

ODA3 INSTITUTE

SECTOR APPLICATION NOTE

Financial Services

Applying AI-IRF™ v1.0 to banking, insurance, capital markets and payments

ODA3-2026-06-RPT-SCS-024 | Public

Document Control

Doc ID	ODA3-2026-06-RPT-SCS-024
Doc Type	Sector Application Note (RPT)
Framework Tag	AI-IRF™ v1.0 (79 controls across 19 domains)
Sector	Financial services — banking, insurance, capital markets, payments
Regulatory Crosswalk	DORA (EU) 2022/2554; EU AI Act (EU) 2024/1689; GDPR; MiFID II; RBI FREE-AI Committee Report (India); SEBI AI/ML consultation (India)
Companion Documents	ODA3-2026-06-TCR-HAI-001 (Technical Report); ODA3-2026-06-EXB-HAI-002 (Executive Brief)
Evidence Basis	Implementation guidance. Regulatory references checked against primary texts; control references checked against ODA3-2026-06-TCR-HAI-001
Publish Date / Review Cycle	Issued 1 June 2026; updated 04 October 2026; review cycle: annual
Classification	Public

Sector Application Note — Financial Services

Applying AI-IRF™ v1.0 to banking, insurance, capital markets and payments

Purpose: This note shows how AI-IRF™ v1.0 incident response controls relate to the obligations financial institutions already work under. It is implementation guidance, not legal or regulatory advice. Organisations should consult qualified counsel before making any compliance claim.

Licence notice — GEL v1.0 | Public. This document is part of the GAISSE Ecosystem published by ODA3 Institute (ODA3 Pvt Ltd) under the GAISSE Ecosystem Licence (GEL) v1.0 (effective 1 May 2026); it was adopted under GEL v1.0 on 1 June 2026. GAISSE™, UAIF™, AI-IRF™, PAI-SF™ and ODA3™ are trademarks of ODA3 Pvt Ltd; registration applications are pending or the marks are common-law marks (GEL §9.1). Commercial use — including consulting, advisory work, regulatory submissions prepared for a fee, or training delivery — requires a separate written commercial licence (GEL §§3.4, 17). AI training data use is prohibited without a licence (GEL §3.6). Provided "AS IS" without warranties (GEL §12). Governing law: Republic of India; DIAC arbitration, New Delhi seat (GEL §14). Attribution (GEL §6): GAISSE Ecosystem developed by ODA3 Institute, licensed under GEL v1.0.

1. Why AI Incident Response Matters in Financial Services

Financial institutions use AI extensively — credit decisioning, fraud detection, algorithmic trading, insurance underwriting, anti-money-laundering (AML) screening and customer service. When these systems fail or are attacked, institutions face strict incident-handling and reporting regimes, most of which are technology-neutral: they apply to AI systems as ICT assets rather than naming AI specifically.

AI-IRF™ v1.0 provides incident response controls — detection, containment, rollback, evidence preservation and regulatory routing — for those failures. This note shows where those controls fit within the regimes financial institutions already follow.

2. Regulatory Landscape

2.1 DORA — Digital Operational Resilience Act (EU) 2022/2554

DORA has applied since 17 January 2025 to EU financial entities, including banks, investment firms, insurers, payment institutions and crypto-asset service providers, with an oversight framework for critical ICT third-party providers. DORA does not mention AI, but AI systems are ICT assets within its scope.

- **Articles 5–16 — ICT risk management:** governance (Art. 5), the ICT risk management framework (Art. 6), identification of ICT assets and dependencies (Art. 8), protection and prevention (Art. 9), detection (Art. 10), response and recovery (Art. 11) and backup (Art. 12), with a simplified framework for certain smaller entities (Art. 16).
- **Articles 17–19 — incident management and reporting:** an ICT incident management process (Art. 17), classification of incidents (Art. 18) and reporting of major ICT-related incidents (Art. 19). Under the implementing standards, an initial notification is due within 4 hours of classifying an incident as major and no later than 24 hours after becoming aware of it, an intermediate report within 72 hours of the initial notification, and a final report within one month.
- **Articles 28–30 — ICT third-party risk:** risk assessment, contractual provisions and monitoring of ICT third-party providers, including providers of AI models and platforms.

2.2 EU AI Act — High-Risk Systems in Financial Services

Under Annex III point 5, the EU AI Act classifies as high-risk AI systems used to evaluate the creditworthiness of natural persons or establish their credit score (excluding systems used to detect financial fraud) and AI systems used for risk assessment and pricing in life and health insurance. AI used in employment decisions is separately high-risk under Annex III point 4. AML and fraud-detection systems are not listed as high-risk under Annex III.

High-risk systems must meet Articles 9–15 (risk management, data governance, technical documentation, record-keeping, transparency, human oversight, and accuracy, robustness and cybersecurity). For Annex III point 5 systems, conformity assessment is based on internal control (Article 43(2), Annex VI). Serious incidents are reported under Article 73. Application dates depend on the operative AI Act timetable.

2.3 Algorithmic Trading — MiFID II

MiFID II Article 17 requires investment firms engaged in algorithmic trading to have effective systems and risk controls, including thresholds and limits, controls to prevent erroneous orders, and business continuity arrangements. The supporting technical standards (RTS 6) include a kill functionality allowing firms to cancel unexecuted orders immediately. These requirements apply to AI-driven trading strategies as to any other algorithm.

2.4 India — RBI FREE-AI Committee Report

On 13 August 2025, the Reserve Bank of India published the report of its Committee on a Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) in the financial sector. The report sets out seven guiding principles ("Sutras") — trust, people first, innovation, fairness, accountability, explainability and resilience — and 26 recommendations under six pillars: infrastructure, policy, capacity, governance, protection and assurance. It is a committee report with recommendations; institutions should track which recommendations RBI implements through binding directions, alongside existing requirements such as the IT governance and outsourcing Master Directions.

2.5 India — SEBI

On 20 June 2025, SEBI issued a consultation paper, "Guidelines for Responsible Usage of AI/ML in Indian Securities Markets", proposing principles on model governance, human oversight, disclosure, testing and monitoring for market participants using AI/ML. Institutions should confirm the current status of these proposals before relying on them.

3. AI-IRF™ v1.0 Control Mapping

Control definitions are those in Section 7 of ODA3-2026-06-TCR-HAI-001. A mapping shows where a control can contribute evidence; it does not establish compliance with the mapped obligation.

AI-IRF™ v1.0 controls	Related obligations	How the controls contribute
Regulatory operations (REG-1–4)	DORA Arts. 17–19; EU AI Act Art. 73; GDPR Arts. 33–34	A jurisdictional decision tree routes each AI incident to the applicable reporting regimes, with deadline calculation and retained evidence packages
Detection, triage and severity (MSR-1–5, REL-1–3, SEV-CLS, SEV-RPT)	DORA Arts. 10, 17, 18	Machine-speed detection with reliability safeguards and deterministic, versioned severity classification support consistent classification of major incidents
Agentic permissions (APA-1–5) and human approval thresholds (MSR-4)	EU AI Act Art. 14; MiFID II Art. 17; DORA Art. 9	Human approval for payment initiation, large data exports and actions above a financial-impact threshold, with pre-execution gates on every tool call
Model lifecycle and supply chain integrity (MLC-1–5, BOM-1–5)	DORA Arts. 8, 9, 28–30; EU AI Act Art. 15	Signed model identifiers, runtime manifest validation, supplier attestation, vendor notification and tested 15-minute rollback
Model extraction defence (MEX-1–4)	DORA Art. 9; EU AI Act Art. 15	Detection of systematic extraction of proprietary credit, fraud or trading models through API access, with rate limiting and key revocation
Zero trust (ZTA-1–4) and discovery (SAI-1–5)	DORA Arts. 8, 9; GDPR Art. 32	Identity-first access, segmentation, and discovery of unsanctioned AI tools with data-loss prevention on AI egress
Content safety and bias (CSS-5–7)	EU AI Act Art. 10 (Annex III point 5 systems)	Monthly bias analysis and quarterly demographic impact assessment for credit scoring and life and health insurance pricing
Hallucination detection (HAL-1–5)	EU AI Act Art. 15; consumer protection rules	Grounding verification, confidence thresholds and fact-checking for AI-generated customer communications and financial advice

4. Sector-Specific Control Guidance

4.1 Credit Decisioning AI

- **CSS-5 and CSS-6 (bias monitoring):** credit scoring is high-risk under Annex III point 5(b). Monthly bias analysis and a quarterly demographic impact assessment provide documented results, not just a policy commitment.
- **MLC-5 (drift-triggered retraining):** population shift in applicants can degrade a model without obvious errors. Drift should trigger a dual-approval retraining workflow.
- **HAL-2 (confidence and human review):** credit decisions with confidence below 0.7 require human review before action.

4.2 AML and Fraud Detection AI

- **SEV-CLS and SEV-RPT (classification and reportability):** suppressed or overridden alerts, and missed suspicious activity, should be classified and assessed for reportability with a deterministic, versioned method.
- **APA-4 (permission audit trail):** every grant, denial and override is logged with signed, immutable timestamps, so compliance teams can reconstruct the system's decision path.
- **BOM-3 (supplier attestation):** third-party watchlists and typology databases require supplier attestation and authenticity checks before integration.

4.3 Algorithmic Trading and Capital Markets AI

- **MSR-4 and APA-3 (human approval thresholds):** actions above the defined financial-impact threshold require human approval — complementing, not replacing, MiFID II Article 17 kill functionality.
- **MEX-1 to MEX-4 (extraction defence):** proprietary trading models exposed through APIs need extraction detection, dynamic rate limiting and API key revocation within 5 minutes of confirmed extraction.
- **BOM-4 and MLC-2 (supply chain and rollback):** playbooks should cover compromise of market-data or model suppliers, with vendor notification within 24 hours and tested rollback.

4.4 Insurance Underwriting and Pricing AI

- **CSS-6 and CSS-7 (impact assessment):** life and health insurance pricing is high-risk under Annex III point 5(c). Assess outcomes across demographic groups and identified vulnerable groups, including proxy variables.
- **SEV-CLS (anomaly classification):** anomalous pricing outputs, such as extreme outliers, should be detected and classified as incidents for investigation.

5. Implementation Pathway

Step	Activity	Financial services context
1	Scope definition	Start with the highest-risk AI — credit scoring, life and health insurance pricing, trading or AML — rather than the full portfolio.
2	Reporting map	Map which regimes an AI incident could trigger — DORA Article 19, EU AI Act Article 73, GDPR and national rules — and configure the REG-1 decision tree.

Step	Activity	Financial services context
3	Preparation	Complete PREP-1 to PREP-7, including pre-approved playbooks, designated human approval authority and monthly rollback drills.
4	DORA integration	Record AI systems in the DORA ICT asset inventory and include AI providers in the register of information on ICT third-party arrangements.
5	Exercise	Run tabletop exercises for a compromised third-party model and a model-driven erroneous trading or credit event; retain the records.
6	Use in existing programmes	Use AI-IRF™ evidence within DORA ICT risk management documentation, AI Act technical files and board risk reporting, as each regime permits.

6. Frequently Asked Questions

Question	Answer
Do AI-IRF™ controls satisfy DORA?	No single framework satisfies DORA. AI-IRF™ controls can provide documented evidence for the AI-specific parts of ICT risk management, incident handling and third-party risk; DORA's broader obligations remain.
Will supervisors accept AI-IRF™ evidence?	Supervisors do not pre-approve frameworks. Evidence is assessed on its quality and relevance to the specific obligation.
How does AI-IRF™ relate to ISO/IEC 27001?	They are complementary. ISO/IEC 27001 covers the information security management system; AI-IRF™ v1.0 covers incident response for AI systems.
Can we start with a single AI system?	Yes. Starting with one high-risk system, such as the credit scoring model, and expanding is a practical approach.

7. Notably Absent

- No certification or audit service is operating. Certification is not currently offered. This note describes control implementation only.
- No compliance determination under DORA, the EU AI Act, GDPR, MiFID II, RBI or SEBI requirements is made or implied.
- No claim that DORA, MiFID II or GDPR address AI explicitly; their obligations are technology-neutral.
- No claim that RBI's FREE-AI recommendations or SEBI's AI/ML proposals are binding requirements unless and until implemented by the regulator.
- No regulator or standards-body endorsement of AI-IRF™ v1.0 is claimed.

Enquiries: contact@oda3.org

GAISSF Ecosystem developed by ODA3 Institute, licensed under GEL v1.0. | © 2026 ODA3 Pvt Ltd | oda3.org