

NIST AI RMF v1.0

NIST AI RMF helps organizations identify, assess, and manage AI-related risks to promote trustworthy, secure, and privacy-respecting AI.



What it is

NIST AI Risk Management Framework (AI RMF) v1.0 is a risk management framework that assists organizations in identifying, assessing, and managing risks associated with the design, development, deployment, and use of artificial intelligence (AI) systems. Its primary purpose is to promote trustworthy and responsible AI while addressing cybersecurity, privacy, and broader risk considerations across organizational contexts.

Developed and published by the National Institute of Standards and Technology (NIST), the AI RMF is intended for organizations of all sizes and sectors involved with AI technologies. The framework is used by risk managers, technology leaders, compliance teams, and developers to govern AI risks alongside established frameworks like NIST CSF and NIST SP 800-53. It covers issues such as transparency, accountability, data protection, and the integration of security controls within AI workflows.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION NIST AI RMF v1.0
EFFECTIVE January 26, 2023	DOMAIN Risk Management	FAMILY NIST Frameworks
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.nist.gov/itl/ai-risk-management-framework>

Why it matters

- **Strengthen AI risk governance** Improve the oversight of AI development and deployment through structured risk identification, assessment, and mitigation processes.
- **Enhance regulatory preparedness** Support compliance with emerging AI-related laws and standards by aligning risk management practices with recognized national guidance.
- **Promote operational resilience** Enable organizations to maintain critical functions by anticipating, addressing, and recovering from AI-driven incidents or disruptions.
- **Improve transparency and accountability** Foster clear documentation and tracking of AI decision-making processes, supporting stakeholder trust and external audit requirements.

How SmartSuite supports NIST AI RMF v1.0

AI Risk Functions and Ownership

Organize AI risk work by AI RMF functions with clear ownership and cadence.

Use Case and Impact Mapping

Document intended use, affected stakeholders, and impact considerations per use case.

Measurement and Evaluation Evidence

Capture testing results, validation metrics, and monitoring outputs over time.

Mitigation, Approval, and Remediation Tracking

Track mitigations, approvals, residual risk acceptance, and remediation timelines.

Vendor and Model Provider Oversight

Manage third-party AI due diligence, controls, and evidence for sourced models.

AI Risk Program Reporting and Readiness

Report AI risk posture, gaps, and readiness across systems and business areas.

Common framework mappings

Official resources

NIST AI Risk Management Framework (AI RMF) v1.0

Provides a comprehensive framework for managing risks in Artificial Intelligence systems.

nist.gov/itl/ai-risk-management-framework

NIST AI RMF Playbook

Offers guidance for implementing the NIST AI RMF in organizational contexts.

nist.gov/itl/ai-risk-management-framework/ai-rmf-playbook

NIST AI RMF Workshop Sessions

Describes insights and discussions from workshops related to the AI RMF.

nist.gov/itl/ai-risk-management-framework

AI RMF Crosswalk with ISO/IEC Standards

Defines the alignment between AI RMF and relevant international standards.

airc.nist.gov/airmf-resources/crosswalks

Frequently asked questions

What is the NIST AI Risk Management Framework (AI RMF) used for?

The NIST AI RMF helps organizations identify, assess, and manage the risks associated with the design, development, deployment, and use of artificial intelligence systems. It provides structured guidance for fostering trustworthy, accountable, and secure AI within different organizational and regulatory contexts.

Is the NIST AI RMF required or certifiable?

The NIST AI RMF is a voluntary guidance framework and does not currently have a formal certification process or mandate. Organizations may choose to implement the AI RMF to align with industry best practices, meet regulatory expectations, or support internal risk management objectives.

What organizations or systems does the AI RMF apply to?

The AI RMF applies to any organization designing, developing, deploying, or using AI systems, regardless of size or sector. Its guidance is relevant to risk managers, compliance teams, developers, and executives involved in AI governance and operational risk.

What are the key concepts and artifacts in the AI RMF?

Core concepts within the framework include the Map, Measure, Manage, and Govern functions, which structure risk management activities across the AI lifecycle. Artifacts may include risk assessments, control mappings, inventories of AI systems, governance policies, and compliance documentation.

How does implementation of the NIST AI RMF typically proceed?

Implementation often begins with an inventory of AI systems and related assets, followed by structured risk assessment and mapping of risks to controls and governance policies. Organizations establish roles, oversight mechanisms, and ongoing monitoring practices to manage residual risk.

How does the NIST AI RMF relate to other frameworks like NIST CSF or NIST SP 800-53?

The AI RMF is designed to complement existing risk management and cybersecurity frameworks, such as the NIST Cybersecurity Framework and NIST SP 800-53. It references these frameworks when aligning AI risk controls and governance with broader organizational security and compliance strategies.

What are the ongoing compliance requirements for AI RMF?

Ongoing requirements include continuous risk monitoring, periodic reassessment of AI systems and controls, routine compliance checks, incident response planning, and regular updates to documentation. Teams must demonstrate due diligence in managing AI-related risks over time.

How would SmartSuite support NIST AI RMF?

SmartSuite supports NIST AI RMF by enabling organizations to track risks, manage AI-specific controls, and link assets to policies and governance profiles. It facilitates evidence collection, compliance monitoring, remediation management, and audit readiness with configurable dashboards and reporting tools, ensuring organizations can meet regulatory and framework requirements efficiently.

License included / downloadable: Yes The NIST AI Risk Management Framework is publicly available through official NIST publications.

Full framework page and mappings: smartsuite.com/frameworks/nist-ai-risk-management-framework-ai-rmf-v1-0