

ODA3 INSTITUTE

EXECUTIVE BRIEF

UAIF™ v1.0 Executive Brief

Unified AI Incident Framework — A Shared Language for AI Incidents

ODA3-2026-06-EXB-STD-001 | Public

© ODA3 Pvt Ltd

Document Control

Doc ID	ODA3-2026-06-EXB-STD-001
Doc Type	Executive Brief (EXB)
Framework Tag	UAIF™ v1.0
Audience	Board Members, Risk Committees, CISOs, AI Governance Leads, Compliance Officers
Companion Documents	ODA3-2026-06-TCR-STD-002 (Technical Specification); ODA3-2026-06-TCR-STD-003 (Schema Specification)
Governing Licence	GAISSF Ecosystem Licence (GEL) v1.0
Publication State	Final Publication designated 30 July 2026
Publish Date / Review Cycle	Issued June 2026; updated 04 October 2026; review cycle: quarterly
Classification	Public

UAIF™ v1.0 Executive Brief

Unified AI Incident Framework — A Shared Language for AI Incidents

Methodology Note: This brief summarises the UAIF™ v1.0 normative documents — the Technical Specification (TCR-STD-002), the Schema Specification (TCR-STD-003) and the machine-readable schema (uaif-core-v1.0.json). It contains no financial estimates and draws on no proprietary incident data. Normative behaviour, field definitions and scoring details are set out in the Technical Specification; readers who need evidence sourcing should use the companion documents.

1. The Problem

Organisations deploying AI systems face fragmented incident-reporting obligations and have no shared, machine-readable language for describing AI incidents. Each regime asks for reporting but leaves out a common way to classify, score and exchange incident records.

Regulation / Standard	Requires	Leaves Undefined
EU AI Act Article 73	Serious-incident reporting for high-risk AI systems	A cross-organisation severity scale and machine-readable incident schema
NIST AI Risk Management Framework 1.0	GOVERN and MANAGE functions, including incident tracking and communication	Operational incident record structure
ISO/IEC 42001:2023 (AI management systems)	Incident communication and corrective action within the management system	Cross-organisation comparability
EU Digital Operational Resilience Act (DORA)	Major ICT-related incident classification and reporting for financial entities	AI-specific incident taxonomy
EU NIS2 Directive	Significant-incident reporting for essential and important entities	AI-specific incident criteria

2. What UAIF Delivers

Capability	Business Value
Structured severity scoring	Consistent triage and board-reportable metrics
Regulatory trigger routing	Technical routing assistance for reporting decisions such as EU AI Act Article 73. The regulatory_trigger field is a routing flag only; legal counsel determines definitive obligations.
Causal separation chain	Better post-incident analysis and liability documentation
Generative and agentic AI classification	Coverage for retrieval-augmented generation (RAG) data leakage, prompt injection and AI-agent privilege escalation
Machine-readable schema	A published, validated JSON Schema that lets incident records move between tools and organisations

3. Architecture Overview

UAIF organises each incident record into seven layers:

Layer	Name	Governance Relevance
L0	Incident Identity & Workflow	Audit trail, deduplication, workflow state
L1	Causal Separation Chain	Root-cause isolation
L2	Severity Scoring	Board-reportable severity tiers
L3	Acute vs Chronic Harm	Long-term systemic risk
L4	Incident vs Vulnerability	Separating exposure from realised incidents
L5	Generative, Agentic & Control Plane	Prompt injection, RAG, Model Context Protocol (MCP), OAuth delegation, agent escalation
L6	Regulatory & Cross-Sector Metadata	Jurisdictional routing, regulatory obligation mapping, sector classification

Adoption Profiles and Extensions

Organisations adopt UAIF through one of three profiles, optionally adding either of two extensions:

Profile / Extension	Primary Use Case	Complexity
Core (profile)	Rapid deployment	Low
Enterprise (profile)	Governance maturity	Medium
Regulatory (profile)	Formal reporting obligations	High
SOC_SIEM (extension)	Integration with security operations centres and security information and event management tools	Medium
AI_Security (extension)	Generative and agentic AI security	Medium

4. Severity Scoring — Governance Implications

Output	Range	Governance Use
Severity Analytical Score	0.0–10.0	Comparative analytics and prioritisation

Output	Range	Governance Use
Severity Presentation Score	0.0–10.0	Operational triage and regulatory routing
Severity Level	1–5	Escalation and board thresholds
Regulatory Trigger	Yes/no flag with confidence band	Technical routing assistance only; not a legal determination
Severity Rationale	Machine-readable audit trail	Evidence and assurance documentation

5. Regulatory Alignment

UAIF provides technical routing and interoperability support across major governance and regulatory frameworks. Legal counsel remains responsible for definitive reporting determinations.

6. Licensing and Commercial Terms

Component	Licence	Notes
Core Specification	GEL v1.0 (non-commercial)	Commercial use requires a separate written licence (GEL v1.0 §17).
Reference implementation (oda3-uaif)	GEL v1.0 (non-commercial), on publication	Developed; not yet published. Commercial embedding will require a separate written licence (GEL v1.0 §17).
UAIF-Compatible designation	Written authorisation from ODA3 Institute	Requires written authorisation (GEL v1.0 §9.3). No designation is currently issued.
UAIF Certified designation	Reserved to ODA3 Institute	Certification authority is reserved to ODA3 Institute (GEL v1.0 §10.5). No certification service currently operates.

Any future certification or compatibility programme will be announced separately once its governance and operational gates close. Statements of factual alignment, such as "maps to UAIF Category Y", are permitted without authorisation (GEL v1.0 §10.3).

7. Notably Absent

- No legal determination of EU AI Act Article 73, GDPR, NIS2, DORA or sectoral obligations.
- No certification or compatibility designation is currently issued, and none can be claimed from framework use alone.
- No empirical claim that default harm weights are sector-validated.
- No published reference implementation or Conformance Test Suite yet; both are developed but not yet published.
- No warranty of operational integration with security monitoring or governance, risk and compliance platforms before platform testing.
- No pre-incident AI safety certification capability.

8. Decision Guide for Leadership

- **Board and Risk Committee:** decide whether AI incidents should be reported against UAIF severity levels, and which level triggers board escalation.

- **General Counsel:** review regulatory-trigger confidence bands and set legal review procedures for LOW-confidence outputs. Regulatory triggers are technical routing assistance only.
- **CISO:** choose the adoption profile — Core, Enterprise or Regulatory — and whether the SOC_SIEM or AI_Security extension applies.
- **AI Governance Lead:** confirm which AI systems' incidents will be recorded in UAIF format and who owns the records.

9. Contact and Resources

ODA3 Institute: oda3.org | UAIF documentation: docs.oda3.org/frameworks/uaif | Enquiries: contact@oda3.org

UAIF™ is a framework of ODA3 Institute, referenced under the GAISSE Ecosystem Licence (GEL) v1.0. | GAISSE Ecosystem developed by ODA3 Institute, licensed under GEL v1.0. | © 2026 ODA3 Pvt Ltd