5. ISO/IEC 42001 AI risk assessment checklist

Use this checklist before approving deployment of an AI system or AI-enabled use case. It is designed to support ISO/IEC 42001-aligned assessment evidence and should be used with your organization's AIMS procedure, risk criteria, and licensed copy of the standard.

AI system / use case	Business owner	Assessment date	Reviewer / approver

☐ Not started	☐ In progress	☐ Complete	☐ Exception approved	☐ Reassessment required

Scope and governance

- ☐ AI system is in the AI inventory.
- ☐ Business owner is assigned.
- ☐ Technical owner is assigned.
- ☐ Intended use is documented.
- ☐ Prohibited uses are documented.
- ☐ Lifecycle stage is documented.
- ☐ Assessment scope and exclusions are approved.

Impact and stakeholders

- ☐ Affected individuals and groups are identified.
- ☐ Customer, employee, societal, and organizational impacts are considered.
- ☐ Vulnerable or protected groups are considered where relevant.
- ☐ Human rights, fairness, safety, privacy, and accessibility impacts are considered.
- ☐ Impact assessment is updated for the current use case.

Data and model

- ☐ Data sources are documented.
- ☐ Data quality is assessed.
- ☐ Personal or sensitive data is identified.
- ☐ Data provenance and usage rights are reviewed.
- ☐ Model limitations are documented.
- ☐ Validation results are available.
- ☐ Bias/fairness testing is performed where relevant.
- ☐ Robustness and security testing are performed where relevant.

Operations and human oversight

- ☐ Human oversight is defined.
- ☐ Users are trained.
- ☐ Escalation path exists.
- ☐ Override process exists.
- ☐ Logs are retained.
- ☐ Incident process includes AI-related events.
- ☐ Change-management process covers model, data, prompt, and vendor changes.

Supplier and third-party risk

- ☐ Vendor role is documented.
- ☐ Vendor due diligence is completed.
- ☐ Data-use terms are reviewed.
- ☐ Audit or assurance evidence is obtained where needed.
- ☐ Model/version-change notification requirements are defined.
- ☐ Exit or fallback plan exists.

Risk treatment and acceptance

- ☐ Inherent risks are scored.
- ☐ Risk treatment plan is documented.
- ☐ Controls are mapped to risks.
- ☐ Residual risks are scored.
- ☐ Acceptance authority is appropriate.
- ☐ Acceptance has review date and conditions.
- ☐ Monitoring plan is active.

Assessment notes

Open issues / exceptions	
Evidence links or file references	
Approval conditions / next review date	