

- CLIENT BRIEFING

Managing AI risk, the *NIST* way

A short read of the NIST AI Risk Management Framework: what it asks of organizations that design, build, deploy or use AI systems, and where a team should start.

doi.org/10.6028/NIST.AI.100-1 · Summary of the 48-page framework

01 / 16

- THE FRAMEWORK

Voluntary, non-sector-specific, and built to be used

2020

DIRECTED BY LAW

Written under the National Artificial Intelligence Initiative Act of 2020 (P.L. 116-283).

7

TRUSTWORTHY AI TRAITS

Part 1 defines seven characteristics a trustworthy AI system should show.

4

CORE FUNCTIONS

Part 2 turns the framework into Govern, Map, Measure and Manage.

Source: NIST AI 100-1, Executive Summary, p. 1-2

02 / 16

- PART 1

Trustworthy AI is *valid and reliable* first,
then safe, secure, accountable, explainable, private and
fair

01

Works as intended

Valid and reliable is the base. Safe, plus secure and resilient, build on it.

02

Can be questioned

Accountable and transparent, explainable and interpretable, privacy-enhanced.

03

Fair, bias managed

Harmful bias is named as a risk to manage, not a box to tick once.

The framework does not prescribe a risk tolerance. Each organization sets its own.

03 / 16

- PART 2 · GOVERN

Govern sits across everything. It shapes how you Map, Measure *and Manage AI risk*

Govern builds a culture of risk management, sets policies and processes, and ties technical work to company values. NIST describes it as cross-cutting, infused through the other three functions.

After Govern is in place, most users start with Map.

- IN PRACTICE

Three functions you run per system

01 → Map the context

Frame the risks of one AI system: its purpose, its users, and who it could affect across the lifecycle.

02 → Measure the risk

Test before deployment and regularly in operation, with quantitative, qualitative or mixed methods.

03 → Manage the response

Put resources on mapped and measured risks, with plans to respond, recover and communicate.



NIST says the process should be iterative, with cross-referencing between functions.

• WHERE TO START

Pick **one** AI system. Run the four functions on it this quarter.

SCOPE

1 system, 4 functions

Choose functions and subcategories that fit your resources.

GOVERN

Name owners, write the risk policy, set your own risk tolerance.

MAP AND MEASURE

Document context and impacts, then test against the seven trustworthy traits.

USE THE PLAYBOOK

The NIST AI RMF Playbook lists suggested actions for each outcome.