AI Governance Framework

Based on NIST AI Risk Management Framework 1.0

Framework Overview

The NIST AI Risk Management Framework (AI RMF 1.0) provides a voluntary, flexible framework for managing AI risks. Published in January 2023, it is referenced by NCUA as authoritative guidance for credit unions evaluating, implementing, and managing AI technologies.

Source: NIST AI 100-1 (January 2023); NCUA AI Resource Center (August 2025)

The Four Core Functions

1. GOVERN - Establish Risk Culture & Accountability

The GOVERN function is cross-cutting and enables all other functions. It establishes the organizational culture, structures, and processes for AI risk management.

Key Actions:

- Establish board-level oversight and accountability for AI initiatives
- Define AI risk appetite aligned with credit union's mission and values
- Create cross-functional AI governance committee (IT, Risk, Compliance, Operations)
- Develop AI-specific policies addressing data privacy, consent, and explainability
- Allocate resources for AI risk management activities
- Establish incident response procedures for AI-related events

2. MAP - Contextualize and Identify Risks

The MAP function establishes context to frame risks to AI systems. It enables identification of risks and risk-contributing factors.

Key Actions:

- Inventory all AI use cases (both sanctioned and shadow AI)
- Identify data inputs, outputs, and member touchpoints
- Document third-party AI vendors and their access to member data
- Assess potential harms: financial, reputational, member trust, regulatory
- Map AI systems to applicable regulations (GLBA, FCRA, ECOA, state laws)
- Identify high-risk use cases requiring enhanced controls

3. MEASURE - Assess and Analyze Risks

The MEASURE function employs quantitative, qualitative, or mixed-method tools to analyze and assess AI risks.

Key Actions:

- Establish metrics for AI system performance and fairness
- Conduct bias testing for credit decisions and member services
- Perform adversarial testing and red team exercises
- Measure model drift and accuracy degradation over time

- Assess security vulnerabilities (prompt injection, data poisoning)
- Document measurement methodologies and results

4. MANAGE - Implement Risk Response

The MANAGE function operationalizes risk response strategies through continuous monitoring and improvement.

Key Actions:

- Implement controls based on risk assessments
- Deploy continuous monitoring for AI system behavior
- Maintain human oversight for high-stakes decisions
- Create audit trails for AI-assisted decisions affecting members
- Establish feedback loops for continuous improvement
- Regularly test and update incident response procedures

Characteristics of Trustworthy AI

NIST identifies these characteristics as essential for trustworthy AI systems:

Characteristic	Credit Union Application
Valid & Reliable	AI systems produce accurate, consistent results across member populations
Safe & Secure	Member data is protected; systems resist manipulation and attacks
Fair (Bias-Free)	Credit decisions and services are equitable across demographic groups
Accountable & Transparent	Clear ownership of AI decisions; members informed when AI is used
Explainable	AI decisions can be explained to members and regulators
Privacy-Enhanced	Data minimization; consent obtained; GLBA compliance maintained

Implementation Roadmap

Phase 1: Foundation (Months 1-3)

- Establish AI governance committee with executive sponsorship
- Conduct comprehensive AI inventory (including shadow AI)
- Develop initial AI acceptable use policy
- Train leadership on AI risks and opportunities

Phase 2: Implementation (Months 4-9)

- Deploy technical controls (DLP, network monitoring)
- Implement vendor due diligence program for AI providers
- Establish approved AI tools with enterprise controls
- Roll out employee training program

Phase 3: Maturity (Months 10-12+)

- Implement continuous monitoring and metrics
- Conduct regular risk assessments and audits
- Establish AI model risk management program
- Integrate AI governance into enterprise risk framework

Framework Source: NIST AI Risk Management Framework 1.0 (AI 100-1), January 2023. Available at: nist.gov/itl/ai-risk-management-framework