

CASE STUDY · AI-CASE-2026-001

ARISE Framework™: Three Months, Nine Sectors, One Governance Architecture

Early adoption data from nine industry sectors and six global regions shows why organizations are converging on a common AI assurance language, and how the ARISE Framework™ maps to the EU AI Act, ISO/IEC 42001, NIST AI RMF, and HIPAA at once.

PUBLISHED	April 2026
OBSERVATION	January - April 2026
METHODOLOGY	ARISE Framework™ adoption analysis
CLASSIFICATION	Public

Secure
&
Responsible
Technology.

ENGAGEMENT SNAPSHOT

SUBJECT	OBSERVATION PERIOD	METHODOLOGY	PRIMARY FINDING
Practitioner adoption of the ARISE Framework™ in its first months of public availability.	January – April 2026; findings published April 2026.	Analysis of named-sector practitioner affiliations, engagement depth, and geographic distribution.	Adoption across nine sectors and six global regions; demand for unified AI governance is sector-agnostic and accelerating.

Prepared by Assessed Intelligence. Observation period January – April 2026 · Published April 2026 · Classification: Public. Sector shares describe practitioners with an identified sector affiliation; organizations are referenced by sector rather than by name except where noted.

01 • THE CHALLENGE

Regulatory Fragmentation Without an Assurance Layer

Executive Summary

Within two months of availability, the **ARISE Framework™** attracted practitioners from nine industry sectors and six global regions. That pace of adoption is not incidental. It reflects a convergence already underway in AI governance: organizations across industries, regulatory jurisdictions, and governance maturity levels are reaching the same conclusion simultaneously. Sector-specific compliance frameworks tell organizations *what* must be governed. They do not specify *how* to govern AI systems that generate risk every hour of every day.

The trend line in enterprise AI governance is moving toward unification. The EU AI Act, ISO/IEC 42001, the NIST AI RMF, and a growing body of sector-specific mandates share a common operational gap: they establish obligations at the policy level but leave the assurance mechanisms largely unspecified. Organizations that have tried to close that gap with separate, framework-specific programs are discovering that the overhead is not sustainable. A financial institution cannot operate one governance program for Basel III model risk, a second for EU AI Act conformance, and a third for internal audit requirements. The pressure toward a common assurance language is structural, not aspirational.

What the adoption data shows is not simply that the framework has been adopted across sectors. It shows that the demand for unified AI governance is sector-agnostic, geographically distributed, and accelerating faster than the regulatory mandates that typically drive framework adoption.

The Central Finding

“Regulatory fragmentation is not a barrier. It is the argument for a common assurance

language.”

ARISE FRAMEWORK™ CASE STUDY, APRIL 2026

AI systems that generate risk continuously cannot be governed by frameworks designed for periodic review. Annual audit cycles are insufficient: a misconfigured agent permission can persist for months before detection under traditional review models. Regulatory fragmentation compounds the problem. A healthcare organization subject to HIPAA, the EU AI Act where applicable, and emerging clinical AI guidance cannot run three separate governance programs without significant operational overhead. A financial institution managing model risk under Basel III while preparing for EU AI Act compliance needs a common assurance layer that maps to both without duplicating either.

02 • THE SOLUTION

One Governance Architecture

The **ARISE Framework™**, developed by Assessed Intelligence, was built for exactly this environment. Its seven domains, Govern, Manage, Identify, Protect, Detect, Respond, and Validate, are not compliance categories derived from any single regulation. They are operational assurance functions that map to the requirements embedded within multiple frameworks at once.

ARISE DOMAINS	REGULATORY REQUIREMENT ADDRESSED	FRAMEWORKS
Detect • Validate	Ongoing conformance monitoring and evidence of continued compliance.	EU AI Act
Protect • Respond	Data protection safeguards and incident response obligations.	HIPAA
Identify • Govern	Model inventory, accountability, and risk ownership.	NIST AI RMF • ISO/IEC 42001

Current mappings cover 14 frameworks, 6 criteria, and 8 regulations, and they continue to grow monthly. The mapping is not exhaustive: sector-specific mandates such as NERC CIP for energy, DORA for EU financial services, and emerging healthcare AI frameworks contain additional operational requirements that the framework addresses but has not yet fully mapped.

Nine Sectors, One Architecture

Information Technology, Consulting, and Financial Services are the three largest named-sector cohorts, together accounting for 67 percent of practitioners with an identified sector affiliation. Each sector faces distinct regulatory obligations; each finds operational relevance in the framework for the same reason: AI systems generate risk continuously, and existing compliance frameworks do not specify how to govern that risk at the operational level.

SECTOR	SHARE	GOVERNANCE DRIVER
Information Technology	29%	AI embedded in live infrastructure, including payments technology such as InterSwitch, rather than isolated test environments; university technology programs signal adoption in the pre-professional pipeline.
Consulting	25%	A transferable assurance methodology that maps to each client's regulatory requirements without a custom framework per engagement.
Financial Services	13%	The most complex regulatory profile in the cohort; practitioners are moving from assessment into integration with model risk management programs.
Education	—	Governing AI tools in educational settings while preparing the next generation of practitioners; policy must precede adoption.
Communication Services	—	Regulatory bodies and communications authorities evaluating the framework as reference architecture for the organizations they regulate.
Health Care	—	Clinical decision support, diagnostic imaging, and patient data, where model failure has direct patient-safety implications.
Energy	—	AI-assisted grid management at the intersection of operational technology governance and AI risk.
Manufacturing	—	AI in quality control, supply chain, and worker safety, where an inventory of deployments must come before controls.
Utilities, Materials & Real Estate	—	Sectors historically outside AI governance discourse now applying structured assurance to their deployments.

Patterns That Distinguish Application from Awareness

- **Sustained Multi-Session Engagement:** A significant share of practitioners returned for multiple sessions, indicating active application rather than one-time awareness scanning. Engagement is most concentrated in consulting, where practitioners reference the framework repeatedly during client work.
- **Regulatory Authority Participation:** Government regulatory bodies are engaging with the framework as potential reference architecture for the standards they will impose. That signal precedes formal adoption and represents an earlier, more durable form of institutional uptake than standards-body channels.
- **University and Research Adoption:** The framework has already been incorporated into curriculum at multiple academic institutions. Health informatics representation is notable given that clinical AI governance is a fast-growing academic discipline.
- **Governance Multipliers:** A consulting practitioner applies the framework across many client organizations; a financial services practitioner extends it into the institutions their model risk program governs. Adoption is propagating through advisory and institutional networks rather than top-down mandates.

Adoption Without Geographic Constraint

Verified practitioner organizations span the United States, the United Kingdom, Nigeria, Kenya, Ethiopia, Algeria, Ghana, Malaysia, the Philippines, Indonesia, Bangladesh, Pakistan, Germany, the Netherlands, Chile, Argentina, and Nepal. The framework is being applied simultaneously under the EU AI Act, emerging African AI policy frameworks, APAC data governance regimes, and US sector-specific regulation.

The spread also reflects different maturity stages. Practitioners in established regulatory environments, such as EU member states preparing for AI Act obligations, engage with the domains that address conformance monitoring and audit readiness. Practitioners in markets where AI regulation is nascent engage with Govern and Identify as foundational architecture rather than as compliance requirements. The framework accommodates both without separate configurations.

03 • IMPLICATIONS

Implications

- **Regulators Are Watching First:** Regulatory authority practitioners are evaluating the framework as reference architecture for standards they will impose on others. That signal precedes formal regulatory adoption and carries more weight than general practitioner interest.
- **Advisory Networks Multiply Reach:** Consulting density means each adopting practitioner represents multiple client governance engagements, so the framework spreads through advisory networks rather than one organization at a time.
- **The Pipeline Is Already Learning It:** Academic engagement shows ARISE literacy entering the practitioner pipeline before regulatory pressure requires it.
- **A Common Governance Language:** Compliance frameworks specify what must be governed but not how to govern it continuously. The **ARISE Framework™** provides the operational assurance layer that closes that gap across regulatory environments, not instead of them.

NEXT STEP

Put the ARISE Framework™ to work for your organization.

Every engagement starts with an honest picture of where you stand. Our advisors map your environment against the ARISE Framework and build the path to governance that holds up under scrutiny.

Speak with an Advisor → assessedintelligence.com/contact

The ARISE name and symbol are registered trademarks of Assessed Intelligence. Third-party use requires written license.