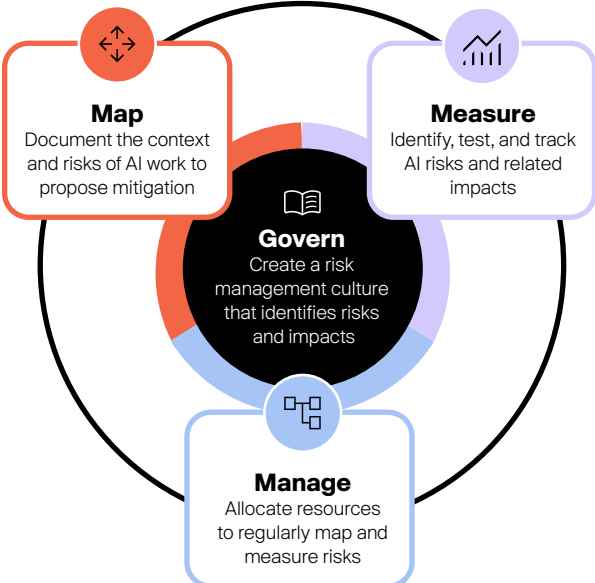# Adopting the NIST AI Risk Management Framework to ensure safety and compliance

Mitigating AI risks with the NIST RMF

Managing risks is critical to delivering missions in an ethical, responsible and safe way, so that AI is used for intended aims and aligns with your organization's values. Adopting the National Institute of Standards and Technology's (NIST) voluntary AI Risk Management Framework (RMF) guidelines can promote AI risk mitigation best practices and help AI actors like risk management professionals, contractors, and AI builders map, measure, manage, and govern risks posed throughout the end-to-end AI lifecycle.
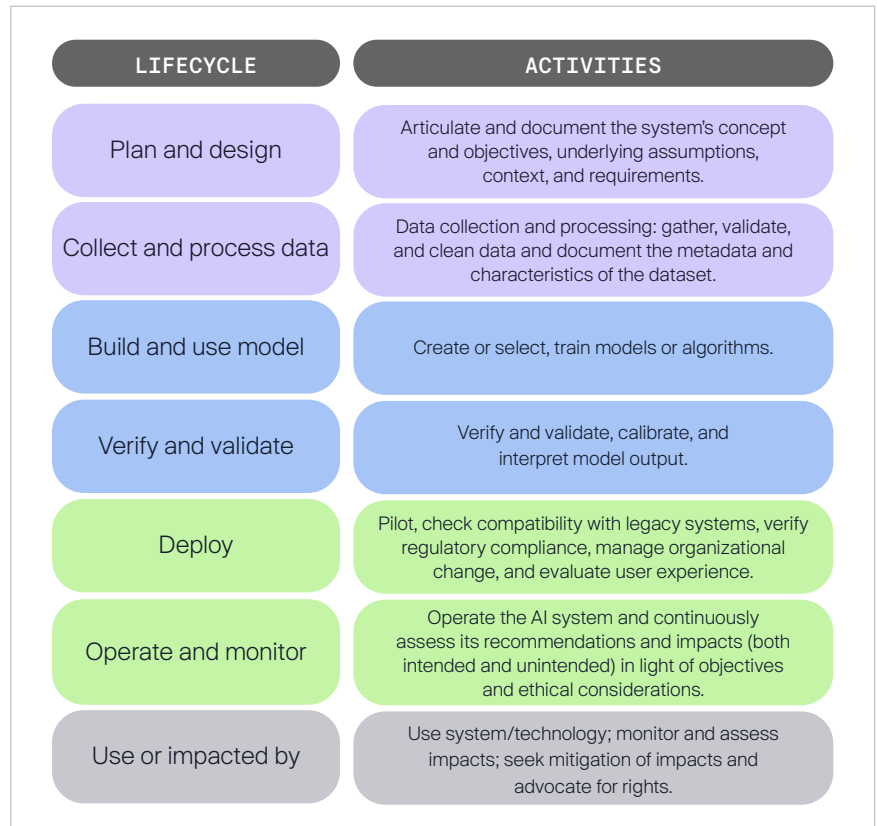
The AI RMF Core defines outcomes and actions to promote understanding of risk management activities across four core functions: map, measure, manage, and govern.

Learn more about adopting the NIST AI RMF with Domino

Map
Document the context and risks of AI work to propose mitigation

Measure
Identify, test, and track AI risks and related impacts

Govern
Create a risk management culture that identifies risks and impacts

Manage
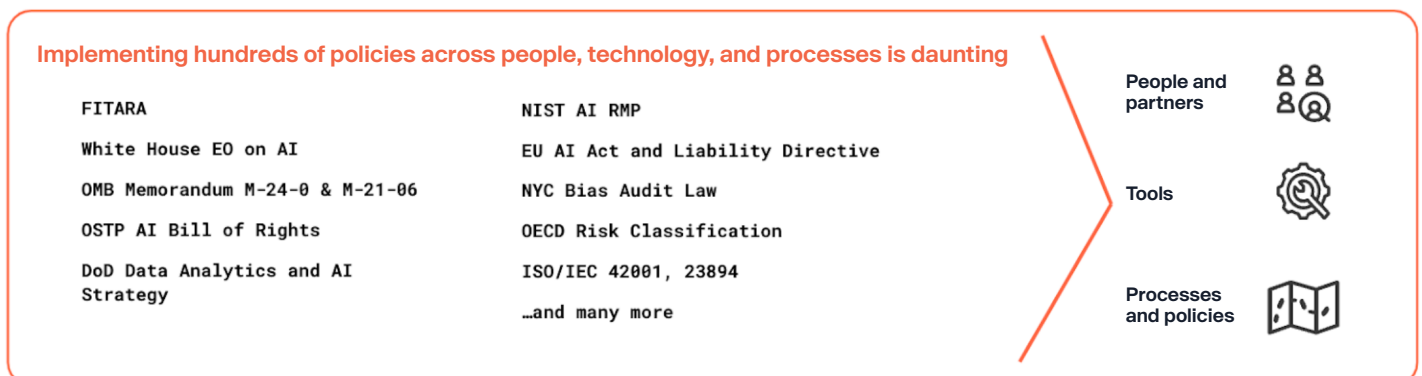Allocate resources to regularly map and measure risks

The NIST AI RMF emphasizes the importance of testing, evaluation, verification, and validation (TEVV) throughout an AI lifecycle and it defines the general operational context for an AI system and defines trustworthy AI.

LIFECYCLE	ACTIVITIES
Plan and design	Articulate and document the system's concept and objectives, underlying assumptions, context, and requirements.
Collect and process data	Data collection and processing: gather, validate, and clean data and document the metadata and characteristics of the dataset.
Build and use model	Create or select, train models or algorithms.
Verify and validate	Verify and validate, calibrate, and interpret model output.
Deploy	Pilot, check compatibility with legacy systems, verify regulatory compliance, manage organizational change, and evaluate user experience.
Operate and monitor	Operate the AI system and continuously assess its recommendations and impacts (both intended and unintended) in light of objectives and ethical considerations.
Use or impacted by	Use system/technology; monitor and assess impacts; seek mitigation of impacts and advocate for rights.

Source: NIST

Why institute the NIST RMF?

AI governance challenges and new threats keep evolving, including data security and privacy threats, risks from inadequate testing of AI models and practices, emerging new technologies like GenAI, and inefficient annual review processes that leave risk "landmines" uninspected.

Implementing hundreds of policies across people, technology, and processes is daunting

```
FITARA                          NIST AI RMP
White House EO on AI            EU AI Act and Liability Directive
OMB Memorandum M-24-0 & M-21-06 NYC Bias Audit Law
OSTP AI Bill of Rights          OECD Risk Classification
DoD Data Analytics and AI       ISO/IEC 42001, 23894
Strategy
                                …and many more
```

People and partners

Tools

Processes and policies

Lastly, despite growing incidents and emerging regulations, most government agencies are underprepared for incoming regulations and the pace of AI innovation. The most regulated organizations comply with regulations and responsible AI principles, in a siloed fashion, at great cost, while impeding innovation. For example, 48% of organizations Domino surveyed lack the resources to achieve their AI Governance goals. Source: Domino's REVelate Survey

The NIST AI RMF helps fast-track compliance

The voluntary NIST AI Risk Management Framework provides a process that integrates and involves people, processes and culture, alongside the right technologies (e.g., security, privacy, supply chain, risk management), to minimize unmitigated and unexpected negative AI impacts that can harm missions.

Beyond and before technology can help address NIST framework guidelines, organizations should tailor their NIST adoption approach to match their AI governance maturity. Without the right people and resources in place, NIST cannot be fully operationalized with technology alone. For example, supporting the NIST AI RMF is more challenging for organizations using legacy methods and technologies, such as manually documenting or looking up information in spreadsheets, or disparate systems where AI is not built, monitored or maintained. Manual processes make it costly and inefficient to inspect new technologies like GenAI, which can operate as "black boxes." And as AI models become more advanced, technology is needed to monitor data quality across the spectrum of data sources and users, as is ongoing model monitoring, to ensure small inaccuracies do not impact downstream decisions, risks, and compliance.

How Domino helps support the NIST RMF

From a technology standpoint, Domino Governance helps AI builders and reviewers build, operate and govern the end-to-end AI/ML lifecycle. Domino streamlines and automates the process of collecting, reviewing, and tracking all materials to enforce compliance with any policy — now and in the future. That is how Domino delivers out-of-the-box governance that is both universal and customizable for agencies — simplifying compliance today and tomorrow with one system of record.

FOR RISK MANAGERS AND COMPLIANCE MANAGERS

Model inventory and lifecycle management: Domino Governance provides a centralized repository and universal system of record for comprehensive model cataloging, offering visibility into model lineage, dependencies, and recording-keeping across all AI activities. This feature is fundamental to effective risk mitigation across an agency's AI projects, users, data, models, and use cases.

Automated evidence generation: Domino Governance automatically generates evidence for compliance and reproducibility, by versioning model metadata, code changes, data lineage and more. By automatically creating a comprehensive audit trail of model development and validation, Domino reduces the time and costs of reviews and audits.

Centralized policy management and visibility: Domino Governance centralizes all policies and evidence of policy adoption in one place, for a single source of truth for all model-related policies like NIST RMF and others. This ensures accuracy and consistency for auditors and regulators.

FOR DATA SCIENCE AND ANALYTICS LEADERS

Policy compliance risk identification and management: Domino Governance ensures policy adherence through simple to use templates and checklists, embedded where AI builders already work — reducing friction and saving time. Model monitoring is built-in, policies are automatically enforced using scripts, and builders are notified when model drift, divergence, and data quality checks exceed thresholds.

Comprehensive view for accelerated approvals: Domino Governance offers a 360°, holistic view of all responsible AI policies, artifacts, and the context of work — supporting your NIST RMF aligned practice. Domino's solution accelerates these processes by providing reviewers with all necessary information in one place, enabling faster decision-making while maintaining thorough oversight.

Frictionless collaboration: Domino Governance allows reviewers, risk managers, and data scientists to seamlessly share artifacts with the context behind work. And smart automation notifies the right people, at the right time and asks for action, for frictionless collaboration.

Starting the NIST RMF journey

Domino's Governance solution is embedded where AI builders work, with pre-built templates and checklists and scripts that automate adoption and enforcement of NIST AI RMF principles across the AI lifecycle.

Domino has also transformed the NIST RMF into a practical resource to help agencies begin the process of adopting proper controls and policies across the AI lifecycle to prevent AI systems from perpetuating inequity, mistrust, and undesirable outcomes.

Conclusion

Mapping, measuring, and monitoring AI risks helps ensure mission-critical, AI-driven work is governed. The NIST Risk Management Framework provides a process and risk-based approach to achieving ethical, safe and compliant AI.

About Domino Data Lab

Domino Data Lab empowers the largest AI-driven enterprises to build and operate AI at scale. Domino's Enterprise AI Platform unifies the flexibility AI teams want with the visibility and control the enterprise requires. Domino enables a repeatable and agile ML lifecycle for faster, responsible AI impact with lower costs. With Domino, global enterprises can develop better medicines, grow more productive crops, develop more competitive products, and more. Founded in 2013, Domino is backed by Sequoia Capital, Coatue Management, NVIDIA, Snowflake, and other leading investors.

Learn more at **www.domino.ai** →

See how Domino can help you address the NIST AI RMF →

 Domino