Aegentra
ACADEMY

PIMS scope and applicability decision record (ISO/IEC 27701:2025)

The twelve decisions to record before a Statement of Applicability can be produced

Clause 4 asks you to determine the boundaries; this is the record of having done it. The 2025 edition matters here — ISO 27701 is now stand-alone, so the PIMS scope no longer has to sit inside an ISO/IEC 27001 ISMS scope. Integration is now a choice, not a requirement.

#	DECISION TO RECORD	WHY IT MATTERS	WORKED EXAMPLE ANSWER	ANNEX A TABLES ENGAGED	EVIDENCE
1	Is the PIMS standalone or integrated with an existing ISMS?	Since the 2025 revision this is a genuine choice. Integration reuses ISO 27001 clauses 4-10; standalone certifies privacy on its own.	Integrated — an ISO 27001 ISMS is already certified, so the PIMS extends its scope rather than duplicating it	A.1, A.2, A.3	Scope statement approved by management, referencing the ISMS scope if integrated
2	In which activities are we a PII controller?	Decides where Table A.1 applies.	Employee records, recruitment, marketing, website analytics, our own customer account data	A.1	RoPA rows marked controller
3	In which activities are we a PII processor?	Decides where Table A.2 applies.	Customer end-user data hosted in the platform, support tickets	A.2	RoPA rows marked processor, plus the DPAs
4	Which organisational units are in scope?	An unclear boundary is the most common Stage 1 finding.	All Australian entities; the New Zealand subsidiary is excluded this cycle and stated as such	All	Org chart with in-scope units marked and the exclusion justified
5	Which systems process PII?	You cannot protect what is not inventoried.	Platform, CRM, HRIS, payroll, support desk, marketing automation, analytics, SIEM	All	System inventory cross-referenced to the RoPA
6	Where is PII stored and processed geographically?	Drives APP 8 obligations and transfer controls.	Primary AU region; support desk and marketing in the US; backups in Singapore	A.1, A.2	Transfer register with the safeguard for each destination
7	Who are the PII principals?	Different groups carry different expectations and rights.	Employees, job applicants, customer staff, customers' end users, prospects, website visitors	A.1	Principal categories listed in the RoPA
8	What is the legal and regulatory context?	The PIMS has to produce evidence for a named obligation.	Privacy Act 1988 and the 13 APPs; Notifiable Data Breaches scheme; GDPR for EU customers	All	Obligations register with owners
9	Which interested parties have requirements?	Clause 4.2 asks specifically for this.	Customers via contract, the OAIC, employees, the board, insurers	All	Interested-party analysis with the requirement each imposes
10	Which controls are excluded, and why?	Every exclusion needs a scope-based justification an auditor will accept.	Table A.2 controls are applicable because we act as a processor; no exclusions claimed this cycle	A.1, A.2, A.3	Statement of Applicability with a written justification per exclusion
11	Who owns the PIMS?	Clause 5 requires assigned responsibility, not a committee in general.	Privacy Officer owns the PIMS; the CTO owns platform controls; the board Audit and Risk Committee oversees	All	Responsibility matrix signed by management
12	How will effectiveness be measured?	Clause 9 requires monitoring and measurement, not just operation.	Privacy request turnaround, access review completion, transfer register currency, incident count and time to notify	All	Measurement plan with targets and reporting cadence

Free to use and adapt. This template is published in full by Aegentra Academy, an official PECB authorised training partner in Australia. Get the rest of the set and the course it accompanies at aegentra.com.au/academy/iso-27701-lead-implementer.