

ISO 42001 Scope & Evidence Intake Kit

Define your AIMS scope, map controls to evidence, and surface readiness gaps fast; so you know exactly what to fix before the audit.

Control ID	Control Area	Questions	Artifacts
4.1	Context of the Organization	Has the organization identified internal and external issues relevant to its AI systems (regulatory, ethical, technical, market)?	Documented AIMS context analysis; AI regulatory landscape assessment; business strategy documents
4.2	Interested Parties	Have relevant interested parties (customers, regulators, developers, cloud providers) and their AI-related requirements been identified?	Stakeholder register; customer contracts; regulatory requirement mapping
4.3	Scope of AIMS	Is the scope of the AI Management System clearly defined, including cloud platforms, AI models, data pipelines, and teams?	AIMS scope statement; cloud architecture diagrams; in-scope AI inventory
4.4	AIMS	Has an AI Management System been established, implemented, maintained, and continually improved?	AIMS manual; process maps; governance operating model
5.1	Leadership	Does top management demonstrate accountability and support for AI governance and risk management?	Executive AI governance charter; steering committee minutes
5.2	AI Policy	Is there an approved AI policy addressing responsible use, risk, and compliance?	AI Governance Policy; Responsible AI Policy
5.3	Roles & Responsibilities	Are AI roles, responsibilities, and authorities defined for engineering, security, and compliance?	RACI matrix; job descriptions; AI accountability assignments
6.1	Risk & Opportunity Actions	Are AI risks and opportunities identified, assessed, and addressed across the AI lifecycle?	AI risk register; AI impact assessments; threat models
6.2	AI Objectives	Have measurable AI objectives been established and monitored?	AI KPIs/KRIs; OKRs; monitoring dashboards
7.1	Resources	Are sufficient resources (people, cloud infrastructure, tooling) allocated to manage AI responsibly?	Cloud capacity plans; ML tooling inventory; staffing plans
7.2	Competence	Are AI engineering personnel competent based on education, training, and experience?	Training records; certifications; skills matrix
7.3	Awareness	Are personnel aware of AI policies, risks, and their responsibilities?	Security & AI awareness training; attestations
7.4	Communication	Are internal and external AI-related communications defined and controlled?	Communication plans; customer AI disclosures
7.5	Documented Information	Is AI documentation controlled, versioned, and retained appropriately?	Document control procedures; policy repositories
8.1	Operational Planning	Are AI lifecycle processes planned and controlled (design, development, deployment, monitoring)?	SDLC/ML lifecycle procedures; MLOps workflows
9.1	Monitoring & Measurement	Is AI performance and risk effectiveness regularly measured and reviewed?	Metrics reports; management review inputs
9.2	Internal Audit	Are internal audits of the AIMS conducted at planned intervals?	Internal audit plans; audit reports
9.3	Management Review	Does top management review the AIMS and AI risks regularly?	Management review minutes
10.1	Nonconformity & Corrective Action	Are AI nonconformities addressed with root cause analysis and corrective actions?	Corrective action plans; RCA documentation
10.2	Continual Improvement	Is the AIMS continually improved based on monitoring, audits, and incidents?	Improvement backlog; roadmap updates
A.4.1	Resources for AI systems	Have required technical, human, cloud, and financial resources for AI systems been identified and documented across lifecycle stages?	AI architecture diagrams; cloud resource inventories; MLOps tooling lists; skills matrix
A.4.2	Resources for AI systems	Are responsibilities assigned for managing AI infrastructure, models, and supporting services?	RACI charts; platform ownership documentation
A.5.1	Assessing impacts of AI systems	Has the organization defined criteria to assess ethical, legal, operational, and societal impacts of AI systems?	AI Impact Assessment methodology; risk scoring criteria
A.5.2	Assessing impacts of AI systems	Are AI impact assessments performed prior to deployment and upon significant changes?	Completed AI impact assessments; change management records
A.6.1	AI system life cycle	Is a documented AI system lifecycle defined covering design, development, testing, deployment, monitoring, and retirement?	AI/ML SDLC documentation; MLOps pipelines
A.6.2	AI system life cycle	Are controls applied at each lifecycle stage to address risk, security, and compliance?	Lifecycle control checklists; gated deployment approvals
A.7.1	Data for AI systems	Are data sources for AI systems identified, classified, and approved prior to use?	Data inventories; data classification registers
A.7.2	Data for AI systems	Are data quality, bias, and representativeness evaluated and documented?	Bias assessments; data quality metrics
A.7.3	Data for AI systems	Are controls in place for data protection, retention, and deletion in AI pipelines?	Data governance policy; retention schedules; deletion logs
A.8.1	Information for interested parties	Is appropriate information about AI system purpose, limitations, and risks provided to customers and other interested parties?	Customer AI disclosures; product documentation
A.8.2	Information for interested parties	Are communication channels established to address AI-related inquiries or concerns?	Support workflows; incident escalation procedures
A.9.1	Use of AI systems	Are acceptable and prohibited uses of AI systems defined and communicated?	AI Acceptable Use Policy; user guidelines
A.9.2	Use of AI systems	Are mechanisms in place to detect and respond to misuse of AI systems?	Usage monitoring; abuse detection alerts
A.10.1	Third-party & customer relationships	Are third-party AI providers and components assessed for risk, compliance, and contractual obligations?	Vendor AI risk assessments; due diligence reports
A.10.2	Third-party & customer relationships	Do contracts define responsibilities for AI data, models, security, and compliance?	Customer and vendor contracts; DPAs; AI clauses
A.10.3	Third-party & customer relationships	Are ongoing monitoring and reviews performed for third-party AI services?	AI Vendor performance reviews; reassessment schedules