

Specimen: five rows of the oversight register

ISO/IEC FDIS 42105, Edition 1, stage 50.20 FDIS ballot, 26 August 2026. The draft is guidance, not a certifiable requirement. The register states the held oversight controls the guidance will operate on, in our words, with the clause cited. The planning date of 16 February 2027 is our estimate from the stage record, not an ISO date.

What this is. This is a labelled specimen: the first five rows of the register, the column order and the plan. It is not a client record. 47 units, 142 evidence items, 102 common gaps, the plan and the board brief. It does not reproduce the ISO text and it does not certify.

The dated plan

When	Action	What it covers	Evidence to keep
Days 1 to 14	Decide and record	Decide whether to adopt the guidance, watch it or decline it. Record the decision, the owner and the reason.	A one-page decision record with owner and date.
Days 15 to 30	Name the systems and roles	Inventory every AI system with an owner, purpose, life-cycle stage, risk tier and role.	A dated inventory with a named person per system.
Days 31 to 45	Approve the policy and the authority	Approve the oversight policy and name the person who can pause, override and stop the system.	The approved policy and the role authority.
Days 46 to 60	Set the impact thresholds	Define sensitive and restricted uses, the impact scale and the approval route above a threshold.	The threshold document and the approval route.
Days 61 to 75	Write the operator pack	Give the operator the intended use, the limits, the failure modes and the override procedure.	The operator pack, versioned, with the date received.
Days 76 to 90	Test the override and the stop	Run a live test at production volume and record the time it took.	The test record, the time and the person who invoked it.
Days 91 to 105	Measure and review	Put an oversight measure in place, take the first reading and book the management review.	The measure, the reading and the review date.
Days 106 to 120	Audit and brief the board	Sample the oversight decisions, record the findings and brief the board on the date and the decisions.	The audit sample, the findings and the one-page brief.
On publication	Re-baseline	Rebuild the register against the published ISO/IEC 42105 text and record the change.	The published record, the reissued files and the change log row.
Plus 90 days	Prove it operates	Show a quarter of evidence, the review and the corrective action if the measure moved.	The quarterly evidence pack and the review minute.

The register

Ref	Unit	Theme	Held citation	Requirement	Oversight meaning	Evidence	Gap
OH-01	Context and the role you play	Accountability	ISO/IEC 42001:2023, 4.1	Work out the internal and external issues that affect whether the AI management system can do what it is meant to, and settle which role the organization plays for each AI system: provider, producer, customer, partner or subject. The role determines which duties follow.	The overseer's duty changes with the role. A provider must design oversight into the system; a deployer must assign it to competent people. If the role is recorded only for the organization as a whole, the operator of a specific system has no stated duty.	A register of internal and external issues, with a recorded decision on climate change; A documented role determination for each AI system in scope; An intended purpose statement for each system	Role recorded for the organization as a whole but not per system; Legal issues such as prohibited uses missing from the issues register
OH-02	What the management system covers	Accountability	ISO/IEC 42001:2023, 4.3	Set the boundaries and applicability of the AI management system, and keep the scope as documented information. The scope fixes which activities the management-system requirements cover, and it must be traceable to the context analysis.	An oversight register that sits outside the management-system scope will not be audited, resourced or reviewed. The scope should name the systems, the business units and the third parties whose oversight controls are inside the system.	A documented scope statement; Traceability from the scope to the context issues and interested-party requirements; A list of systems and activities inside and outside the scope, with reasons	Systems in use excluded without justification; Scope not linked to the context analysis
OH-03	The AI policy	Accountability	ISO/IEC 42001:2023, 5.2	Top management must set an AI policy suited to the organization's purpose that gives a framework for objectives, commits to meeting applicable requirements and commits to continual improvement. It must be documented, communicated and available to interested parties where suitable.	The policy is where the authority to override and stop a system should be granted. A policy that commits to human oversight without naming who may intervene leaves the operator with a duty and no power.	An approved policy with the four required elements; Cross-references to related policies; Communication records and the version in force	Policy lacks the commitment to meet applicable requirements; Policy never communicated beyond the governance team
OH-04	Roles, responsibilities and authorities	Accountability	ISO/IEC 42001:2023, 5.3	Top management must allocate responsibilities and authorities, make them known, and assign responsibility for keeping the management system conformant and for reporting its performance to top management.	This is the clause that makes oversight a job rather than a committee. Name the person who can pause or stop the system, the person who reviews the decision and the person who reports performance upward.	A role matrix or RACI for the AI management system; A named owner for conformity; A named owner for performance reporting, with the reporting date	No one assigned to report performance to top management; Roles assigned but not communicated
OH-05	AI risk assessment	Life cycle	ISO/IEC 42001:2023, 6.1.2	Run a defined process for assessing AI risk that follows the policy and objectives, gives comparable results when repeated, identifies risks to the objectives, and analyses consequences for the organization, individuals and society, with realistic likelihood where applicable.	The risk assessment decides where oversight is needed and how intense it should be. If consequences are assessed only for the organization, the overseer is not told what the system can do to a person.	The risk assessment procedure; Evidence the method gives comparable results when repeated; A consequence analysis covering the organization, individuals and society	Consequences assessed for the organization only; Scoring changes between assessments so results cannot be compared

Board brief (one page)

ISO/IEC FDIS 42105 is draft guidance on human oversight of AI systems. It is at the FDIS ballot, stage 50.20, and is not published. The planning date is 16 February 2027, our estimate. The board is asked to take three decisions: adopt or decline the guidance as an internal reference; name the person who can pause, override and stop each high-impact system; and approve the 120-day plan and its resource. The evidence the auditor will ask for is the policy, the named role and its authority, the operator pack, the tested override, the logs, the measures and the review. This is not a certification and not legal advice.

Item	Decision	Owner	Date	Reason
Adopt ISO/IEC 42105 as guidance, watch it, or decline it				
Apply the 47-unit register to the AIMS oversight controls				
Name the person who can pause, override and stop each system				
Set the sensitive and restricted use thresholds				
Subscribe to the change watch				
Review the register at the next management review				

Not legal advice; does not certify. Source record: a5798f632c2c0f21. Retrieved 2026-10-21. The full register columns, the evidence list and the plan are in the CSV and XLSX.