**PACIFIC CERTIFICATIONS**

Trusted Global ISO Certification Body

# ISO/IEC 27701:2025 Gap Analysis Template

## Privacy Information Management Systems

Downloadable Website Resource for PIMS Readiness and Certification Planning

| Standard | Purpose | Prepared by |
|---|---|---|
| ISO/IEC 27701:2025 | Gap analysis and action planning | Pacific Certifications |

This gap analysis template helps organizations compare their current privacy governance, PII processing controls and privacy management arrangements with ISO/IEC 27701:2025 requirements. It is suitable for organizations acting as PII controllers, PII processors or both.

Pacific Certifications provides independent third-party certification assessment and certificate issuance services. This template is a general readiness resource and does not replace the official ISO/IEC 27701:2025 standard, applicable privacy laws, customer contracts, regulatory obligations or organization-specific legal review.

# How to Use This Gap Analysis Template

Review each requirement area and compare it with the organization's current privacy information management system. Mark the implementation status, identify available evidence, describe gaps, define actions, assign ownership and set target dates for closure.

- Use Implemented where the privacy requirement is fully established, maintained and supported by objective evidence.
- Use Partially Implemented where the privacy process exists but is incomplete, inconsistent, not fully documented or not supported by adequate records.
- Use Not Implemented where the requirement has not been addressed or evidence is not available.
- Use Not Applicable only when a documented justification is available and the decision does not affect PIMS scope, accountability or intended outcomes.
- Use the final action plan to prioritize privacy governance, PII inventory, lawful basis or processing purposes, controller/processor obligations, data subject rights, breach handling, supplier privacy controls and continual improvement.

## Organization Details

| | | | |
|---|---|---|---|
| **Organization Name** | | **Prepared By** | |
| **Location / Site** | | **Date** | |
| **PIMS Scope** | | **Review Type** | Gap Analysis |
| **Role in PII Processing** | | **Controller / Processor / Both** | |

## Suggested Gap Rating

| Rating | Meaning | Typical Evidence Condition | Priority |
|---|---|---|---|
| **Implemented** | Requirement is addressed and maintained. | Evidence is current, controlled and consistently applied. | Monitor |
| **Partially Implemented** | Requirement is addressed in part. | Evidence is incomplete, inconsistent or not fully communicated. | Medium |
| **Not Implemented** | Requirement is missing. | No adequate process, record or accountable owner is available. | High |
| **Not Applicable** | Requirement is not applicable. | Justification is documented and approved. | Review |

## Clause 4 - Context of the Organization and PIMS Scope

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| 4.1 | Determine internal and external issues relevant to privacy management, PII processing, regulatory exposure and stakeholder expectations. | | | | | |
| 4.2 | Identify interested parties including data subjects, customers, regulators, processors, controllers, staff and service providers. | | | | | |
| 4.3 | Define the PIMS scope including business functions, processing activities, locations, systems, products, services and controller/processor roles. | | | | | |
| 4.4 | Establish, implement, maintain and continually improve the PIMS and related privacy processes. | | | | | |

## Clause 5 - Leadership and Privacy Accountability

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| 5.1 | Demonstrate leadership commitment, accountability and integration of privacy requirements into business processes. | | | | | |
| 5.2 | Establish and communicate a privacy policy aligned with organizational purpose, processing context and compliance obligations. | | | | | |

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **5.3** | Assign and communicate privacy roles, responsibilities and authorities, including responsibility for PIMS performance and privacy escalation. | | | | | |

## Clause 6 - Planning for Privacy Risks and Objectives

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **6.1** | Identify privacy risks and opportunities associated with PII processing, data subject rights, legal obligations and third-party arrangements. | | | | | |
| **6.2** | Define measurable privacy objectives and plans to achieve them, including owners, timelines, resources and evaluation methods. | | | | | |
| **6.3** | Plan changes to the PIMS in a controlled manner considering privacy risk, processing changes, suppliers, technologies and affected parties. | | | | | |

## Clause 7 - Support and Documented Information

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **7.1** | Determine and provide resources needed to operate and improve the PIMS. | | | | | |
| **7.2** | Define competence requirements and retain evidence of competence for personnel with privacy responsibilities. | | | | | |

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **7.3** | Ensure awareness of privacy policy, privacy objectives, PII handling responsibilities and consequences of nonconformity. | | | | | |
| **7.4** | Establish internal and external communication processes for privacy matters, data subject requests, incidents and regulatory communication. | | | | | |
| **7.5** | Control documented information required for the PIMS, including policies, records, procedures and evidence of privacy control operation. | | | | | |

# Clause 8 - Operation and PII Processing Controls

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **8.1** | Plan, implement and control privacy operations, including outsourced processes and changes affecting PII processing. | | | | | |
| **PII Inventory** | Maintain records of PII processing activities, categories of PII, processing purposes, systems, locations and recipients. | | | | | |
| **Privacy Notices** | Define and maintain privacy notices or communication methods explaining purposes, rights, retention and sharing practices. | | | | | |
| **Lawful Basis / Purpose** | Document processing purposes, legal or contractual basis where applicable and controls against incompatible processing. | | | | | |
| **Data Minimization** | Limit PII collection, use, disclosure and retention to what is necessary for defined purposes. | | | | | |
| **Data Subject Rights** | Establish processes for access, correction, deletion, restriction, objection, portability and similar requests where applicable. | | | | | |
| **Consent Management** | Control consent collection, withdrawal, evidence retention and related processing rules where consent is used. | | | | | |
| **PII Disclosure** | Control disclosure, transfer, sharing and publication of PII, including approvals and records. | | | | | |
| **Retention and Disposal** | Define retention periods, disposal methods and evidence of secure deletion or anonymization where required. | | | | | |

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **Privacy Incidents** | Identify, report, assess, escalate and record privacy incidents and PII breaches, including notification decision records. | | | | | |

# Controller and Processor Readiness Areas

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **Controller Role** | Define controller responsibilities for processing purposes, notices, rights handling, lawful processing and processor oversight. | | | | | |
| **Processor Role** | Define processor responsibilities for acting on documented instructions, confidentiality, sub-processing and assistance to controllers. | | | | | |
| **Joint / Shared Processing** | Define accountability and responsibility allocation where multiple parties determine or support PII processing. | | | | | |
| **Supplier Privacy Controls** | Assess and control suppliers, processors, sub-processors and outsourced services that handle PII. | | | | | |
| **Cross-border Transfer** | Identify international transfer scenarios and maintain controls, approvals or safeguards required by applicable obligations. | | | | | |
| **Privacy by Design** | Integrate privacy requirements into projects, new services, system changes, product design and procurement. | | | | | |
| **DPIA / Privacy Risk Assessment** | Perform privacy impact or risk assessments for high-risk processing, new technologies or significant processing changes. | | | | | |
| **Security of PII** | Coordinate privacy requirements with information security controls to protect confidentiality, integrity and availability of PII. | | | | | |
| **Training and Awareness** | Provide role-based privacy awareness for personnel handling PII or managing privacy | | | | | |

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| | obligations. | | | | | |
| **Regulatory Interface** | Maintain processes for regulator communication, complaints, investigations and compliance evidence where applicable. | | | | | |

## Clause 9 - Performance Evaluation

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **9.1** | Monitor, measure, analyze and evaluate PIMS performance, privacy objectives, control effectiveness and compliance indicators. | | | | | |
| **9.2** | Conduct internal assessments at planned intervals to determine PIMS conformity and effective implementation. | | | | | |
| **9.3** | Conduct management review covering PIMS suitability, adequacy, effectiveness, privacy risks and improvement needs. | | | | | |

## Clause 10 - Improvement

| ISO/IEC 27701 Area | Requirement Focus | Current Status | Evidence Available | Gap / Risk Identified | Action Required | Owner / Target Date |
|---|---|---|---|---|---|---|
| **10.1** | Identify nonconformities, take correction, manage consequences and evaluate need for corrective action. | | | | | |
| **10.2** | Continually improve the suitability, adequacy and effectiveness of the PIMS and privacy controls. | | | | | |

# Gap Analysis Summary and Action Plan

Use this section to summarize the major gaps identified during the review. Prioritize actions that affect privacy accountability, processing transparency, data subject rights, PII security, third-party processing, breach handling, regulatory obligations and continual improvement.

| No. | Major Gap / Issue | Risk or Impact | Corrective Action | Responsible Person | Target Date / Status |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |

## Certification Readiness Notes

- Confirm that the PIMS scope clearly identifies covered processes, systems, locations, PII categories and controller or processor roles.
- Confirm that privacy policy, privacy objectives, PII processing records, risk assessments and operational controls are approved and current.
- Confirm that evidence exists for data subject request handling, privacy notices, consent records where applicable, breach handling, supplier controls and retention or disposal controls.
- Confirm that internal assessment, management review, nonconformity handling and continual improvement records are available before certification assessment.

## Contact Pacific Certifications

For ISO/IEC 27701:2025 certification assessment and certificate issuance, contact Pacific Certifications at support@pacificcert.com or visit www.pacificcert.com.