Kailash Consult Free resource · kailashconsult.com/resources

ISO 42001 Readiness Checklist

Every ISO/IEC 42001:2023 clause and Annex A control area in plain words, the evidence an auditor expects, and the gap teams most often miss.

How to use

- Work through clauses 4 to 10 first: they are the management system an auditor certifies.
- Then decide which Annex A controls apply to you and record why in your Statement of Applicability.
- Use 'Your status' to track Ready, Partial, Not yet or N/A. Partial and Not yet are your gap list.

Example answers and mappings are templates, not facts about your company. Edit every bracket and validate each statement before sharing it with a customer or auditor.

Context and scope (clause 4)

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E01	4.1 Context	Know the internal and external issues that affect your AI management system, including your role (developer, provider, user of AI).	Context document listing issues and your AI role(s).	AI role not stated, so obligations stay unclear.
E02	4.2 Interested parties	Identify who cares about your AI systems (customers, users, regulators) and what they require.	Interested parties register with requirements.	Customer AI requirements from contracts not captured.
E03	4.3 Scope	Define which AI systems, products, teams and locations the AIMS covers.	Written scope statement.	Scope too vague to audit, or excludes the main AI product.
E04	4.4 AI management system	Establish, run and improve the AIMS as a whole.	AIMS manual or overview linking all parts.	Documents exist but nothing ties them together.

Kailash Consult

Leadership (clause 5)

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E05	5.1 Leadership	Top management visibly backs the AIMS and gives it resources.	Approved policy, budget, meeting minutes.	Leadership involvement not evidenced.
E06	5.2 AI policy	A leadership-approved AI policy fit for your purpose, with commitments to meet requirements and improve.	Signed AI policy, communicated to staff.	Generic AI policy copied from a template.
E07	5.3 Roles	Assign and communicate AIMS roles, responsibilities and authorities.	RACI or role descriptions.	No one clearly owns AI risk.

Planning (clause 6)

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E08	6.1.2 AI risk assessment	A repeatable method to identify, analyze and evaluate AI risks.	Risk method and AI risk register.	Only security risks, no AI-specific risks (bias, misuse, reliability).
E09	6.1.3 AI risk treatment	Choose treatments and controls, and produce a Statement of Applicability against Annex A.	Risk treatment plan; Statement of Applicability with reasons.	Annex A controls excluded with no justification.
E10	6.1.4 AI system impact assessment	Assess consequences of AI systems for individuals, groups and society.	Impact assessment per AI system.	Impact assessment missing or done once and never updated.
E11	6.2 AI objectives	Measurable AI objectives with owners, resources and deadlines.	Objectives list with metrics.	Objectives are not measurable.
E12	6.3 Planning of changes	Make changes to the AIMS in a planned way.	Change records.	Changes made ad hoc.

Support (clause 7)

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E13	7.1 Resources	Provide what the AIMS needs: people, tools, data, compute.	Resource plan or budget.	AI governance has no budget or time.
E14	7.2 Competence	People doing AIMS work are competent, with evidence.	Training records, role skills matrix.	No record of AI-specific competence.

Kailash Consult

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E15	7.3 Awareness	Staff know the AI policy and their part in it.	Awareness training completion.	Engineers unaware of the AI policy.
E16	7.4 Communication	Decide what to communicate about the AIMS, to whom and when.	Communication plan.	External communication undefined.
E17	7.5 Documented information	Control AIMS documents: versions, approval, access.	Document control procedure.	Out-of-date documents in use.

Operation (clause 8)

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E18	8.1 Operational control	Run AI processes as planned and control outsourced parts.	Procedures and evidence they are followed.	Outsourced model providers not controlled.
E19	8.2 to 8.4 Assessments in operation	Repeat AI risk assessment, treatment and impact assessment at planned intervals and on change.	Dated reassessments.	Assessments not rerun after a model or feature change.

Performance and improvement (clauses 9 and 10)

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E20	9.1 Monitoring	Decide what to measure about AI systems and the AIMS, and do it.	Metrics and monitoring results.	No AI performance monitoring after release.
E21	9.2 Internal audit	Audit the AIMS at planned intervals, independently.	Audit plan and report.	No internal audit before certification.
E22	9.3 Management review	Leadership reviews AIMS performance and decides changes.	Management review minutes.	Review never held or not minuted.
E23	10.1 / 10.2 Improvement	Fix nonconformities, find root causes and keep improving.	Corrective action log.	Issues fixed without root cause analysis.

Free to use inside your company. Not for resale. kailashconsult.com/resources

Annex A control areas

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E24	A.2 Policies related to AI	AI policy, aligned with other policies, reviewed regularly.	AI policy and review record.	AI policy conflicts with security or privacy policies.
E25	A.3 Internal organization	Roles for AI and a way to report AI concerns.	Roles; concern reporting process.	No channel for staff to raise AI concerns.
E26	A.4 Resources for AI systems	Document data, tools, compute and people used by AI systems.	Resource inventory per AI system.	Model and data dependencies undocumented.
E27	A.5 Assessing impacts of AI systems	Process to assess impacts on individuals, groups and society, and record results.	Impact assessment procedure and records.	Societal impacts ignored.
E28	A.6 AI system life cycle	Responsible design, requirements, verification and validation, deployment, operation, monitoring, technical documentation and event logs.	Life cycle records per AI system.	No validation evidence before release; no event logs.
E29	A.7 Data for AI systems	Data acquisition, quality, provenance and preparation are managed.	Data records: sources, quality checks, lineage.	Training or fine-tuning data provenance unknown.
E30	A.8 Information for interested parties	Users get the documentation they need; incidents and required reports are communicated.	User documentation; incident communication process.	No customer-facing AI documentation.
E31	A.9 Use of AI systems	Processes and objectives for responsible use, and use only as intended.	Intended use statements; responsible use process.	Intended use not defined, so misuse cannot be detected.
E32	A.10 Third-party and customer relationships	Allocate responsibilities with suppliers and customers; manage AI suppliers.	Supplier assessments; contract clauses.	Model providers not assessed as AI suppliers.

Certification path

ID	Clause / control	What it requires (plain words)	Evidence an auditor expects	Common gap
E33	Stage 1 audit	Certification body reviews your documentation and readiness.	Complete AIMS documentation.	Booked before internal audit and management review are done.
E34	Stage 2 audit	Certification body checks the AIMS works in practice.	Records showing operation over time.	Too little operating evidence.
E35	Surveillance	Certificate is valid three years with annual surveillance audits.	Ongoing records.	AIMS stops running after certification.

Free to use inside your company. Not for resale. kailashconsult.com/resources

Free resource from Kailash Consult. Free to use inside your company. Not for resale or redistribution. kailashconsult.com/resources

Kailash Consult