

From EU AI Act Obligations to Operational Evidence

Executive Brief — Applying GAISSE™, UAIF™ and AI-IRF™

DocID: ODA3-2026-07-EXB-HAI-004
Classification: Public

Table of Contents

From EU AI Act Obligations to Operational Evidence

Executive Brief

Companion Technical Report: ODA3-2026-07-TCR-HAI-004

Classification: Public — Executive guidance

Methodology note

This brief is derived from the companion Technical Report, which uses primary EU sources and the governing GAISSE™, UAIF™ and AI-IRF™ publications. It describes operational support relationships, not legal equivalence. It contains no claim of certification, conformity assessment, regulatory approval or guaranteed compliance.

The board-level issue

The EU AI Act timetable is now staged. Stand-alone high-risk requirements apply from 2 December 2027, and product-embedded high-risk requirements from 2 August 2028. Other requirements already apply or arrive sooner. A single “AI Act deadline” is therefore no longer a sufficient governance model.

The board should expect management to answer five questions:

1. Which AI systems and GPAI models are in scope?
2. Which legal-entity and actor roles apply?
3. Which obligations apply now, and which follow a transition date?
4. What operational evidence demonstrates that assigned controls work?
5. How will a potential serious incident be classified, contained, reviewed and, where required, reported?

The three-framework operating model

Framework	Operational role	Board-level output
GAISSF™ v1.0	Governance, control objectives, ownership and evidence expectations	Approved control scope, owners, evidence register and exceptions
UAIF™ v1.0	Structured incident identity, classification, severity rationale and exchange	Consistent incident record and decision context
AI-IRF™ v1.0	Detection, triage, containment, evidence preservation, recovery and routing	Tested playbooks, response decisions and corrective actions

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

GAISSF's near-term Foundational profile contains 52 controls across D1–D8. Its seven D9 physical-AI controls are conditional, not universal. UAIF uses seven layers to separate incident identity, cause, analytical severity, harm pattern, vulnerability context, emerging AI modalities and regulatory metadata. AI-IRF then applies the organization's response, containment, recovery and review process. Framework profile and severity labels do not determine legal conformity or reportability.

What changes now

The revised dates should be used to replace deadline-driven remediation with a controlled evidence program. Management should establish a dated applicability register, a system and model inventory, assigned control owners, evidence requirements, incident-record standards and tested response procedures.

The target is not a general statement that the organization is “AI Act compliant.” The target is a reviewable chain:

Applicability decision → control → evidence → incident record → response → regulatory decision → corrective action

Decisions required

Decision 1 — Approve the applicability and classification method

Require a documented method for actor role, prohibited-practice screening, high-risk classification, GPAI status, Article 50 modality and transitional dates. Legal counsel retains authority for legal conclusions.

Decision 2 — Approve one evidence operating model

Require each mapped obligation to have an owner, implementation description, evidence location, validation method, exception process and review trigger.

Decision 3 — Separate severity from reportability

Require UAIF severity and routing fields to be treated as technical decision support. Article 73 reportability, competent authority and timing must be determined through role- and fact-specific review.

Decision 4 — Fund the 90-day readiness cycle

Authorize inventory and applicability work in days 0–30, control and incident-structure implementation in days 31–60, and exercises plus remediation in days 61–90.

Decision 5 — Control external claims

Prohibit public statements that framework adoption equals EU AI Act compliance, certification, regulatory approval or conformity assessment.

90-day outcome

By day 90, management should be able to present:

- an approved AI-system and GPAI inventory;
- documented actor-role and applicability decisions;
- a scoped GAISSE control and evidence register;
- a validated UAIF incident-record template;
- mapped and exercised AI-IRF playbooks;
- tested transparency, logging, human-oversight and evidence-preservation controls;
- a regulatory-review decision procedure; and
- a funded roadmap through the applicable 2027 or 2028 date.

Not represented as complete

This brief does not represent that harmonized standards are complete, that ODA3 certification infrastructure is operational, that an organization has passed conformity assessment, or that technical scoring determines legal reportability. It provides no universal implementation-cost estimate, sector-validated severity weights, platform-integration warranty or sector-specific algorithmic-bias remediation method. Sector-specific product law, data protection, employment, consumer-protection and contractual requirements require separate review.

Board direction

Treat the extended timetable as an evidence-building window. Require management to report progress through verified artifacts and tested decisions, not percentage-complete compliance claims.

Publication control

Document ID	ODA3-2026-07-EXB-HAI-004
Status	Publication candidate — register confirmation required
Regulatory baseline	19 July 2026
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
Licence	GAISSF Ecosystem Licence (GEL v1.0)

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

This publication provides operational and implementation guidance. It is not legal advice, certification, conformity assessment, regulatory approval or a guarantee of compliance. Applicability and legal sufficiency require review for the relevant actor, system, model, sector, jurisdiction and facts.