NIST AI Risk Management Framework

LIMRA and LOMA AI Industry Group

LIMRA LOMA

Navigate With Confidence

The NIST AI RMF Summarized

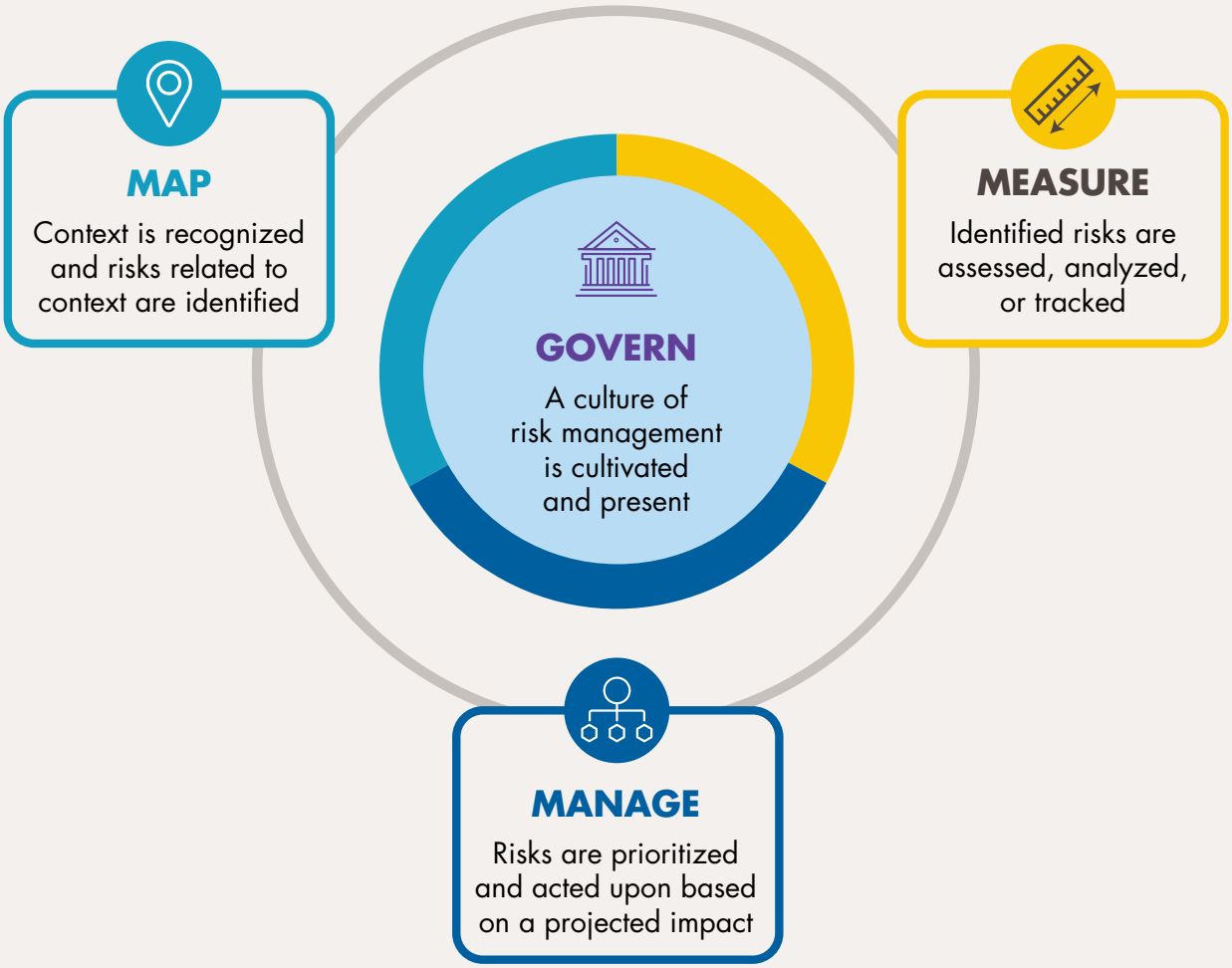
The NIST AI Risk Management Framework (RMF) provides a voluntary, flexible, and rights-preserving structure for understanding and addressing the full lifecycle of AI risks, from design through deployment and monitoring, while promoting trustworthy and explainable AI. The key characteristics of trustworthy AI according to the RMF is that AI should be:

- Valid and reliable
- Safe
- Secure
- Explainable
- Privacy-enhanced
- Fair
- Accountable

Kartik Sakthivel, Ph.D., MS-IT/MS-CS, MBA, PGC-IQ
Vice President & Chief Information Officer, LIMRA and LOMA
ksakthivel@limra.com

The AI RMF is composed of four core functions — map, measure, manage, and govern — as depicted in the figure below.

While insurers are in varied stages of AI maturity, the NIST AI RMF offers a clear path for integrating risk-aware, compliant, and trustworthy AI into operations. Applying these principles across the value chain, from underwriting and claims to marketing and customer experience, can help ensure that AI enhances rather than undermines the values of fairness, transparency, and long-term trust that define our industry. To better understand the applicability of the NIST RMF, the four core functions of the framework have been contextualized for our industry below.



1. MAP: Contextualize and Identify AI Risks

The purpose of the MAP core function is to comprehend the context of AI development and usage, and to identify associated risks. For instance, within underwriting, MAP would help a firm determine whether AI is being used to assess risk, segment applicants, or automate eligibility decisions. It will also assist in being able to understand pertinent regulatory constraints such as being able to protect against discrimination based on protected classes. In marketing, if AI is used for customer segmentation, MAP would help evaluate risks of socioeconomic profiling, redlining, or exclusion. In claims, MAP would help set context of the use of AI in fraud detection or automated triage and ensure that it is mapped for fairness and transparency. Within customer service, MAP would ensure that conversational AI, such as chatbots and virtual agents, are reviewed for accuracy, escalation protocols, and accessibility. In our industry, to align to the MAP core function, insurers should consider:

1. Identifying high-risk use cases (see AIGG AIRE Framework)
2. Establishing clear goals and use intent, (i.e., is the AI model supporting human decisions, or replacing them?)
3. Assessing which stakeholders (such as regulators, actuaries, compliance) need to be involved early on

2. MEASURE: Analyze and Monitor AI Risks

The purpose of the MEASURE core function is to assess and track performance and risk attributes of AI systems using qualitative and quantitative methods. Within our industry, we would track risk attributes pertinent to things such as bias and fairness by the use of statistical parity, disparate impact ratio, or equalized odds to evaluate underwriting or pricing models. Performance metrics would be used to measure false positives/negatives for claims fraud models, underwriting decisioning, or lapse prediction. Metrics around explainability would evaluate whether agents, underwriters, and customers can understand AI-influenced decisions (this is especially true for adverse action notifications). Privacy measures would be used to monitor data handling compliance (HIPAA, GDPR, CCPA/CPRA). This is particularly important for AI models trained on sensitive information like medical data or behavioral patterns. In our industry, to align to the MEASURE core function, insurers should consider:

1. Establishment of baseline metrics for accuracy, fairness, and explainability by use case
2. Identification of leading indicators of model drift or degraded fairness over time
3. The embedding of measurement checkpoints into the model development and approval lifecycle

3. MANAGE: Address and Minimize AI Risks

The purpose of the MANAGE core function is to implement risk management practices and controls to reduce the likelihood or impact of AI-related harms. Within our industry, we can seek to manage third-party vendor risk by requiring vendors to disclose training data sources, audit trails, and model lineage. We can manage model validation by the formalization of review processes by actuarial, model risk management (MRM), and compliance before deployment. Aligning to the MANAGE core function is also the aspect of change management, wherein firms should ensure that the retraining or tuning of AI models triggers revalidation. This is especially important in dynamic environments like claims or sales. In our industry, to align to the MANAGE core function, insurers should consider:

1. Defining and enforcing escalation protocols for AI anomalies or failures
2. Maintaining inventory of all AI systems, owners, and risk classifications
3. Aligning model documentation with internal audit and regulatory expectations

4. GOVERN: Establish Organizational Structures for Oversight

The purpose of the GOVERN core function is to ensure that AI risk management is supported by governance structures, policies, culture, and accountability mechanisms. Within our industry, we can align to the GOVERN core function by establishment of an AI Governance Committee, which serves as a cross-functional group across the value chain and includes departments such as the business unit, domain experts, IT, legal, compliance, data science, actuarial, etc. to oversee AI projects. For high-risk models, firms should convene ethics or fairness reviews to assess systemic bias or societal impact. Aligning to the GOVERN core function would also encompass development of policy frameworks that include AI-specific policies like acceptable uses of AI, transparency and disclosure requirements, AI-related data usage, and model documentation policies. GOVERN also includes AI training and literacy to ensure that employees understand AI and its risks and use it responsibly. In our industry, to align to the GOVERN core function, insurers should consider:

1. Embedding accountability across business units, not just within IT
2. Providing transparency to regulators and customers about how AI decisions are made
3. Aligning governance efforts with NAIC Model Bulletin expectations for oversight and model review

Trustworthiness Characteristics

Trustworthy AI systems must meet various criteria valued by stakeholders to reduce risks. The NIST RMF outlines characteristics of trustworthy AI, defining these as:

- Valid and reliable
- Safe
- Secure and resilient
- Accountable and transparent
- Explainable and interpretable
- Privacy-enhanced
- Fair with managed bias

The RMF advises the balancing these traits according to the AI system's context is crucial and neglecting any of these can lead to negative consequences. The RMF states that the characteristic *valid and Reliable* is a necessary condition of trustworthiness and is shown as the base for other trustworthy characteristics. *Accountable and transparent* is shown as a vertical box because it relates to all other characteristics.

The grid below provides an illustrative view of how these characteristics relate to our industry.

Trustworthiness Characteristic	Relation
Valid and reliable	Life expectancy models, lapse prediction, and underwriting algorithms must perform consistently across populations.
Safe	Avoid unintended decisions that could misclassify or penalize applicants.
Secure and resilient	Protect against adversarial inputs or model manipulation, such as during claims intake or identity verification.
Explainable	Ensure adverse action notices clearly explain model rationale, especially in underwriting.
Privacy-enhanced	Limit data exposure in sensitive use cases such as health-related underwriting or beneficiary modeling.
Fair	Prevent bias in pricing, eligibility, or marketing practices, particularly against protected classes.
Accountable	Maintain clear ownership, auditability, and mechanisms for review or appeal.

Sources

Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Gebru, T. (2019, January), *Model Cards for Model Reporting*.

NAIC MODEL BULLETIN: USE OF ARTIFICIAL INTELLIGENCE SYSTEMS BY INSURERS, NAIC. (2023, December).

Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST. (2023, January).

Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST. (2024, July).

Advancing the financial services industry by empowering our members with

LIMRA LOMA
Navigate With Confidence

0614-2025