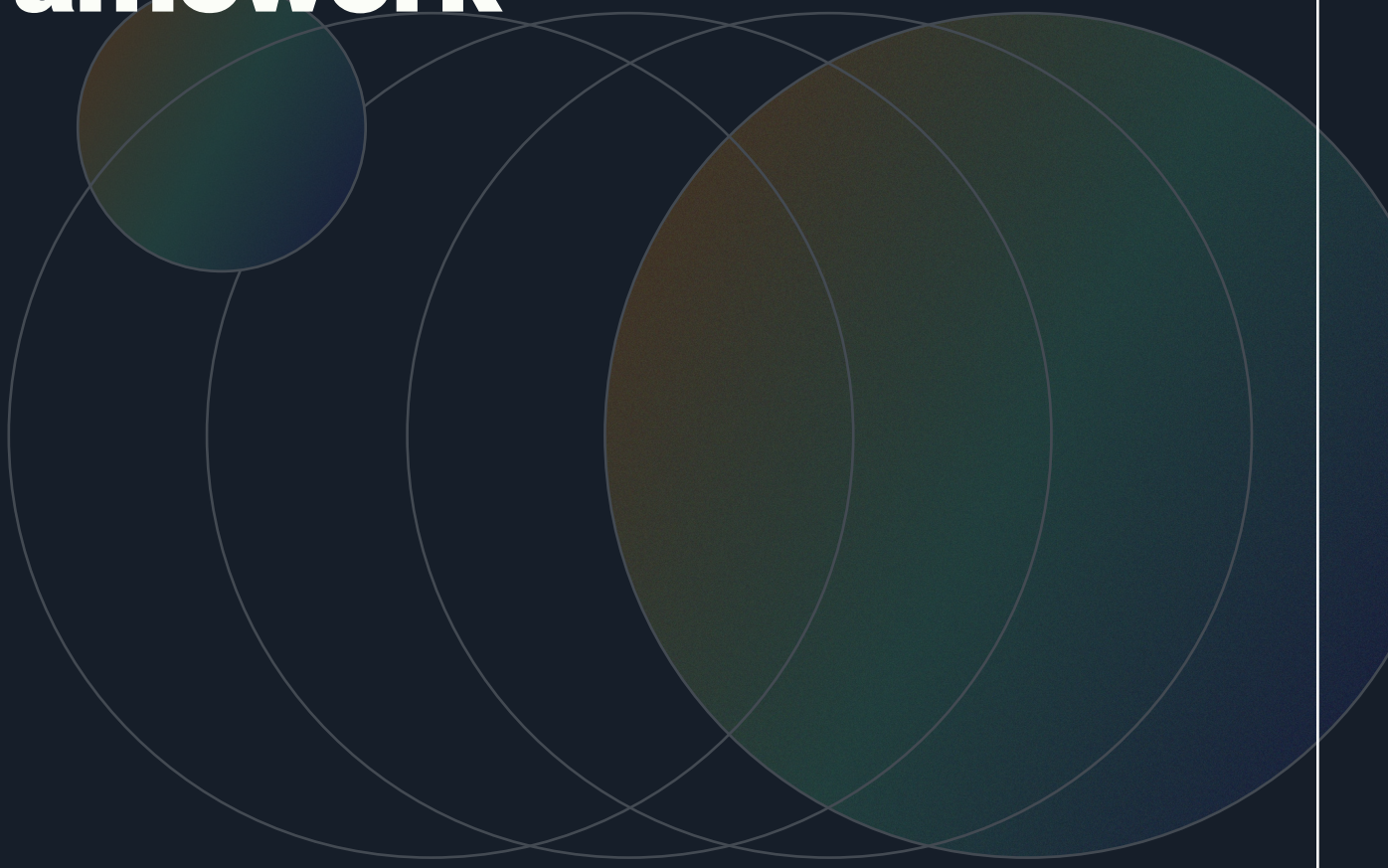
RSI | *Whitepaper*

NIST AI Risk Management Framework

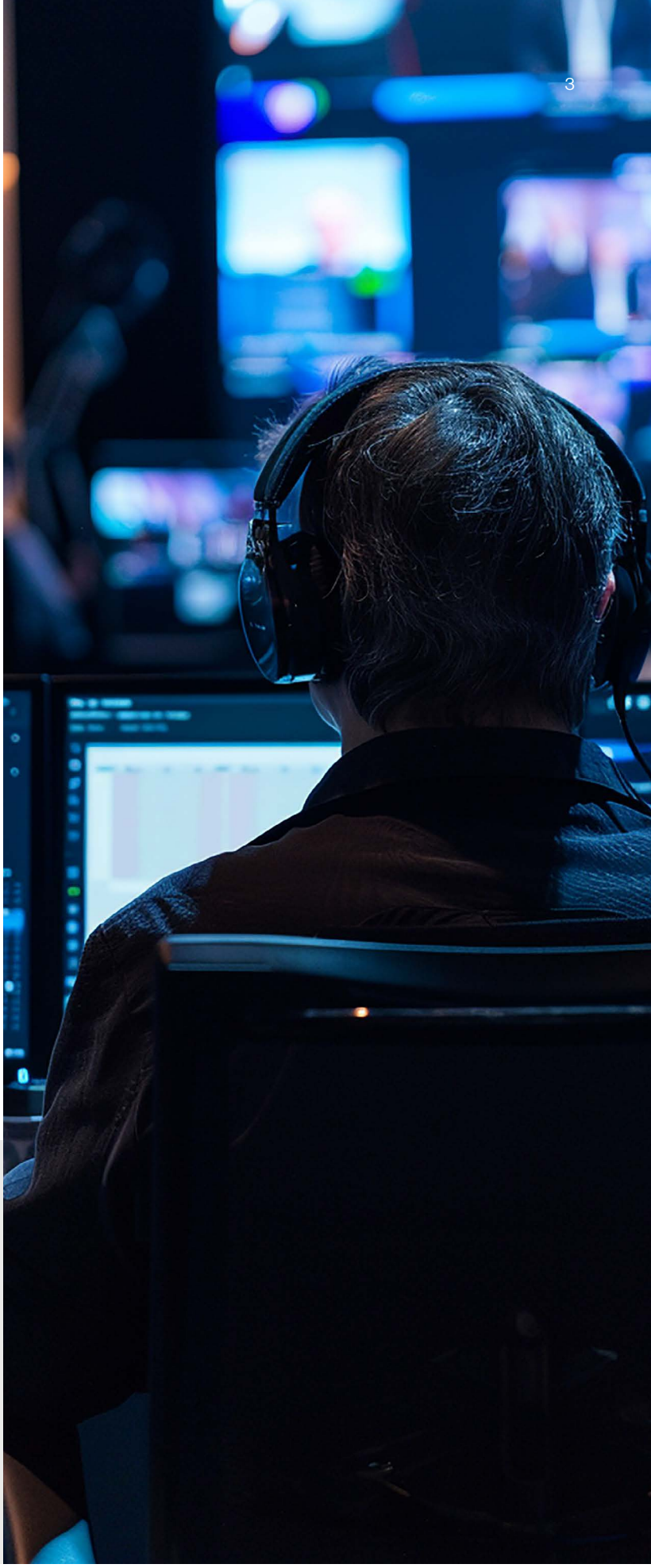


858.999.3030 | info@rsisecurity.com
2025

Introduction of the NIST AI RMF

AI has revolutionized industries with new opportunities for automation, data analysis, and content generation. However, these capabilities bring unique risks, especially regarding data privacy, security, and fairness. Governments have developed guidelines, such as the NIST AI RMF, to help organizations safely harness AI. Published in 2023, this framework helps manage AI-related risks through assessments and governance. Despite its value, the complexity of the NIST AI RMF poses challenges for many businesses in understanding its requirements and implementing compliant AI governance.

This whitepaper intends to educate stakeholders in finance, healthcare, government, and other impacted industries about what this new NIST cybersecurity framework means for them and how they can stay compliant and secure by implementing AI risk management. In it, we provide an overview of the regulatory context leading up to the new NIST framework's publication, an explanation of its requirements, and guidance on long-term compliance.

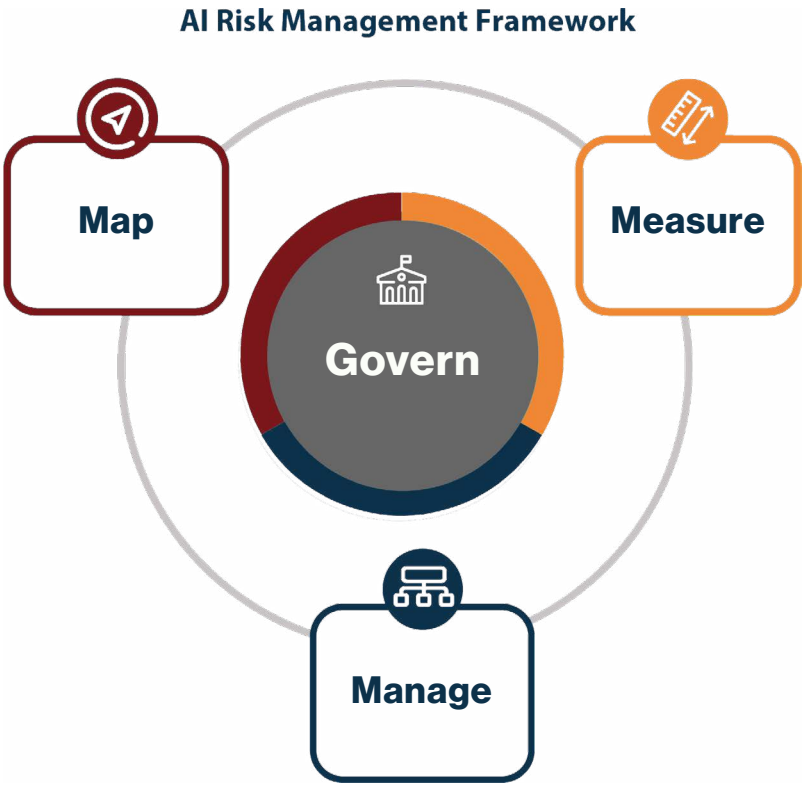


Understanding the NIST AI Risk Management Framework

The NIST AI Risk Management Framework (AI RMF) is a voluntary set of best practices aimed at mitigating risks associated with AI and machine learning development. While not legally required, the framework is highly recommended for industries facing regulatory pressures or dealing with clients, particularly in the public sector, who may expect compliance. The AI RMF is structured around four core functions—Govern, Map, Measure, and Manage—that collectively help organizations ensure the safety, fairness, and effectiveness of AI systems.

1 Govern

The Govern function of the NIST AI RMF outlines the essential policies, processes, and responsibilities for managing AI risk. It focuses on creating a top-down structure that ensures AI risk management is effectively established and overseen. This function provides the framework for coordinating resources and setting the foundation for the other functions—Map, Measure, and Manage—by defining governance logistics and oversight mechanisms.



2 Map

The Map function of the NIST AI RMF focuses on identifying and understanding AI risks. It translates policies into actionable practices, builds consensus on the AI ecosystem, and assigns stakeholder responsibilities. This function lays the groundwork for measuring and managing AI risks effectively within a well-governed framework.

3 Measure

The Measure function focuses on establishing performance metrics for AI systems, based on goals set in the Map function. It sets standards for testing, evaluation, validation, and verification (TEVV) to ensure that assessment data is accurate and useful. These controls guide the adjustment of AI systems, supporting governance and management efforts.

4 Manage

The Manage function focuses on implementing risk controls and mitigation strategies. It ensures that the protections outlined in the Govern, Map, and Measure functions are put into practice. This includes prioritizing risks, managing third-party risks, and developing incident response and recovery plans to maintain system integrity and security.

RSI Security's NIST AI RMF Services

- Gathering key documents and identifying AI tools, risks, and necessary controls.
- Conducting a gap analysis, developing a risk management plan, and implementing NIST AI RMF controls.
- Training stakeholders on AI risks and compliance requirements.
- Delivering a detailed report with compliance recommendations and guidance on emerging AI governance frameworks.

Key Components of NIST AI Risk Management Advisory

1 Preparatory and Gap Analysis

Advisors assess AI systems and their broader tech ecosystem to identify security, ethical, and legal risks. They analyze infrastructure, compare existing controls to NIST AI RMF requirements, and determine necessary security solutions.

2 Framework Development

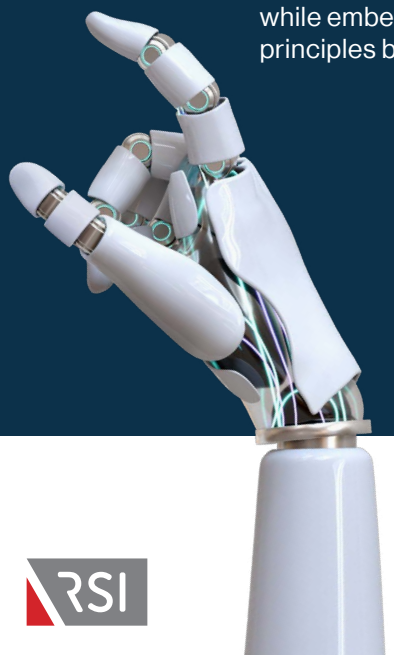
Advisors develop a customized control framework to meet NIST AI RMF requirements efficiently. They tailor 10-25 key controls to address your specific risks, ensuring streamlined implementation and long-term management.

3 Regulatory Compliance Support

Your advisor ensures compliance with NIST AI RMF while also preparing for future AI regulations. They design adaptable controls that meet current standards and can evolve with industry, regional, and client requirements.

4 Ongoing Risk Management

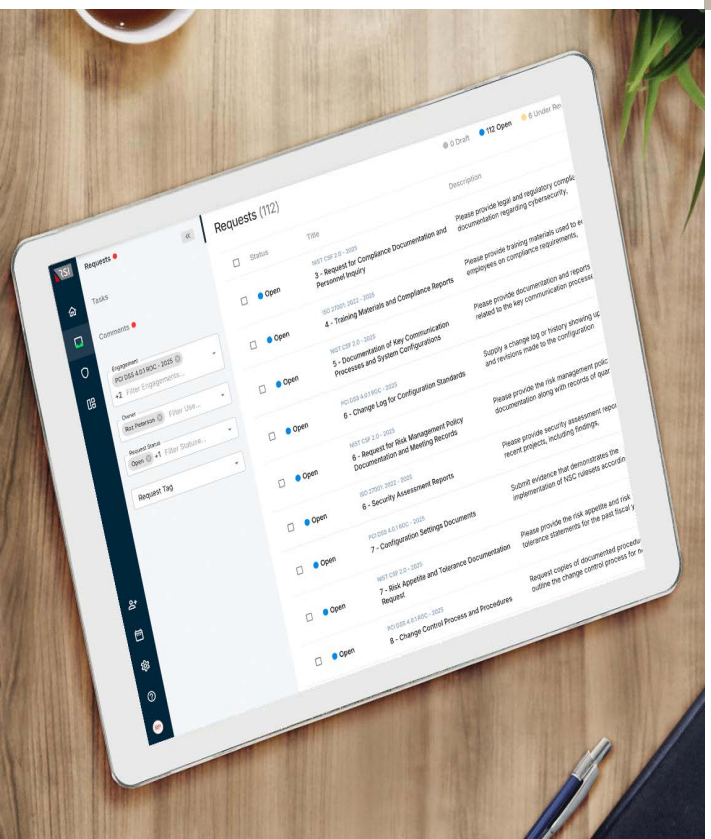
Your advisor develops scalable controls and best practices for continuous monitoring and risk management. Effective implementation enhances visibility, flexibility, and accountability while embedding transparency and ethical principles by design.



RSI Security's GRC Tool: Your NIST AI RMF Management Solution

RSI Security's GRC Tool empowers seamless implementation of NIST AI RMF, along with all other governance, risk, and compliance (GRC) needs. Highlights of the platform include:

- Pre-built templates for NIST AI RMF and other common frameworks like SOC 2, ISO, CMMC, and NIST.
- Automations for repetitive and time-consuming tasks such as data gathering, documentation, and reporting.
- Step-by-step verification for every NIST AI RMF requirement.
- Integrations with popular tools like Slack, G Suite, and Microsoft 365 for seamless communication and data flow.
- Real-time collaboration with team members and clients.
- Intuitive dashboards and comprehensive reporting for tracking, assessing, and mitigating risk.



Achieve NIST AI RMF Compliance Today

RSI Security will jump-start your NIST AI RMF compliance process with a free consultation. Our experts provide insights on how ready you are for NIST AI RMF implementation, what specific controls need to be installed, and what benefits you can expect from NIST AI RMF compliance.

To learn more about RSI Security's NIST AI RMF services, get in touch today!