ISO/IEC 42001 Readiness & Gap Assessment Checklist

A practical checklist for assessing AI management system readiness against ISO/IEC 42001:2023 clauses 4 to 10 and Annex A

ISO/IEC 42001 · ISO/IEC 23894 · ISO 31000 · EU AI Act · ISO 27001

Certification against ISO/IEC 42001 depends on an AI management system that runs, not an AI policy on file. This checklist follows the clause structure of the standard, so each gap you find points to the clause an auditor will test.

A Context & Scope (Clause 4)

- ☐ External and internal issues relevant to your AI use are documented, including legal, ethical and contractual factors
- ☐ Your role for each AI system is defined, for example AI provider, producer, customer or partner
- ☐ Interested parties and their requirements are identified, including customers, regulators and affected people
- ☐ The scope of the AI management system is documented, naming the AI systems, sites and business units covered

B Leadership & AI Policy (Clause 5)

- ☐ Top management has approved the AI policy and shows commitment through resources and review
- ☐ The AI policy covers your AI objectives, commitments to applicable requirements and continual improvement
- ☐ The AI policy is version-controlled, communicated and available to interested parties as appropriate
- ☐ Roles, responsibilities and authorities for the AI management system are assigned to named people

C Planning: Risk, Impact & Objectives (Clause 6)

- ☐ An AI risk assessment process is defined with criteria for acceptable risk, and applied to each AI system
- ☐ AI risk treatment selects controls, and every Annex A control is recorded as applied or excluded with a reason in the Statement of Applicability
- ☐ An AI system impact assessment process covers consequences for individuals, groups and society
- ☐ Measurable AI objectives are set, with owners, resources, deadlines and a way of tracking them
- ☐ Changes to the AI management system are planned rather than made ad hoc

D Support (Clause 7)

- [ ] Resources for the AI management system are identified: people, data, tools, systems and computing
- [ ] Competence requirements are defined for AI roles, with training and evidence of competence kept
- [ ] Staff know the AI policy, their contribution and the consequences of not following it
- [ ] Documented information required by the standard is controlled, versioned and retained

E Operation (Clause 8)

- [ ] Operational processes for AI systems are planned, controlled and evidenced
- [ ] AI risk assessments are repeated at planned intervals and when significant changes are proposed
- [ ] Risk treatment plans are implemented and their effectiveness is checked
- [ ] AI system impact assessments are repeated when systems or their context change
- [ ] Externally provided AI systems, data and services are controlled

F Annex A Controls

- [ ] Policies related to AI and the internal organisation, including a process for reporting concerns (A.2, A.3)
- [ ] Resources and data for AI systems are documented and managed for quality, provenance and preparation (A.4, A.7)
- [ ] Impact on individuals, groups and society is assessed and documented (A.5)
- [ ] The AI system life cycle is controlled from requirements through design, verification, deployment, operation and monitoring (A.6)
- [ ] Information for interested parties, responsible use of AI and third-party and customer relationships are covered (A.8 to A.10)

G Performance Evaluation (Clause 9)

- [ ] What is monitored and measured is defined, including AI system performance and AI objectives
- [ ] An internal audit programme covers the whole AI management system, with independent auditors
- [ ] Management review is held at planned intervals and covers audit results, risks, objectives and changes
- [ ] Results of monitoring, audit and management review are retained as evidence

H Improvement & Certification Readiness (Clause 10)

- [ ] Nonconformities are recorded, root causes found and corrective actions tracked to closure
- [ ] The effectiveness of corrective actions is checked before they are closed
- [ ] Continual improvement of the AI management system is evidenced, not only stated
- [ ] The Statement of Applicability matches the controls actually in place on the day of the audit
- [ ] An accredited certification body has been selected and the Stage 1 documentation review planned

© XGRC® Software, a Strategix product. Strategix Application Solutions (Pty) Ltd, Reg No. 2015/192960/07. ISO 27001:2022 certified. info@xgrcsoftware.com