

A specimen of the AI privacy readiness kit

Five rows from the live record. The paid kit carries all 38 control records, the full evidence list and the dated plan.

SPECIMEN: NOT THE FULL KIT, NOT YOUR DATA

RECORD DATE	2026-10-22
CURRENT RECORD	ISO/IEC 42001:2023, ISO/IEC 27701:2025 and ISO/IEC 27001:2022, the published standards a certificate is issued against
DRAFT	ISO/IEC FDIS 27091, Edition 1, stage 50.00, registered for formal approval 13 July 2026
PLANNING DATE	18 February 2027 (planning estimate, not an ISO date)
TRANSITION	None. The draft is guidance, is not certified against and does not change an ISO/IEC 42001 certificate.
SOURCES	ISO page 56582; its stage feed; ISO/IEC 42001:2023 Annex A record; ISO/IEC 22989:2022 for the lifecycle stages.
LICENCE	One organization, internal use and its consultants. Not for resale. The standard text remains ISO's.

What this is. A register of the controls that apply today, the evidence an auditor asks for, the common gaps and a dated plan. The requirements are our words, not ISO's. The draft text is not public and is not reproduced, and no 27091 clause number is claimed. Dates marked estimate are derived from the public stage record. **Not legal advice; does not certify.**

What is inside

- **The register:** 5 rows, each with the control, the requirement in our words, the privacy overlay, an owner and a due date.
- **The gap list:** 11 common failures, each with an action and an owner.
- **The evidence list:** 16 records an auditor asks for, by control.
- **The dated plan:** 7 milestones from the system register to the review after publication.

How to use it

Start with the register. Put an owner and a due date on every row that is not already evidenced. Use the evidence list to collect the records, the gap list to decide what to fix first, and the plan to sequence the work. Re-check the ISO stage at the planning date; the change watch tells you when the record moves.

Control register (specimen: five rows)

REF	CONTROL	CONTROL TITLE	REQUIREMENT IN OUR WORDS	PRIVACY OVERLAY	OWNER	DUE
ISO42001-A.2.2	A.2.2	AI policy	Document a policy governing how the organization develops or uses AI systems.	Where the draft lands: the policy is the first document it will test Public scope		
ISO42001-A.5.2	A.5.2	AI system impact assessment process	Put in place a way of assessing what an AI system could mean for individuals, groups of individuals and societies across its life cycle.	Where the draft lands: the evaluation mechanism Public scope		
ISO42001-A.6.2.8	A.6.2.8	AI system recording of event logs	Decide in which life cycle phases the AI system records event logs, and make sure it does so at least while it is in use.	Where the draft lands: accountability in operation Reading		
ISO42001-A.7.5	A.7.5	Data provenance	Set out a documented way of keeping a record of where data used in AI systems come from and how they change, over the life of both the data and the system.	Where the draft lands: traceability of personal data Reading		
ISO42001-A.10.3	A.10.3	Suppliers	Set up a process so that the services, products or materials the organization obtains from suppliers fit its approach to developing and using AI systems responsibly.	Where the draft lands: treatment through the contract Reading		

Source for every row: ISO/IEC 42001:2023 Annex A control record, retrieved 2026-10-22. Privacy overlay: the public 27091 record. Not legal advice; does not certify.

Common gaps (specimen: five controls)

CONTROL	COMMON GAP	ACTION	OWNER
A.2.2	Generic IT policy relabelled as the AI policy		
A.2.2	No process for exceptions to the policy		
A.5.2	No defined triggers, so assessments are optional		
A.5.2	Assessment results never feed design decisions		
A.6.2.8	No logging while the system is in use		
A.6.2.8	Logs kept for less time than legal requirements		
A.6.2.8	Out-of-range outputs not captured		
A.7.5	Provenance lost after data transformations		
A.7.5	No verification for third-party data		
A.10.3	Supplied models integrated without documentation		
A.10.3	No corrective action route when a supplier's system misbehaves		

Evidence list (specimen: five controls)

CONTROL	CATEGORY	RECORD AN AUDITOR ASKS FOR	OWNER
A.2.2	AI policy	Documented AI policy covering development and/or use of AI	
A.2.2	AI policy	Evidence the policy reflects business strategy, values, risk appetite, legal and contractual requirements and impact on interested parties	
A.2.2	AI policy	Policy principles and a process for deviations and exceptions	
A.5.2	Impact assessment	Impact assessment procedure stating triggers (criticality of purpose, complexity and automation, data sensitivity, significant changes)	
A.5.2	Impact assessment	Process steps: identification, analysis, evaluation, treatment, documentation and communication	
A.5.2	Impact assessment	Named assessors and the way results inform design or use	
A.6.2.8	Event logging	Logging decision per life cycle phase	
A.6.2.8	Event logging	Operational event logs supporting traceability and detection of operation outside intended conditions	
A.6.2.8	Event logging	Log content such as time of use, production data and out-of-range outputs	
A.6.2.8	Event logging	Log retention aligned with intended use, retention policy and law	
A.7.5	Data provenance	Provenance records covering creation, update, transcription, abstraction, validation, transfer of control, sharing and transformation	
A.7.5	Data provenance	Decision on whether provenance verification measures are needed	
A.10.3	Suppliers	Supplier selection and requirements process scaled to what each supplier provides and its risk	
A.10.3	Suppliers	Supplier monitoring and evaluation records	
A.10.3	Suppliers	Integration documentation for supplied AI components	
A.10.3	Suppliers	Corrective action requests to suppliers and supplier-provided documentation	

Dated plan

DATE	MILESTONE	WHAT IT MEANS	RECORD TO KEEP	DONE
2026-11-30	List the AI systems and the personal data	One register of every AI system the organization develops, buys or uses, with the personal data it touches, the lifecycle stages controlled, the role played and the owner. Mark the systems with no personal data and keep them on the list.	A dated system register with an owner on every row.	
2027-01-31	Settle the role and run the impact assessment	For each system, record whether the organization is a controller, a processor or both, and run the impact assessment over the people in the data: the decision or output, the harm if it is wrong, the likelihood, the severity and the control.	A role determination per system and a current impact assessment with an approver.	
2027-03-31	Fix the data record and the supplier terms	Record the provenance of every dataset and model version, the minimisation decision for each personal data field, and the privacy terms in each AI supplier contract: retention, subprocessors, model change notice and deletion on exit.	A provenance record and reviewed supplier terms.	
2027-06-30	Set the logs and test the incident route	Decide the retention for prompts, outputs and event logs, restrict access, prove that a subject request can be answered, and test the route for an internal and an external privacy concern.	A log retention decision, an access review and a tested incident route.	
2027-09-30	Audit the privacy evidence and review it	Add an AI privacy sample to the internal audit: trace one system from the register through the assessment, the data record, the supplier terms and the logs. Take the indicators and the findings to management review.	An audit report with an AI privacy section and a management review minute.	
2027-02-18	Check the ISO stage at the planning date	The planning date is an estimate. Check the stage feed at 50.20, 50.60, 60.00 and 60.60, and read the published text when it lands. Update the overlays and the procedures if the scope or the subject changed.	A dated stage note and the update list.	
After publication	Update the references and close the loop	Compare the published text with this record and update the procedures, the assessment and the training. Keep the ISO/IEC 42001 or ISO/IEC 27701 certificate and its surveillance cycle; the guidance does not create a transition deadline.	A signed update record and the next review date.	

After publication. Replace the planning date with the date ISO records at stage 60.60, read the published text, update the overlays and the control references, and keep the ISO/IEC 42001 certificate and its surveillance cycle. The register is a working document, not a certificate.