ISO/IEC 42001 Annex A — All 38 Controls on Two Pages

Your plain-English map of the AI Management System (AIMS) control set. ISO/IEC 42001:2023 groups its **38 Annex A controls into 9 objectives**, from AI policy through third-party relationships. Use this sheet to scope your Statement of Applicability, brief stakeholders, or follow along during the live session.

A.2 Policies | A.3 Organization | A.4 Resources | A.5 Impact Assessment | A.6 Life Cycle | A.7 Data | A.8 Interested Parties | A.9 Use of AI | A.10 Third Parties

A.2 Policies Related to AI — 3 controls

Objective: give management direction and support for AI, in line with business and regulatory requirements.

A.2.2 AI policy
Publish a formal, management-approved policy stating how your organization develops and uses AI.

A.2.3 Alignment with other policies
Check where AI touches existing policies (security, privacy, HR, quality) and keep them consistent.

A.2.4 Review of the AI policy
Revisit the AI policy at planned intervals — and whenever technology, law, or risk changes.

A.3 Internal Organization — 2 controls

Objective: establish accountability so responsible AI has clear owners inside the organization.

A.3.2 AI roles and responsibilities
Assign a named owner for every AI-related duty — no orphaned responsibilities.

A.3.3 Reporting of concerns
Give staff a safe, defined channel to raise concerns about how AI systems behave.

A.4 Resources for AI Systems — 5 controls

Objective: account for every resource an AI system depends on, so risks can be fully understood.

A.4.2 Resource documentation
Keep an inventory of everything each AI system needs to run — data, tools, compute, people.

A.4.3 Data resources
Document the data your AI systems rely on: what it is, where it comes from, how it's handled.

A.4.4 Tooling resources
Record the tools, frameworks, and libraries behind each AI system's build and operation.

A.4.5 System & computing resources
Document the infrastructure and compute that host, train, and serve your AI systems.

A.4.6 Human resources
Identify the skills and people required across each stage of the AI life cycle.

A.5 Assessing Impacts of AI Systems — 4 controls

Objective: assess how AI systems affect individuals, groups, and society throughout their life cycle.

A.5.2 Impact assessment process
Define a repeatable process for assessing the potential consequences of each AI system.

A.5.3 Documentation of assessments
Write assessment results down and retain them for a defined period — auditors will ask.

A.5.4 Impact on individuals & groups
Evaluate how the system could affect specific people or groups — fairness, safety, privacy, rights.

A.5.5 Societal impacts
Consider the wider picture: environmental, economic, and cultural effects of the system.

A.6 AI System Life Cycle — 9 controls

Objective: ensure responsible design, development, deployment, and operation — the largest control group.

A.6.1.2 Objectives for responsible development
Set measurable responsible-AI objectives — fairness, transparency, safety — before you build.

A.6.1.3 Responsible design & development processes
Bake responsible-AI checkpoints directly into your design and development workflow.

A.6.2.2 Requirements and specification
Specify what the AI system must do — and must not do — before development begins.

A.6.2.3 Documentation of design & development
Record key design choices: architecture, model selection, training decisions, trade-offs.

A.6.2.4 Verification and validation
Test that the system works as specified and actually meets its responsible-AI objectives.

A.6.2.5 Deployment
Release AI systems through a controlled, documented deployment process — no silent go-lives.

A.6.2.6 Operation and monitoring
Monitor behavior and performance in production; detect and act on drift or failures.

A.6.2.7 Technical documentation
Maintain technical docs so users, operators, and auditors can understand the system.

A.6.2.8 Recording of event logs
Keep event logs so incidents can be traced, investigated, and explained after the fact.

A.7 Data for AI Systems — 5 controls

Objective: manage data as a governed asset — because AI quality and risk start with data quality.

A.7.2 Data for development & enhancement
Define and manage the data used to train, tune, and improve AI systems.

A.7.3 Acquisition of data
Know exactly where data comes from — and confirm you have the rights to use it.

A.7.4 Quality of data
Define quality criteria for AI data and check that datasets actually meet them.

A.7.5 Data provenance
Track the origin and every transformation of your data, end to end.

A.7.6 Data preparation
Document how data is selected, cleaned, labeled, and transformed before use.

A.8 Information for Interested Parties — 4 controls

Objective: keep users, regulators, and stakeholders properly informed about your AI systems.

A.8.2 System documentation & user information
Tell users what the system does, its limitations, and how to use it correctly.

A.8.3 External reporting
Let external parties report adverse impacts — and have a process to handle those reports.

A.8.4 Communication of incidents
Notify affected parties when an AI incident occurs, in a planned and timely way.

A.8.5 Information for interested parties
Provide stakeholders the information they're entitled to — obligations, disclosures, updates.

A.9 Use of AI Systems — 3 controls

Objective: ensure AI systems — including those you buy — are used responsibly and as intended.

A.9.2 Responsible use processes
Define rules for using AI responsibly — covering internal builds and third-party AI alike.

A.9.3 Objectives for responsible use
Set objectives for responsible use and manage day-to-day usage against them.

A.9.4 Intended use of the AI system
Use each system only for its documented, intended purpose — scope creep is a risk event.

A.10 Third-Party & Customer Relationships — 3 controls

Objective: manage AI risks and responsibilities that cross organizational boundaries.

A.10.2 Allocating responsibilities
Make AI responsibilities explicit across suppliers, partners, and customers — in writing.

A.10.3 Suppliers
Ensure suppliers' AI products and services meet your responsible-AI requirements.

A.10.4 Customers
Consider customer needs and expectations when they are the ones using your AI.

Already ISO 27001 certified? You have a head start: your ISMS governance, risk process, supplier controls, and documentation discipline map directly onto large parts of A.2, A.3, A.7 and A.10. We'll walk through the overlap live in the session — bring this sheet and your questions.

See These Controls in Action — Live

Join GSDC's ISO 27001 & ISO 42001 Webinar 2026 for expert-led guidance on information security, AI governance, and building an audit-ready AIMS. Your seat is reserved — [SESSION DATE & TIME].

JOIN THE SESSION

gsdcouncil.org/certification-program/iso-27001-and-42001-webinar-2026