

# NIST AI RMF ASSESSMENT

As AI becomes central to medium-sized enterprise (MSE) innovation, organizations must ensure systems are trustworthy, transparent, and aligned with ethical and regulatory expectations.

While MSEs are uniquely positioned to leverage their agility and flexibility to implement advanced AI-based technologies for competitive gains and operational efficiency, limited resources, expertise, and organizational readiness can pose significant barriers.

**MORE THAN 60% OF MSEs ARE ACTIVELY EXPLORING AI TECHNOLOGIES, YET ONLY ABOUT 1% CONSIDER THEMSELVES MATURE IN TERMS OF FULLY INTEGRATING AI INTO THEIR WORKFLOWS.**

## RISK IDENTIFICATION, ASSESSMENT, AND MITIGATION

The National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF) provides a structured approach to managing AI risks.

**Avertium's NIST AI RMF Assessment service helps organizations to confidently align their unique needs with the framework's best practices.**

Whether developing AI in-house, using or integrating third-party models, or scaling AI across business units, our expert-led assessment provides a clear path to responsible and secure AI adoption:

- Enable secure innovation balanced with business productivity
- Reduce risk exposure
- Build stakeholder trust
- Integrate smoothly with business operations and meet compliance
- Understand foundational requirements and needed remediation

## INDUSTRY AND COMPLIANCE FOCUS

A growing number of compliance regulations require proof of secure and responsible AI adoption and use, especially in sectors handling sensitive data or high-risk applications:

- ✓ Healthcare
- ✓ Telecommunications

- ✓ Manufacturing
- ✓ Finance

- ✓ Retail
- ✓ Government Contracts

Organizations in these increasingly AI-reliant industries that face high regulatory, ethical, or operational risk can benefit from this assessment:

- Align AI-specific risks with enterprise-wide risk management strategies
- Understand how to define roles, responsibilities, and accountability
- Proactively demonstrate AI risk management to regulators and stakeholders
- Gain customer trust and competitive market advantage

## WHAT YOU GAIN

Avertium provides a clear path to responsible and secure AI adoption by identifying compliance gaps and recommending remediation steps. We take a comprehensive and programmatic approach, tailored to each customer's needs:

### ACCESS TO EXPERTISE

- » **Experience:** Deep expertise in applying NIST principles across diverse environments to scale security programs, protect sensitive data, and serve core business objectives.
- » **Consultative Approach:** Clear and collaborative communication across technical and non-technical teams to convey the critical role of data security and compliance within the context of the business, facilitating AI adoption.

### SECURE INNOVATION FOR COMPETITIVE ADVANTAGE

- » **Trustworthy AI:** Detailed understanding of how to implement AI with fairness, transparency, privacy, and accountability to foster trust with users, customers, and regulators.
- » **Strategic Edge:** Means to enable automation, free up human talent for strategic work and reduce operational costs through enhanced efficiency, innovation and decision-making.

### MATURE MODELING

- » **Maturity Rating:** Avertium goes further to assess your AI adoption and implementation maturity using the NIST implementation tiering model, providing a rating of AI compliance maturity based on the NIST framework.
- » **Guided Adoption:** Clear understanding of where you stand so you can prioritize investments, scale AI responsibly, and build external trust and transparency.

## OUR PROCESS

Avertium evaluates the people, processes, and systems across your organization according to the unique controls comprising NIST AI RMF's Govern, Map, Measure, and Manage functional areas:

1. Hold project kickoff and provide access to Avertium's GRC platform
2. Review documentation and conduct stakeholder interviews
3. Provide expert analysis and a detailed report outlining compliance, gaps, and actionable recommendations

# ASSESS. DESIGN. PROTECT.

Avertium's signature Assess, Design, Protect approach adapts to your needs. Discover a flexible, collaborative framework that can be applied at any stage of your security and compliance journey.

## **ASSESS** | *Know where you are and where you're going.*

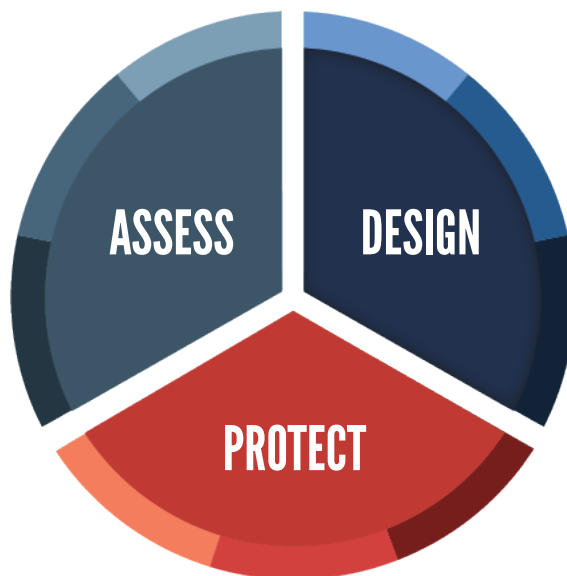
Start with an assessment. Set your goals. Measure the gaps. Then turn insight into action by building a roadmap to success.

## **DESIGN** | *Build a foundation suited for resilience and scale.*

Put the plan in action. Design frameworks and implement programs that adapt, scale, and align to your business needs.

## **PROTECT** | *Reinforce security operations with managed services.*

Extend programs and investments with co-managed threat detection, automated response, and 24/7 coverage.



## RELATED SERVICES

Avertium offers a wide range of associated security and compliance services under a single roof:

1. Policies and procedures (prerequisite)
2. Remediation assistance
3. Microsoft Purview services
4. Data Governance and Compliance program creation

NIST AI RMF Assessment may be combined with other frameworks (e.g. NIST CSF, HIPAA, PCI-DSS) for a comprehensive, efficient, and cost-effective risk review.\*

*\*Assessment interviews must be conducted in tandem to qualify*

## ABOUT AVERTIUM

[Avertium](#) is a cyber fusion and MXDR leader, delivering comprehensive security and compliance services to mid-market and enterprise customers. Our unique “Assess, Design, Protect” methodology addresses and improves security strategy, reduces attack surface risk, strengthens compliance, and provides continuous threat protection. Avertium maximizes customer security investments and enables customers to focus on growth, innovation, and business outcomes, while assuring that their security infrastructure is resilient and adaptive to evolving threats. That's why customers trust Avertium to deliver better security, improved compliance, and greater ROI.