NIST AI Risk Management Framework Core Functions Guide

Type: Framework Guide

Target Audience: Risk Managers, AI Program Leads, Compliance Teams

The NIST AI Risk Management Framework provides a flexible, four-stage lifecycle approach for managing AI risks and promoting trustworthy AI. This guide details each core function and its key activities.

1. GOVERN

Purpose: Establish culture, policies, and accountability for AI risk management

Key Activities

- ☐ Define organizational risk tolerance for AI
- ☐ Assign roles and responsibilities for AI governance
- ☐ Establish AI policies and procedures
- ☐ Ensure leadership commitment and accountability
- ☐ Create documentation requirements
- ☐ Set up AI ethics training programs
- ☐ Establish third-party AI vendor policies

Outcome: Foundation for systematic AI risk management across the organization

2. MAP

Purpose: Understand context, stakeholders, and risks for each AI system

Key Activities

- ☐ Inventory all AI systems in use or development
- ☐ Identify all stakeholders affected by AI systems
- ☐ Document intended purposes for each system
- ☐ Catalog potential misuses and failure modes
- ☐ Assess operational context and deployment environment
- ☐ Map data flows and dependencies
- ☐ Identify regulatory requirements by jurisdiction

Outcome: Clear picture of AI landscape, exposure, and risk surface

3. MEASURE

Purpose: Test for bias, security vulnerabilities, and performance issues

Key Activities

- ☐ Conduct quantitative testing (accuracy, precision, recall)
- ☐ Perform qualitative assessment (stakeholder feedback)
- ☐ Execute security vulnerability testing
- ☐ Implement performance monitoring
- ☐ Conduct bias detection across demographic groups
- ☐ Perform robustness and adversarial testing
- ☐ Test explainability and interpretability

Outcome: Evidence-based risk assessment with quantified metrics

4. MANAGE

Purpose: Prioritize and implement risk treatments and mitigations

Key Activities

- ☐ Prioritize identified risks by severity and likelihood
- ☐ Select treatment options (avoid, mitigate, transfer, accept)
- ☐ Implement controls and safeguards
- ☐ Monitor control effectiveness
- ☐ Document risk decisions and rationale
- ☐ Iterate and continuously improve
- ☐ Report to stakeholders on risk status

Outcome: Active risk reduction with documented treatment decisions

Framework Integration Points

Framework	Integration with NIST AI RMF
EU AI Act	GOVERN/MAP fulfills risk management (Art. 9); MEASURE supports accuracy/robustness (Art. 15)
ISO/IEC 42001	Aligns with AI management system clauses; GOVERN maps to leadership requirements
ISO 27001	MANAGE integrates with information security controls; shared risk assessment approach
GDPR	MAP supports data flow documentation; MEASURE includes privacy impact assessment

Implementation Status Tracker

Function	Status	Owner	Target Date
GOVERN	[ ] Not Started [ ] In Progress [ ] Complete		
MAP	[ ] Not Started [ ] In Progress [ ] Complete		
MEASURE	[ ] Not Started [ ] In Progress [ ] Complete		
MANAGE	[ ] Not Started [ ] In Progress [ ] Complete		

Organization: _____

Reviewed By: _____ **Date:** _____