AI Risk Assessment Starter Template

Prepared by Dynamic Comply

This template provides a **high-level starting point** for identifying and assessing Artificial Intelligence (AI) risks within your organization. It is structured to align with the principles of ISO/IEC 42001, the international standard for Artificial Intelligence Management Systems (AIMS). ISO/IEC 42001:2023 requires organizations to establish processes for identifying and managing risks associated with their AI systems. This template is a simplified guide; a comprehensive ISO/IEC 42001 implementation will involve more detailed risk assessments, controls, and documentation.

Use this template to begin identifying potential AI risks relevant to your organization's context and the defined scope of your AIMS.

1. **AI System Name & Description**:

_____

2. **Intended Purpose and Use Case**:

_____

3. **Who Uses the AI?** (internal users, customers, public, etc.)

_____

4. **What Data Does It Use?**

_____

5. **Does It Involve Personal or Sensitive Data?**

□ Yes □ No

6. **Potential Harms if the AI Fails or Misbehaves**:

- Reputational harm

- Legal or regulatory risk

- Safety risks

- Privacy violations

(Check all that apply)

7. **Current Risk Mitigations in Place**:

_____

8. **Known Issues or Concerns**:

_____

Key AI Risk Categories to Consider:

ISO/IEC 42001 Annex C provides potential AI-related organizational objectives and risk sources to consider when managing risks. Other sources highlight common AI risks:

- **Bias & Fairness Risks:** Potential for discriminatory outcomes due to data or algorithmic issues, including algorithmic bias and dataset contamination.
- **Security Risks:** Vulnerabilities to adversarial attacks, data poisoning, unauthorized access, data breaches, and other cyber threats.
- **Transparency, Explainability & Accountability Risks:** Difficulty understanding how AI decisions are made (lack of explainability), lack of traceability, or unclear responsibility for AI outcomes.
- **Data Quality Risks:** Issues with the accuracy, completeness, representativeness, integrity, or provenance of data used by AI systems.
- **Compliance & Regulatory Risks:** Failure to meet legal, ethical, or regulatory requirements related to AI use, including adherence to standards like GDPR, the EU AI Act, or NIST AI RMF.
- **Performance & Reliability Risks:** AI system failure, model drift, inaccuracy of generated data, or failure to meet objectives.
- **Impact on Users & Stakeholders:** Potential negative consequences for individuals or groups affected by the AI system.
- **Third-Party/Supply Chain Risks:** Risks introduced by using AI systems, data, or services provided by external vendors or suppliers.

Risk Assessment Table Structure:

Identify potential risks associated with your AI systems based on the categories above and your specific context, and document them using a structure similar to this table. ISO 42001 requires evaluating risks based on likelihood and impact.

Risk ID	Identified Risk (Brief Description)	Affected AI System / Process / Data Source	Potential Impact (What could go wrong - e.g., financial, legal, reputational, safety, ethical harm?)	Likelihood (e.g., 1-5 scale)	Impact (e.g., 1-5 scale)	Risk Score (Likelihood x Impact)	Risk Level (High/Medium/Low based on score and your criteria)	Existing Controls / Mitigation Measures (Measures currently in place to modify the risk)	Residual Risk Level (Risk level remaining after existing controls)	Planned Treatment / Action (If needed, outline actions to reduce, avoid, transfer, or accept the risk to reach acceptable risk level)	Owner (Responsible person/team)
AI-001	Algorithmic Bias in Hiring Tool leading to discriminatory outcomes for certain candidate groups	HR Recruitment AI System	Legal challenges; Reputational damage; Loss of trust; Ethical concerns					[Describe any existing bias detection techniques, fairness metrics monitoring, data validation, human review points]		[Plan to conduct a formal bias audit; Implement fairness-aware machine learning techniques; Update training data]	[Assign Owner]
AI-002	Data Poisoning Attack impacting the integrity of the training data for the sentiment analysis model	Customer Feedback Processing AI (Training Data)	Inaccurate sentiment analysis; Misinformed business decisions; Reputational harm; Security breach					[Describe existing data validation checks upon ingestion, access controls for data sources, monitoring for unusual model behavior]		[Plan to implement adversarial training defenses; Enhance monitoring for data anomalies; Review data source security]	[Assign Owner]
AI-003	Lack of Explainability for High-Risk Loan Application AI System making decisions difficult to understand	Financial Loan Approval AI	Inability to justify decisions to applicants or regulators; Legal challenges; Loss of trust; Non-compliance with transparency mandates					[Describe existing logging of features used for prediction; Basic system documentation]		[Plan to implement LIME/SHAP or other post-hoc explainability techniques; Improve system documentation; Train staff on explaining AI outcomes]	[Assign Owner]

How to Use This Template (High-Level):

1. **Define Scope:** Clearly determine which AI systems, processes, or decisions are within the scope of your AIMS.
2. **Identify Risks:** For each scoped AI system/process, brainstorm potential risks using the categories provided and considering your organizational context. Engage relevant stakeholders, including technical teams, compliance officers, legal advisors, and business unit representatives.
3. **Describe & Assess:** Briefly describe each identified risk and the affected area. Assess the potential impact and likelihood using a consistent scale (e.g., 1-5 or 1-10). Calculate the initial risk score (Likelihood x Impact) and determine a high-level risk level (High, Medium, Low) based on your organization's criteria.
4. **Document Existing Controls:** Note any measures currently in place that help manage or mitigate the identified risk. Annex A of ISO 42001 provides a list of controls to consider.
5. **Assess Residual Risk:** Based on the effectiveness of existing controls, determine the current risk level remaining (residual risk).
6. **Plan Treatment:** For risks with a residual risk level above your organization's defined risk tolerance, outline planned actions to reduce the risk to an acceptable level.
7. **Assign Ownership:** Assign responsibility for each risk and the implementation of planned actions to specific individuals or teams.
8. **Review & Monitor:** ISO 42001 requires ongoing monitoring, review, and continual improvement of your risk management process. Risk assessments should be performed at planned intervals or when significant changes occur.

This is a starting point. For comprehensive assessments aligned with ISO 42001, work with our certified experts at Dynamic Comply.