

FRAMEWORK ON ONE PAGE · VERSION 1.0

The Authorization Layer

Framework library · July 2026

TIME TO USE 30 min orientation	AUDIENCE Enterprise AI governance practitioners	OUTPUT A framework selection and evidence path
-----------------------------------	--	---

? The operational layers tell you the system is behaving. The authorization layer tells you it was ever allowed to.

What it is

Most AI governance frameworks manage what happens after a system is approved. Each operational layer, covering inventory, data foundation, data security and access, model assurance, human oversight, and compliance and audit, assumes that someone already decided the system was allowed to operate, defined what it was permitted to do, and accepted responsibility for its outputs. That decision is itself a layer, it sits beneath all the others, and in most organizations it was never designed.

The operational layers it sits beneath

AI inventory	What AI systems exist, who owns them, and how risky each one is.
Data foundation	Where the data comes from, whether it is accurate, and whether it carries bias.
Data security and access	Who can reach the data and under what controls.
Model assurance	Whether the model performs, stays fair, and holds up over time.
Human oversight	When a person reviews, escalates, or overrides what the system does.
Compliance and audit	Whether the whole arrangement satisfies the regulators and leaves a trail.

A worked example

Situation	A generic enterprise is selecting which framework artifacts are needed before approving a new agent.
Where it lands	Library path selected
Evidence	The team identifies population, intent, ownership, and review questions before selecting the corresponding framework artifacts.
Gap found	The selected records have not yet been assigned to named owners.
Next action	Assign owners and use the selected artifacts as the intake evidence package.
Output	A framework selection with an evidence path.

The one action it produces

A framework selection and evidence path

What good looks like

An organization can build the full operational stack and still fail the first question a regulator asks. The controls may be strong, but they govern a system no one formally authorized. Authorization comes before the operational layers are running. It is the decision the operational layers exist to enforce. Build it first and every layer above it has something real to govern.

What it cannot establish

This object can orient a practitioner to the library and its artifacts. It cannot perform the underlying assessment or establish authorization without organization-specific evidence.

CITE AS