ISO/IEC 27701:2025, ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 29100, ISO/IEC 27018 where cloud PII processing is relevant, and applicable privacy laws in each jurisdiction.

Prepared by Pacific Certifications. This document is intended as a practical guide and template for implementation planning. It is not a substitute for the official ISO/IEC 27701:2025 standard, legal advice, or organization-specific privacy risk assessment.