ODA3 INSTITUTE

Technical Report

From EU AI Act Obligations to Operational Evidence

Applying GAISSF™, UAIF™ and AI-IRF™

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

Table of Contents

Document ID: ODA3-2026-07-TCR-HAI-004
Frameworks: GAISSF™ v1.0 · UAIF™ v1.0 · AI-IRF™ v1.0
Regulatory baseline: 19 July 2026
Audience: CISOs, AI governance leaders, compliance officers, security architects, internal audit and incident-response teams

Executive summary

The EU AI Act no longer presents a single August 2026 deadline. Following the 2026 Digital Omnibus amendment, requirements for stand-alone high-risk AI systems apply from 2 December 2027, while requirements for high-risk AI systems embedded in products covered by sectoral safety legislation apply from 2 August 2028. Other obligations follow different timetables: prohibited practices and AI-literacy requirements have applied since 2 February 2025; governance and general-purpose AI requirements began applying on 2 August 2025, subject to transitional rules; and the main Article 50 transparency application date remains 2 August 2026, with a limited transition to 2 December 2026 for machine-readable marking by certain systems already on the market.

The changed timetable creates a planning window, not an operational exemption. Organizations still need to determine their actor roles, classify systems and models, assign accountable owners, implement controls, preserve evidence, detect incidents, route decisions and demonstrate how conclusions were reached.

ODA3's three-framework ecosystem supports different parts of that work:

- **GAISSF™** provides governance, control objectives, ownership and evidence expectations.
- **UAIF™** provides a structured method and schema for recording and classifying AI incidents.
- **AI-IRF™** provides incident-response architecture, playbook logic, containment, recovery and regulatory-review routing.

Together, the frameworks can support a continuous operational-evidence chain. They do not determine legal applicability, replace conformity assessment, constitute certification, guarantee regulatory compliance or remove the need for legal and sector-specific review.

1. Purpose and scope

This paper translates selected EU AI Act obligations into operational work products and shows where GAISSF, UAIF and AI-IRF may support those work products. It is a traceability and readiness guide, not a legal crosswalk asserting equivalence.

The paper focuses on:

1. governance and accountability;
2. system and model inventory;
3. risk and role classification;
4. technical and operational controls;
5. documentation, logs and evidence;
6. post-market monitoring;
7. serious-incident handling; and
8. transparency and content provenance.

It does not reproduce the complete AI Act, determine whether a particular system is high-risk, decide which organization is a provider or deployer, or state that implementation of any ODA3 control satisfies an EU legal requirement.

2. Regulatory position at the publication date

2.1 Application timeline

Requirement group	Application position at 19 July 2026	Operational implication
Article 5 prohibited practices and Article 4 AI literacy	Applicable since 2 February 2025	Maintain use-case screening, prohibited-practice controls and role-appropriate literacy evidence now.
Governance and GPAI obligations	Applicable from 2 August 2025, subject to transitional provisions	Determine provider/model status and applicable transition before relying on a general date.
Article 50 transparency	Main application date 2 August 2026	Implement role- and modality-specific disclosure, marking and notice controls.
Machine-readable marking for certain systems already on the market before 2 August 2026	Transition to 2 December 2026	Document whether the transition applies and preserve the implementation decision.
Stand-alone high-risk AI systems	2 December 2027	Use the extended period for classification, control implementation, evidence generation and independent review planning.
High-risk AI systems embedded in products covered by sectoral safety legislation	2 August 2028	Coordinate AI Act work with the applicable product-safety and market-surveillance regime.

2.2 Why “the deadline moved” is an incomplete operating model

The applicable date depends on the system category, model status, actor role, placement date, sector and specific provision. A single countdown cannot represent this structure. Readiness therefore starts with a dated applicability record rather than a generic compliance checklist.

Minimum applicability record:

- legal entity and operating jurisdiction;
- AI-system or GPAI-model identifier;
- intended purpose and deployed use;
- provider, deployer, importer, distributor or other relevant role;
- prohibited-practice screening result;
- high-risk classification analysis;
- Article 50 modality and disclosure analysis;
- applicable transitional provision;
- accountable legal and operational owners;
- external counsel or conformity-assessment dependencies; and
- review date, assumptions and unresolved questions.

3. The three-framework operating model

3.1 GAISSF: governance, controls and evidence expectations

GAISSF v1.0 establishes an evidence-oriented security and safety baseline of 59 controls across nine domains. Its Foundational scope contains 52 controls across D1–D8, with seven D9 controls becoming additionally relevant where an AI system can influence or actuate the physical world. **[T1]**

For EU AI Act readiness, GAISSF can help organizations structure:

- control ownership and accountability;
- model, runtime, agentic and supply-chain security;
- content-safety and output controls;
- privacy and data-protection safeguards;
- human oversight and organizational controls;
- regulatory traceability; and
- physical-AI safety evidence where applicable.

GAISSF provides control and evidence structure. It does not establish the legal meaning of an AI Act article or prove that an organization has met it.

Conformance profiles and scope discipline

GAISSF defines three progressively stronger conformance profiles. The **Foundational** profile covers the 52 canonical controls in D1–D8, supported by a documented Statement of Applicability and operating evidence. The **Operational** profile adds every applicable D9 control and operating-effectiveness evidence across the assessed scope. The **Optimized** profile adds continuous monitoring and higher-assurance evidence. These profiles describe framework conformance expectations; they are not EU AI Act conformity-assessment outcomes or certificates. **[T1]**

D9 is conditional. It becomes relevant only where the documented assessment scope includes physical AI or cyber-physical actuation. Organizations should not automatically expand every assessment to D9, and should document both inclusion and exclusion decisions. **[T1]**

3.2 UAIF: incident classification and structured exchange

UAIF provides a structured incident record, severity methodology, causality fields, contextual modifiers and machine-readable exchange. Its regulatory-trigger fields are technical routing aids and require human review. Default weights and thresholds remain subject to calibration and should not be treated as legal thresholds. **[T1]**

For EU AI Act readiness, UAIF can support:

- stable incident identity;
- harm and affected-population recording;
- causal and contributing-factor analysis;
- evidence quality and provenance;
- analytical severity and rationale;
- sensitive-data and critical-sector context;
- consistent handoff between security, legal and compliance teams; and
- machine-readable input to response workflows.

UAIF classifies and records events. It does not determine whether Article 73 is legally triggered.

Seven-layer incident architecture

UAIF structures incident information across seven layers: L0 incident identity and workflow; L1 causal separation; L2 analytical severity; L3 acute and chronic harm; L4 incident and vulnerability distinction; L5 generative, agentic and control-plane context; and L6 regulatory and cross-sector metadata. Its severity model draws structural inspiration from vulnerability-scoring practice but is a post-incident classification and routing method, not a replacement for vulnerability scoring or legal assessment. **[T1]**

Published default weights and thresholds are provisional. They require organization- and sector-specific calibration, documented rationale and human review before operational use. No default score should be presented as independently sector-validated. **[T1]**

3.3 AI-IRF: response, containment, recovery and routing

AI-IRF provides response architecture for AI-specific incidents, including discovery, triage, evidence preservation, containment, regulatory-review routing, recovery and post-incident learning. AIIS, its machine-readable implementation schema, supports structured control and playbook interchange subject to vendor-specific transformation, validation, security review and testing. **[T1]**

For EU AI Act readiness, AI-IRF can support:

- incident declaration and command;
- AI-specific triage and playbooks;
- human-in-the-loop decision gates;
- containment and rollback;
- evidence preservation;
- candidate regulatory routing;
- recovery validation; and
- lessons-learned feedback into governance controls.

AI-IRF supports the operational response process. It does not replace competent legal analysis, determine the competent authority or set a legally binding notification deadline.

3.4 A concrete interoperability example

Where physical AI is within scope, GAISSF D9-CTL-07 links preservation of a cryptographic physical-incident evidence package with population of a UAIF incident record. This illustrates the ecosystem's intended evidence flow: the control establishes preservation expectations, UAIF structures the incident record, and AI-IRF governs response and recovery. The linkage is conditional on D9 applicability and still requires implementation testing in the target tooling environment. **[T1]**

4. From obligation to operational evidence

The ecosystem is most useful when implemented as a traceability chain. This is an ODA3 implementation model derived from the three governing framework sources. **[T2]**

> **Legal applicability decision → system obligation → GAISSF control objective → evidence artifact → UAIF incident record → AI-IRF response action → regulatory-review decision → retained outcome**

Each link must remain independently reviewable. A missing link should be recorded as a readiness gap rather than hidden behind a broad statement of compliance.

4.1 Minimum evidence object

For each mapped obligation, retain:

- obligation identifier and authoritative source;
- applicability decision and assumptions;
- responsible actor and control owner;
- supporting GAISSF control or locally defined control;
- implementation description;
- evidence type, location, owner and retention period;
- validation method and most recent result;
- exceptions and compensating measures;
- linked UAIF incident fields, where relevant;
- linked AI-IRF playbook or response procedure;
- reviewer and approval record; and
- next review trigger.

5. Operational-readiness crosswalk

The mappings below describe source-bounded support relationships. “Primary” means the framework provides the closest operational structure; “supporting” means it contributes evidence or workflow context. Neither term means legal satisfaction. **[T2]**

EU AI Act area	Required operational capability	GAISSF	UAIF	AI-IRF	Representative evidence
Article 4 — AI literacy	Role-based competence, training and retained records	Primary	Supporting for incident-derived learning	Supporting for exercises and responder training	Role matrix, curriculum, attendance, competency checks, exercise records
Article 5 — prohibited practices	Use-case screening, deployment gates and escalation	Primary	Supporting event classification	Primary for containment and escalation	Screening decision, approval gate, blocked-use log, escalation record
Articles 9 and 17 — risk management and quality system	Governed lifecycle, ownership, change control and review	Primary	Supporting incident feedback	Supporting corrective-action workflow	Risk register, control register, change approvals, management review
Article 10 — data and data governance	Provenance, quality, representativeness and access controls	Primary	Supporting evidence and harm context	Supporting incident handling	Data lineage, quality tests, access logs, exception decisions
Article 11 and Annex IV — technical documentation	Controlled system documentation and traceability	Primary	Supporting incident history	Supporting operational procedures	System card, architecture, model/version record, control evidence index
Article 12 — record-keeping	Logging design, integrity, access and retention	Primary	Primary incident record structure	Primary evidence preservation	Log specification, immutable records, clock synchronization, retention evidence
Article 13 — transparency and information to deployers	Intended-use, limitations and operational information	Primary	Supporting incident-derived limitations	Supporting operational notices	Instructions, limitation register, release notes, acknowledgement records
Article 14 — human oversight	Assigned authority, intervention capability and tested procedures	Primary	Supporting decision context	Primary response gates	RACI, override design, approval log, drill result, intervention record
Article 15 — accuracy, robustness and	Security testing, monitoring and resilience	Primary	Supporting incident classification	Primary response and recovery	Test results, monitoring output, red-team

EU AI Act area	Required operational capability	GAISSF	UAIF	AI-IRF	Representative evidence
cybersecurity					findings, rollback evidence
Articles 16, 18 and 20 — provider records and obligations	Ownership, retained documentation and logs	Primary	Supporting incident records	Supporting response records	Obligation register, document-retention evidence, log exports
Article 26 — deployer obligations	Use according to instructions, oversight, monitoring and logs	Primary	Supporting operational incidents	Primary handling and escalation	Deployment approval, operator training, monitoring logs, incident tickets
Article 27 — fundamental-rights impact assessment	Assessment governance and evidence linkage	Supporting	Supporting harm classification	Supporting response planning	FRIA, stakeholder analysis, mitigating-control evidence, approval decision
Article 49 — registration	Accurate inventory and controlled registration data	Primary	Supporting incident linkage	Supporting change triggers	Inventory record, registration submission, version/change log
Article 50 — transparency obligations	Interaction notice, synthetic-content marking and disclosure	Primary	Supporting failure classification	Primary remediation and evidence	UI/voice notice, marking configuration, test result, disclosure log
Articles 53 and 55 — GPAI obligations	Documentation, copyright policy, model evaluation and systemic-risk operations	Primary	Supporting incident structure	Primary incident and mitigation workflow	Model documentation, training-content summary, evaluation report, incident log
Article 72 — post-market monitoring	Continuous monitoring, feedback and corrective action	Primary	Primary event normalization	Primary investigation and remediation	Monitoring plan, signal record, trend analysis, corrective-action evidence
Article 73 — serious-incident reporting	Detection, causal assessment, routing, notification and follow-up	Supporting	Primary structured incident record	Primary response and routing	Incident record, causal assessment, routing decision, submitted notice, follow-up

6. Article 73: a decision process, not a severity threshold

Article 73 should not be implemented as “score above X equals report.” The operational process should separate technical severity from legal reportability. **[T1]**

Recommended decision sequence: **[T2]**

1. create a stable incident identity;
2. preserve time, model, system, actor and evidence context;
3. classify harm, affected parties, sector and operational impact in UAIF;
4. begin AI-IRF containment and investigation without waiting for final legal classification;
5. determine the relevant actor role and whether the system falls within the applicable high-risk regime;
6. assess the statutory serious-incident definition and causal link;
7. determine the competent authority and applicable timing case;
8. record the reporting or non-reporting rationale;
9. submit, update and retain the notification evidence where required; and
10. feed corrective actions back into GAISSF governance and controls.

The corrected AI-IRF Technical Report describes Article 73's tiered timing mechanism without asserting a single attachment date. HAI-004 follows the same approach.

7. A 30/60/90-day readiness pathway

Days 0–30: establish scope and decision ownership [T2]

- approve the actor-role and system-classification method;
- create or reconcile the AI-system and GPAI-model inventory;
- screen prohibited practices and Article 50 modalities;
- identify applicable transition dates;
- assign legal, governance, security, engineering and audit owners;
- establish the evidence repository and naming convention;
- select the GAISSF controls used as the initial operating baseline; and
- define which decisions require documented human approval.

Exit evidence: approved inventory, applicability register, owner matrix, initial control scope and unresolved-dependency log.

Days 31–60: implement controls and incident structure [T2]

- document intended purpose, architecture, versions, data flows and dependencies;
- implement priority logging, human-oversight and transparency controls;
- configure UAIF incident-record fields and validation rules;
- map AI-IRF playbooks to the organization's incident-command structure;
- define evidence retention and access controls;
- test content notices and machine-readable marking where applicable;
- define Article 73 legal-review and escalation procedures; and
- record exceptions and compensating measures.

Exit evidence: control implementation records, test results, UAIF record template, response playbooks and regulatory-routing procedure.

Days 61–90: exercise, challenge and improve [T2]

- run tabletop and technical exercises;
- simulate an Article 5 prohibited-use discovery;
- simulate an Article 50 marking or disclosure failure;
- simulate a potential serious incident without assuming reportability;
- test containment, rollback, evidence preservation and executive escalation;
- conduct an internal evidence-quality review;
- remediate priority gaps; and
- approve the next readiness cycle through 2027 or 2028, as applicable.

Exit evidence: exercise pack, decision logs, corrective-action register, residual-risk acceptance and approved roadmap.

8. Governance model and accountability

Function	Minimum accountability
Board or executive risk owner	Approves risk appetite, major exceptions and readiness funding.
Legal/compliance	Determines legal applicability, reporting duties and authority engagement.
AI governance	Maintains inventory, role classification, control scope and evidence governance.
CISO/security	Implements security controls, monitoring, incident command and technical evidence.
Engineering/model owner	Maintains system documentation, testing, logs, change control and remediation.
Privacy/data governance	Governs personal-data, provenance, quality, access and retention decisions.
Internal audit/assurance	Challenges evidence sufficiency and verifies that claimed procedures operate.

No framework field or automated score should silently replace one of these accountabilities. **[T1]**

9. Notably absent

This paper does not provide: **[T1]**

- a legal opinion on actor role or system classification;
- a declaration of EU AI Act compliance;
- an issued ODA3 certification or assessment result;
- a conformity assessment under the AI Act;
- a guarantee that harmonized standards or common specifications are complete;
- a complete sector-specific product-safety crosswalk;
- a claim that UAIF severity determines Article 73 reportability;
- a claim that AIIS objects can be ingested by every SOAR or GRC product without adaptation;
- empirical validation that all GAISSF, UAIF or AI-IRF thresholds perform consistently across sectors; or
- proof that implementing the listed evidence artifacts makes a control effective;
- empirical validation that UAIF default harm weights are sector-calibrated;
- proprietary sector-calibration packages or confidential pilot datasets;
- a warranty that UAIF or AIIS objects integrate with a particular SIEM, SOAR or GRC platform before target-platform transformation and testing;
- universal monetary-loss, staffing-hour, tooling-cost or implementation-cost estimates;
- sector-specific mathematical or clinical methods for remediating algorithmic bias; or
- treatment of GAISSF D9 as universally mandatory.

Organizations remain responsible for jurisdiction-specific legal review, applicable harmonized standards, sector legislation, data-protection obligations, worker-consultation requirements, contractual duties and competent-authority guidance.

10. Conclusion

The most important effect of the revised EU AI Act timetable is not that organizations can stop. It is that they can replace deadline-driven remediation with a controlled evidence program.

GAISSF, UAIF and AI-IRF are designed to address different operational layers: governance and evidence expectations, structured incident classification, and incident response. Their value lies in connecting those layers while preserving the boundary between technical assistance and legal determination.

The target state is not a badge or a broad claim of compliance. It is a reviewable chain showing what the organization believed applied, which controls it implemented, what evidence those controls produced, how incidents were classified and handled, who made regulatory decisions, and how the organization corrected what failed. **[T2]**

Primary regulatory sources

1. Regulation (EU) 2024/1689, Artificial Intelligence Act, EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
2. European Commission, “AI Act — Regulatory framework for AI”: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
3. European Parliament, “AI Act: EP approves simplification measures and ‘nudifier’ app ban,” 16 June 2026: https://www.europarl.europa.eu/news/en/press-room/20260611IPR45207/ai-act-ep-approves-simplification-measures-and-nudifier-app-ban
4. Council of the EU, “Artificial Intelligence: Council gives final green light to simplify and streamline rules,” 29 June 2026: https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/

ODA3 framework sources

1. GAISSF-NOR-001 — GAISSF™ v1.0 authoritative normative source.
2. GAISSF-NOR-002 — GAISSF™ v1.0 Executive Summary, final publication edition.
3. ODA3-2026-06-TCR-STD-002 — UAIF™ v1.0 Technical Specification.
4. ODA3-2026-06-TCR-STD-003 — UAIF™ v1.0 Schema Specification.
5. ODA3-2026-06-TCR-HAI-001 — AI-IRF™ v1.0 Technical Report, corrected regulatory edition.
6. ODA3-2026-06-EXB-HAI-002 — AI-IRF™ v1.0 Executive Brief.
7. ODA3-2026-06-TCR-HAI-003 — AIIS Implementation Schema, document edition v1.0.1.

Reliance statement

This publication provides technical and implementation guidance. It is not legal advice, does not constitute certification or regulatory approval, and does not guarantee compliance. References to EU AI Act articles are traceability references only. Applicability must be determined for the relevant organization, actor role, system, model, sector, jurisdiction and facts.

Publication control

Document ID	ODA3-2026-07-TCR-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)

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.