



## NIST AI RMF-Based AI Risk Assessment Template

Prepared by Dynamic Comply

---

This template offers a high-level approach to AI risk assessment, aligned with the NIST AI Risk Management Framework (AI RMF) Core Functions: **GOVERN**, **MAP**, **MEASURE**, and **MANAGE**. The AI RMF is a voluntary guide for organizations to manage AI risks and foster trustworthy AI systems throughout their lifecycle.

### 1. Define AI System & Context (MAP Function)

- **System Identification:** Briefly name and describe the AI system being assessed.
- **Use Cases:** Identify the specific tasks or applications of the AI system.
- **Data Used:** Note the primary data inputs.
- **Operating Context:** Describe the environment and conditions of use.
- **Stakeholders & Impacts:** Identify who might be affected and list potential positive/negative consequences.

### 2. Identify Potential Risks (MAP Function)

- List potential risks based on the system, data, context, and stakeholders.
  - *Examples:* Bias, privacy, security, safety, transparency, environmental, ethical, financial.

### 3. Assess & Prioritize Risks (MEASURE & MANAGE Functions)

- For each identified risk, estimate the **likelihood** and **magnitude of impact**.
- Prioritize risks based on assessment (e.g., High, Medium, Low).

### 4. Manage Risks (MANAGE Function)

- **Existing Controls:** Note current safeguards mitigating prioritized risks.
- **Mitigation Actions:** Propose steps to reduce high-priority risks not sufficiently controlled.
- **Action Plan:** Outline who is responsible for proposed actions and by when.

### 5. Monitor & Review (MEASURE Function)

- Plan how risks and control effectiveness will be monitored over time.
- Schedule periodic reviews of this risk assessment.

## 6. Connect to Governance (GOVERN Function)

- Briefly document how this assessment aligns with overall organizational AI policies and accountability.

\*Use this as a baseline. For in-depth risk management and system validation, contact Dynamic Comply.\*