

EU AI Act Gap Report

Technical Readiness Assessment

50%

Significant gaps

| | |
|-----------------|----------------------------------------------------------------|
| Generated | 28 March 2026 |
| Organisation | Test organisation |
| System | Test AI system |
| Role | Deployer Arts. 26, 27 — deploying in a professional context |
| System type | High-Risk System (Annex III) |
| Gaps identified | 7 of 7 pillars |
| Critical gaps | 4 |

Organisation and system name are not stored or transmitted.

Executive Summary

Your AI system has notable compliance gaps in 7 of 7 assessed pillars, with an overall readiness score of 50%.

Most urgent: Provider Conformity Verification (Art. 26) — deadline Aug 2026.

Recommended first action

Request the provider's Declaration of Conformity and verify their registration in the EU AI database.

Gap Report

7 pillars assessed · 7 gaps identified · 4 critical

| Priority | Pillar | Status | Article | Enforcement |
|------------------|---------------------------------------------|---------|------------|-------------|
| Critical | Provider Conformity Verification | Partial | Art. 26 | Aug 2026 |
| Critical | Instructions for Use — Implementation | Partial | Art. 26 | Aug 2026 |
| Critical | Human Oversight — Operational | Partial | Art. 26 | Aug 2026 |
| Critical | Log Retention | Partial | Art. 26(6) | Aug 2026 |
| Important | Staff AI Literacy | Partial | Art. 4 | In force |
| Important | Operational Monitoring & Incident Reporting | Partial | Art. 26(5) | Aug 2026 |
| Important | Risk Management — Deployment Context | Partial | Art. 9 | Aug 2026 |

Recommended Actions (7)

Critical Provider Conformity Verification

Art. 26 · Aug 2026

Request the provider's Declaration of Conformity and verify their registration in the EU AI database. Document this check and retain the records as evidence of due diligence.

Critical Instructions for Use — Implementation

Art. 26 · Aug 2026

Obtain the provider's Article 13 instructions-for-use document. Review the intended purpose and operational constraints. Document how your deployment aligns with the intended use and implement all required measures.

Critical Human Oversight — Operational

Art. 26 · Aug 2026

Assign named individuals as human overseers with documented authority to override or suspend the system. Define clear escalation paths, train overseers on the system's outputs and failure modes, and document competence assessments.

Critical Log Retention

Art. 26(6) · Aug 2026

Implement log retention policies ensuring operational logs are stored for at least 6 months under Article 26(6). Check sector-specific regulations (e.g. financial services, healthcare) for longer retention requirements. Document your retention policy and access controls.

Important Staff AI Literacy

Art. 4 · In force

Design and deliver role-appropriate AI literacy training covering: how the system works, its limitations, how to recognise errors, and escalation procedures. Document training completion and maintain records for audit.

Important Operational Monitoring & Incident Reporting

Art. 26(5) · Aug 2026

Establish a documented operational monitoring process covering: (1) regular review of system outputs against the provider's instructions for use, (2) a clear decision rule for when to suspend use, (3) a reporting chain — first to provider, then to market surveillance authority — for serious incidents. This is required under Article 26(5) and is distinct from the provider's Article 72 post-market monitoring obligation.

Important Risk Management — Deployment Context

Art. 9 · Aug 2026

Conduct a context-specific risk assessment covering: your user population, deployment environment, integration points, and use cases beyond the provider's intended scope. Document findings, mitigations applied, and residual risks.