CHECKLIST

ISO 42001

ISO/IEC 42001 alignment involves establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) to govern the responsible use of AI across its lifecycle. ISO/IEC 42001 certification is achieved through an independent, accredited certification body following a formal audit process. Advisory organizations may support readiness and internal preparation but do not conduct certification audits or issue certificates.

This checklist explains what organizations should expect when preparing for ISO/IEC 42001 certification, including how governance activities are planned, implemented, evaluated, and improved. It focuses on management system readiness and internal alignment and does not represent a certification audit.

Independence & Role Clarity Statement

ISO/IEC 42001 certification audits are strictly independent. Advisory organizations do not perform certification audits, make certification decisions, or issue ISO/IEC 42001 certificates.

Preparation & Context

- [ ] Identify and document external factors affecting AI governance (e.g., regulatory landscape, market expectations, societal impact).
- [ ] Identify internal factors, including organizational structure, culture, technology environment, and existing management systems.
- [ ] Identify interested parties (customers, regulators, employees, affected stakeholders) and their AI-related expectations.
- [ ] Define and document the scope of the Artificial Intelligence Management System (AIMS), including in-scope AI systems, processes, and organizational units.

Leadership & Commitment

- [ ] Obtain documented top management commitment to AI governance and the AIMS.
- [ ] Assign and communicate roles, responsibilities, and authorities related to AI governance.
- [ ] Establish appropriate AI governance oversight, such as a steering committee or cross-functional governance group.
- [ ] Develop, approve, and communicate an AI governance policy addressing ethical use, transparency, accountability, and risk management.

Risk Planning

- [ ] Conduct AI risk assessments addressing technical, ethical, operational, legal, and reputational risks.
- [ ] Perform AI system impact assessments to evaluate potential impacts related to fairness, bias, explainability, and societal effects.
- [ ] Define AI governance objectives aligned with identified risks and organizational priorities.
- [ ] Develop risk treatment plans, including mitigation actions, ownership, and timelines.
- [ ] Plan integration with existing management systems (e.g., ISO/IEC 27001, ISO 9001, ISO 27701), where applicable.

Support & Capacity Building

- [ ] Allocate sufficient resources (personnel, tools, budget) to support AIMS operation.
- [ ] Ensure personnel have defined competence for AI-related roles and responsibilities.
- [ ] Implement training and awareness programs covering AI risks, governance obligations, and ethical responsibilities.
- [ ] Establish internal and external communication processes for AI governance matters.
- [ ] Maintain controlled documented information, including policies, procedures, risk assessments, and records.

Operationalization

- [ ] Implement AI lifecycle controls covering design, development, deployment, monitoring, and retirement.
- [ ] Establish data governance controls, including data quality, provenance, privacy, and consent management.
- [ ] Manage third-party AI components and vendors through due diligence, contractual requirements, and ongoing monitoring.
- [ ] Embed human oversight mechanisms, including defined escalation and override procedures.
- [ ] Implement change management for AI system updates and modifications.
- [ ] Establish incident detection and response processes specific to AI-related failures or unintended outcomes.

Performance Evaluation

- [ ] Define and monitor key performance indicators (KPIs) to measure AIMS effectiveness.
- [ ] Conduct internal audits to assess conformity with ISO/IEC 42001 requirements and internal governance processes.
- [ ] Perform management reviews to evaluate performance, resource adequacy, and improvement opportunities.
- [ ] Document nonconformities, incidents, corrective actions, and lessons learned.

Improvement

- [ ] Establish corrective and preventive action (CAPA) processes to address identified gaps or failures.
- [ ] Update policies, procedures, and risk assessments based on audit results, incidents, and evolving AI use cases.
- [ ] Maintain continuous improvement mechanisms aligned with organizational learning and regulatory change.
- [ ] Promote a culture of ongoing accountability, transparency, and responsible AI governance.

Preparing for Certification

Organizations typically engage an accredited certification body to perform ISO/IEC 42001 certification audits once AIMS readiness activities are complete. Prior to certification, many organizations conduct internal audits or independent readiness assessments to validate scope, documentation, and operational effectiveness.

About RSI Security

RSI Security supports organizations in designing, implementing, and maturing Artificial Intelligence Management Systems (AIMS) aligned with ISO/IEC 42001 requirements.

Our services focus on governance design, risk management, documentation support, internal audit preparation, and certification readiness, while maintaining strict independence from certification activities.

www.rsisecurity.com | (858) 999-3030 | info@rsisecurity.com