

ODA3 INSTITUTE

ADOPTION GUIDE

Which GAISSF Ecosystem Framework Do I Need?

Doc ID: ODA3-2026-08-WHP-COM-007

Classification: Public / Freely Distributable

© ODA3 Pvt Ltd. Published by ODA3 Institute.

Executive Summary

ODA3 Institute publishes four frameworks — GAISSF™, UAIF™, AI-IRF™, and PAI-SF™ — and readers arriving from the suite-level or framework-specific introductions often ask a practical next question: which one applies to me? This guide is a short decision aid, not a substitute for reading the frameworks themselves. It routes by immediate objective and system scope, not by a fixed sequence.

METHODOLOGY NOTE

This guide is introductory and conceptual. It contains no client outcome data, no proprietary telemetry, and no incident statistics. It does not constitute a formal scoping determination — it is a starting orientation only.

1. Start With Your Objective, Not the Suite

The four frameworks are complementary, not sequential. There is no single correct order to adopt them in, and no requirement to adopt all four. The right starting question is not "where do I begin in the suite?" but "what am I actually trying to do right now?"

GAISSF™ establishes governance, security controls, evidence expectations, and assurance requirements across the AI-system lifecycle. UAIF™ provides a common structure for identifying and classifying AI incidents. AI-IRF™ coordinates preparation and response activities for AI incidents; response may begin while classification continues. PAI-SF™ provides the deeper physical-AI security control framework where AI can affect the physical world.

2. Decision Table

If your immediate objective is to...	Start with
Govern an AI system's day-to-day safety and security, and structure assurance evidence	GAISSF™
Identify, structure, classify, or exchange a record of an AI-specific incident	UAIF™
Prepare for or coordinate response to an AI incident	AI-IRF™
Secure an AI system capable of physical effect or cyber-physical actuation	PAI-SF™

More than one framework may apply to the same system. A single AI system with physical actuation, for example, may eventually involve all four — but that does not mean all four must be adopted at once, or in a fixed order.

3. Common Starting Scenarios (Hypothetical)

- A team piloting a single internal AI assistant, with no incident history and no physical-world effect, would typically start with GAISSF™ — likely evaluating whether Appendix P.1 SMB Quick-Start is the appropriate profile for that system's scope.
- A SOC team that already runs incident response but has no consistent way to classify AI-specific incidents across tools would typically start with UAIF™, independent of where GAISSF™ adoption stands.

- A team building an incident-response playbook for AI-specific events, with classification work already underway, would typically start with AI-IRF™.
- A team securing a robotics or autonomous-vehicle platform would typically consider PAI-SF™ where physical-AI risks are in scope, alongside the applicable GAISSF™ requirements for the system.

These scenarios are illustrative only. They do not describe an ODA3 client, engagement, or outcome.

KEY PRINCIPLE

Selecting a framework is a scoping decision, not a maturity ranking. A smaller or newer program is not restricted to one framework, and a mature program is not required to have adopted all four.

4. If You're Still Unsure

- If your AI system has no incident history, no physical-world effect, and you have not yet reviewed any GAISSF™ material — start with The 10-Minute Introduction to GAISSF™.
- If you already use NIST AI RMF, ISO/IEC 42001, or SOC 2 and want to know whether adopting GAISSF™ means starting over — read the relevant mapping guide before choosing a framework here.
- If your organization is evaluating the suite as a whole rather than one system — read ODA3 Institute in 15 Minutes first.

NOTABLY ABSENT

This guide does not perform a formal scoping determination, does not establish which GAISSF™ conformance profile applies to a specific system, and does not establish conformance, certification, or regulatory compliance for any framework. It is a routing aid only.

The Ecosystem at a Glance

- GAISSF™ — Govern & Assure: lifecycle governance, controls, evidence expectations, and assurance requirements for AI systems.
- UAIF™ — Classify: a common structure for classifying AI-specific incidents.
- AI-IRF™ — Respond: coordinates preparation and response activities, including detection, containment, recovery, notification, and learning, while incident classification may continue iteratively.
- PAI-SF™ — Secure Physical AI: applies alongside the above, wherever the governed system is capable of physical effect or cyber-physical actuation.

Next Reading

- ODA3 Institute in 15 Minutes
- The 10-Minute Introduction to GAISSF™
- GAISSF™ Appendix P.1 SMB Quick-Start Guide
- Mapping GAISSF to NIST AI RMF / ISO/IEC 42001 / SOC 2

GAISSF™, UAIF™, AI-IRF™, and PAI-SF™ are frameworks of ODA3 Institute, referenced under the GAISSF Ecosystem License (GEL) v1.0.