

ODA3 INSTITUTE

ADOPTION GUIDE

ODA3 Institute in 15 Minutes

Doc ID: ODA3-2026-08-WHP-COM-002

Classification: Public / Freely Distributable

© ODA3 Pvt Ltd. Published by ODA3 Institute.

Executive Summary

ODA3 Institute builds the operational-assurance layer between AI governance requirements and real-world system behavior, while developing the assessment and certification infrastructure needed to evaluate that implementation against documented criteria and evidence. In practice, that means four frameworks — GAISSE™, UAIF™, AI-IRF™, and PAI-SF™ — that together address AI safety and security, incident classification, incident response, and physical-AI security assurance.

This guide is deliberately short. It will not make you an expert in any one framework. It will give you enough to understand what ODA3 Institute is, why the suite is structured the way it is, and which framework is relevant to your situation.

METHODOLOGY NOTE

This guide is introductory and conceptual. It contains no client outcome data, no proprietary telemetry, and no incident statistics. ODA3 Institute was founded in March 2026; nothing in this guide implies a longer operating history than that.

1. Why ODA3 Institute Exists

Many organizations deploying AI today may rely on governance mechanisms also used for conventional software: policies, review processes, and risk registers. Traditional governance instruments may not fully address systems whose behavior and failure modes may be less predictable or less bounded than conventional software — particularly once an AI system gains autonomy, tool access, or the ability to take action in the world.

Organizations may also need to interpret multiple sources of AI governance requirements — regulation, voluntary standards, and sector guidance. The result can be a gap between what those requirements expect and what an organization's controls and evidence can demonstrate.

ODA3 Institute exists to address that gap: not by writing another governance standard, but by building the operational-assurance layer that connects standards to demonstrable system behavior.

2. What ODA3 Institute Is — and Is Not

What it is

- An applied research and advisory firm at the intersection of cybersecurity, AI security, standards development, compliance advisory, and training and certification infrastructure.
- The publisher and steward of four purpose-built frameworks, licensed under one shared license, the GAISSE Ecosystem License (GEL) v1.0.
- An evidence discipline first, a framework author second — controls across the suite are structured so their implementation can be supported by identifiable evidence, not just a policy you can describe.

What it is not

- Not a general cybersecurity firm, and not a pure AI company — the suite specifically addresses AI security and operational assurance.
- Not a certification product in which payment itself establishes conformance — any formal assurance conclusion must be supported by the applicable assessment criteria and evidence. ODA3 Institute's assessment, training, and certification infrastructure is under development.

- Not a single monolithic framework — it is four frameworks, each scoped to a different part of the AI assurance problem.

3. The Four Frameworks

- **GAISSF™** — Global AI Safety and Security Framework. 9 domains with 52 foundational controls, plus 7 legacy D9 physical-AI controls retained within the current release for continuity and cross-reference. Where more detailed physical-AI security assurance is required, PAI-SF™ provides the expanded framework.
- **UAIF™** — Unified AI Incident Framework. 11 sections, 57 fields and tests, a 7-layer architecture, and 5 conformance profiles. Gives organizations a common structure for identifying and classifying AI-specific incidents. Current publication status: pilot-ready; not for production regulatory submission.
- **AI-IRF™** — AI Incident Response Framework. 19 domains and 79 controls covering preparation, detection, classification, containment, recovery, notification, and learning for AI-specific incidents.
- **PAI-SF™** — Physical AI Security Framework. 12 domains and 41 controls for AI-enabled systems capable of affecting the physical world, including robotics, autonomous vehicles, drones, medical robotics, industrial automation, and smart infrastructure.

KEY PRINCIPLE

The four frameworks are complementary, not competing. 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, including detection, containment, recovery, notification, and learning, while incident classification may continue iteratively. Where AI can affect the physical world, PAI-SF™ provides the deeper physical-AI security control framework.

4. A Worked Scenario (Hypothetical)

Consider a hypothetical mid-size insurer running an AI claims-triage assistant. Day-to-day governance and control of the assistant would fall under GAISSF™. If an event involving the assistant is assessed as an AI incident, UAIF™ provides the common structure to classify what happened, while AI-IRF™ coordinates preparation, containment, and recovery — these can proceed iteratively rather than waiting on a fully completed classification. If the organization also operates an AI-enabled system capable of physical effect — for example, an automated inspection drone — PAI-SF™ applies to that physical-AI scope.

This scenario is illustrative only. It does not describe an ODA3 client, engagement, or outcome.

5. Who Should Use This

- CISOs, Security Architects, and AI Governance Leads deciding where AI assurance work should begin.
- Compliance Officers and Standards Body Participants evaluating the suite against frameworks already in scope.
- Boards, CEOs, CFOs, General Counsel, and Risk Committees who need a short, non-technical orientation before a deeper conversation.

6. How the Suite Relates to What You Already Have

The suite is designed as an augmentation layer, not a replacement. It is built to complement and be mapped against frameworks organizations may already use — NIST AI RMF, ISO/IEC 42001, NIST CSF, ISO 27001, SOC 2. The objective is to identify where existing governance and security controls already provide coverage, where the ODA3 frameworks add AI-security or operational-assurance depth, and where additional controls or evidence are needed — not to start over.

NOTABLY ABSENT

This guide does not provide a control-by-control crosswalk, formal assessment methodology, regulatory-equivalence claim, certification conclusion, or evidence of client outcomes. ODA3 Institute's assessment, training, and certification infrastructure is under development; publication of these frameworks does not itself establish certification, compliance, regulatory approval, or effectiveness.

7. Which Framework Do I Need?

More than one framework may apply to the same system — select by objective and scope, not sequence:

Immediate objective	Framework
Govern AI safety/security controls and structure assurance evidence	GAISSF™
Identify, structure, classify, or exchange an AI incident record	UAIF™
Prepare for or coordinate AI incident response	AI-IRF™
Secure AI systems capable of physical effect or cyber-physical actuation	PAI-SF™

The GAISSF 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 when something happens within the governed system.
- AI-IRF™ — Respond: coordinates preparation and response activities, including containment, recovery, notification, and learning; response may begin while incident classification continues.
- PAI-SF™ — Secure Physical AI: applies alongside the above, wherever the governed system is capable of physical effect or cyber-physical actuation.

Next Reading

- Which GAISSF Ecosystem Framework Do I Need? (decision guide)
- The 10-Minute Introduction to GAISSF™
- GAISSF™ SMB Quick-Start Guide
- The AI Assurance Imperative: A Board Member's Guide to GAISSF™

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