PACIFIC CERTIFICATIONS

Trusted Global ISO Certification Body

ISO/IEC 27701:2025 Audit Checklist

Privacy Information Management Systems

Downloadable Website Resource for PIMS Assessment Readiness

Standard	Purpose	Prepared by
ISO/IEC 27701:2025	Clause-wise audit checklist	Pacific Certifications

This audit checklist helps organizations review their Privacy Information Management System against ISO/IEC 27701:2025. It may be used for internal assessment, certification readiness review, supplier privacy review, management system monitoring and improvement planning.

Pacific Certifications provides independent third-party certification assessment and certificate issuance services. This checklist is a general readiness resource and does not replace the official ISO/IEC 27701:2025 standard, applicable privacy laws, contractual requirements or professional legal review.

How to Use This Audit Checklist

Review each question against the organization's current PIMS scope, PII processing activities, controller or processor roles, regulatory obligations and documented information. Mark the result and record evidence, observations and required actions.

- Use C where the requirement is implemented and supported by adequate objective evidence.
- Use PC where the requirement is partly implemented or evidence is incomplete.
- Use NC where the requirement is not implemented, ineffective or unsupported by evidence.
- Use NA only where the organization has documented and approved a justified exclusion or non-applicability decision.
- Review both management system requirements and privacy operational controls, including controller and processor responsibilities where relevant.

Organization and Assessment Details

Organization Name		**Assessment Date**	
Location / Site		**Prepared By**	
PIMS Scope		**Assessment Type**	Internal / Readiness
PII Processing Role		**Controller / Processor / Both**	

Audit Result Key

Result	Meaning	Evidence Expectation	Action
C	Conforming	Current documented information and records support the answer.	Monitor and maintain.
PC	Partially conforming	Process exists but evidence, application or consistency is incomplete.	Define improvement action.
NC	Nonconforming	Requirement is missing, ineffective or unsupported by evidence.	Raise corrective action.
NA	Not applicable	A documented justification is available.	Review during scope changes.

Clause 4 - Context of the Organization and PIMS Scope

Area	Audit Question	Evidence to Review	Result C/PC/NC/NA	Observations / Findings	Action Required
4.1	Has the organization determined internal and external issues that affect privacy management and PII processing?	Context analysis, privacy risk register, regulatory register, business strategy, stakeholder analysis.			
4.2	Has the organization identified interested parties and relevant privacy requirements?	Interested-party register, data subject expectations, customer obligations, regulator requirements, contracts.			
4.3	Is the PIMS scope defined, documented and aligned with processing activities, locations, systems and roles?	PIMS scope statement, process map, PII inventory, site list, system list, controller/processor role analysis.			
4.4	Is the PIMS established, implemented, maintained and improved as a management system?	PIMS procedures, process interaction map, responsibilities, monitoring records, improvement records.			

Clause 5 - Leadership and Accountability

Area	Audit Question	Evidence to Review	Result C/PC/NC/NA	Observations / Findings	Action Required
5.1	Does top management demonstrate accountability and support for the PIMS?	Management review, privacy objectives, resource decisions, meeting minutes, leadership communications.			
5.2	Is a privacy policy established, communicated and maintained?	Approved privacy policy, communication records, intranet notice, employee acknowledgements.			
5.3	Are privacy roles, responsibilities and authorities defined and communicated?	Role descriptions, RACI matrix, appointment letters, escalation matrix, governance committee records.			

Clause 6 - Planning

Area	Audit Question	Evidence to Review	Result C/PC/NC/NA	Observations / Findings	Action Required
6.1	Has the organization assessed privacy risks and opportunities related to PII processing and PIMS outcomes?	Privacy risk assessment, DPIA/PIA records, risk treatment plans, risk acceptance approvals.			

Area	Audit Question	Evidence to Review	Result C/PC/NC/NA	Observations / Findings	Action Required
6.2	Are privacy objectives measurable, monitored and supported by action plans?	Privacy objectives, KPIs, action plans, owners, progress reports, performance dashboards.			
6.3	Are changes to the PIMS planned and controlled?	Change requests, project privacy reviews, change impact assessments, approvals, communication records.			

Clause 7 - Support

Area	Audit Question	Evidence to Review	Result C/PC/NC/NA	Observations / Findings	Action Required
7.1	Are sufficient resources provided for PIMS operation and improvement?	Resource plans, budget approvals, tools, staffing records, service contracts.			
7.2	Are competence requirements defined for privacy-related roles?	Competence matrix, training plans, qualification records, role-based assessment records.			
7.3	Are personnel aware of privacy policy, PII handling duties and consequences of nonconformity?	Awareness materials, attendance records, induction records, staff acknowledgements.			
7.4	Are internal and external privacy communication processes defined?	Communication procedure, breach notification workflow, data subject request workflow, regulator contact list.			
7.5	Is documented information controlled, current and protected from unauthorized change?	Document control procedure, record retention rules, version history, approval records, access permissions.			

Clause 8 - Operation and Privacy Controls

Area	Audit Question	Evidence to Review	Result C/PC/NC/NA	Observations / Findings	Action Required
8.1	Are privacy operations planned and controlled according to PIMS requirements?	Operational procedures, work instructions, process controls, outsourced process controls.			
PII Inventory	Does the organization maintain an accurate inventory of PII processing activities?	ROPA/PII inventory, data maps, system records, process owner validation.			
Purpose and Lawfulness	Are processing purposes, legal bases or applicable justification requirements documented?	Processing purpose register, lawful basis assessment, consent records, contract clauses.			
Privacy Notices	Are privacy notices clear, current and available to relevant data subjects?	Privacy notices, website notices, employee notices, customer notices, update records.			
Collection Limitation	Is PII collection limited to defined and necessary purposes?	Forms, field reviews, data minimization reviews, business justification records.			
Use and Disclosure	Are PII use, sharing, transfer and disclosure controlled and recorded?	Data sharing agreements, approval logs, recipient registers, transfer assessments.			
Data Subject Rights	Are requests from data subjects handled within defined responsibilities and timeframes?	Request logs, identity verification evidence, response records, closure evidence.			
Consent	Where consent is used, is it collected, recorded, managed and withdrawn appropriately?	Consent forms, consent logs, withdrawal records, preference management system.			
Retention and Disposal	Are retention periods defined and is PII securely deleted, anonymized or archived?	Retention schedule, disposal records, deletion tickets, archival controls.			
Privacy Incidents	Are privacy incidents identified, investigated, escalated and recorded?	Incident procedure, incident register, breach assessment, notification decision records, lessons learned.			

Controller and Processor Specific Review Areas

Area	Audit Question	Evidence to Review	Result C/PC/NC/NA	Observations / Findings	Action Required
Controller	Are controller responsibilities for purpose, transparency, rights and processor oversight defined?	Controller responsibility matrix, privacy notices, processor contracts, oversight records.			
Processor	Are processor responsibilities for documented instructions, confidentiality and assistance to controllers controlled?	Processor procedures, customer instructions, confidentiality agreements, service reports.			
Sub-processors	Are sub-processors approved, monitored and subject to privacy obligations?	Sub-processor list, due diligence records, agreements, customer notifications where required.			
Cross-border Transfer	Are international transfers identified and controlled according to applicable obligations?	Transfer register, transfer impact assessments, contractual safeguards, approvals.			
Supplier Privacy	Are suppliers handling PII assessed and monitored?	Supplier assessments, contracts, privacy clauses, performance reviews, corrective actions.			
Privacy by Design	Are privacy requirements considered in projects, systems, products and service changes?	Project privacy checklist, DPIA/PIA, design review notes, change approvals.			
Security of PII	Are security controls coordinated with privacy requirements for PII protection?	Access reviews, encryption records, logging, backup controls, vulnerability management records.			
Complaint Handling	Are privacy complaints received, investigated and resolved?	Complaint register, investigation records, responses, corrective actions.			
Regulatory Interface	Are regulator communications and compliance evidence managed?	Regulator correspondence, compliance calendar, legal register, evidence repository.			

Performance Evaluation and Improvement

Area	Audit Question	Evidence to Review	Result C/PC/NC/NA	Observations / Findings	Action Required
9.1	Does the organization monitor, measure, analyze and evaluate PIMS performance?	PIMS KPIs, privacy metrics, incident trends, request trends, control effectiveness review.			
9.2	Are internal assessments performed at planned intervals and reported to management?	Internal assessment program, checklist, reports, findings, corrective action records.			
9.3	Does management review PIMS suitability, adequacy, effectiveness and improvement needs?	Management review agenda, minutes, input/output records, decisions and action tracking.			
10.1	Are privacy nonconformities controlled and corrective actions implemented?	Nonconformity reports, root cause analysis, correction, corrective action evidence.			
10.2	Is the PIMS continually improved based on performance, incidents, assessments and management review?	Improvement register, trend analysis, improvement projects, updated procedures, lessons learned.			

Audit Summary and Action Plan

Use this section to record major observations, nonconformities, improvement opportunities and agreed actions. Focus on gaps that affect privacy accountability, processing transparency, data subject rights, supplier privacy controls, PII security, incident handling and continual improvement.

No.	Finding / Observation	Clause or Area	Risk / Impact	Corrective Action	Owner / Due Date
1					
2					
3					
4					
5					
6					
7					
8					
9					

Certification Readiness Notes

- Confirm that the PIMS scope, PII inventory, role classification and privacy objectives are approved and current.
- Verify evidence for privacy notices, data subject rights, retention, incident handling, supplier privacy controls and transfer controls.
- Review controller and processor responsibilities separately where the organization performs both roles.
- Complete internal assessment, management review and corrective action closure 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.