DORA

Compliance Gap Analysis

EU Digital Operational Resilience Act (Reg. 2022/2554)

OVERALL: PARTIAL (20.0%)

Organization: AI Agent Runtime B (self-hosted)

Generated: 2026-07-21T11:48:53.303369Z

Generated by: ralphadmin

Report type: Gap Analysis (Self-Assessment)

This is a SELF-ASSESSMENT gap analysis based on SentriKat vulnerability management data. It is NOT a certified DORA audit. Engage a qualified assessor for certification.

Executive Summary

This gap analysis assessed **5** DORA control areas against the organization's current vulnerability-management posture. **1** passed, **4** were partially met, **0** failed and **0** were not applicable, for an overall compliance score of **20.0%** (verdict: **PARTIAL**).

Metric	Value
Total requirements	5
PASS	1
PARTIAL	4
FAIL	0
NOT APPLICABLE	0
Compliance score	20.0%

PASS (1) PARTIAL (4)

Detailed Findings

DORA Art. 8 — Identification of ICT assets and their vulnerabilities

Status: PARTIAL

Financial entities shall identify, classify and document all ICT supported business functions, information assets and ICT assets, and on a continuous basis identify all sources of ICT risk and cyber threats / vulnerabilities relevant to those assets.

Evidence:

• ict_assets_inventoried: 197

• assets_scanned: 0

• agents_reporting: 0

• vulnerabilities_identified: 288

• intel_sources: ['NVD', 'CISA KEV', 'EPSS', 'ENISA EUVD', 'OSV', 'distro feeds']

Findings:

• Asset identification incomplete (agents offline or assets never scanned).

Recommendations:

• Ensure every ICT asset runs a SentriKat agent and is scanned.

DORA Art. 9 — Protection and prevention — vulnerability & patch management

Status: PARTIAL

Financial entities shall continuously monitor and control the security of ICT systems and minimise the impact of ICT risk through sound ICT security policies, including patch and vulnerability management with defined remediation timeframes.

Evidence:

• sla_policies_in_place: False

• open_critical: 13

• avg_remediation_days: None

• backport_aware_suppression: Ubuntu/Debian/RHEL/Alpine/Oracle/Amazon/SUSE distro feeds

Findings:

• Define remediation SLAs and clear open critical vulnerabilities.

Recommendations:

• Set SLA policies per severity; track remediation to closure.

DORA Art. 10 — Detection — continuous monitoring of ICT systems

Status: PARTIAL

Financial entities shall have mechanisms to promptly detect anomalous activities and ICT vulnerabilities, with multiple layers of control and defined alert thresholds enabling prompt response.

Evidence:

• continuous_scanning: False

• last_scan_age_hours: None

• agents_online: 0

• kev_epss_prioritization: True

Findings:

• Continuous detection not fully active (stale scans or offline agents).

Recommendations:

• Keep scheduled scans daily and agents online; alert on KEV/EPSS.

DORA Art. 11 — Response and recovery — remediation handling

Status: PARTIAL

Financial entities shall put in place a comprehensive ICT business continuity policy and response/recovery plans, including documented handling of identified ICT vulnerabilities to closure.

Evidence:

• remediation_assignments_resolved: 0

• findings_awaiting_action: 8

• tracker_integration: Jira / GitHub / GitLab / YouTrack / webhook

• sla_policies_in_place: False

Findings:

• No remediation SLA/response policy detected.

Recommendations:

• Link remediation to an issue tracker for an auditable trail.

DORA Art. 28-30 — ICT third-party risk — software supply chain

Status: PASS

Financial entities shall manage ICT third-party risk, including the software supply chain: maintaining a register of components and assessing the vulnerabilities of third-party / open-source software.

Evidence:

• dependency_scanning: OSV ecosystem+version (no CPE guess)

• sbom_export: CycloneDX / SPDX / STIX

• vex_export: CycloneDX VEX from risk exceptions

• license_compliance: deps.dev SPDX policy

Recommendations:

• Export SBOM/VEX for your providers; track third-party component CVEs.

Data Sources & Provenance

Intelligence feeds this assessment was computed from, and their freshness at generation time. The edge is what SentriKat does with them: deterministic FP-free matching, backport-aware suppression, and air-gap operation.

Source	Category	Status	Last update	Records
NVD — CVE feed	CVE master	FRESH	2026-07-20 10:22:37	364,763
NVD — CPE dictionary	CVE master	PRESENT	—	70,132
CISA KEV — known exploited	Exploitation	FRESH	2026-07-20 10:22:37	1,637
EPSS — exploit prediction	Exploitation	PRESENT	—	346,847
ENISA EUVD	Regional	PRESENT	—	13
CISA Vulnrichment	CVSS enrichment	NEVER	—	0
OSV.dev — packages	Dependencies	NEVER	—	0
deps.dev — licenses	Dependencies	NEVER	—	0
Vendor advisories (Red Hat / MSRC / Debian online)	Backport fixes	NEVER	—	0
Ubuntu USN	Distro (backport-aware)	FRESH	2026-07-20 10:21:59	97,732
Debian Security Tracker	Distro (backport-aware)	FRESH	2026-07-20 10:22:37	215,384
RHEL / Rocky / AlmaLinux (OSV)	Distro (backport-aware)	FRESH	2026-07-20 10:21:28	331,812
Alpine (OSV)	Distro (backport-aware)	FRESH	2026-07-20 10:16:03	43,091
Oracle Linux ELSA	Distro (backport-aware)	FRESH	2026-07-20 10:21:26	100,546
Amazon Linux ALAS	Distro (backport-aware)	FRESH	2026-07-20 10:21:27	40,606
SUSE SLE (OSV)	Distro (backport-aware)	FRESH	2026-07-20 10:20:33	44,750
openSUSE Leap (OSV)	Distro (backport-aware)	FRESH	2026-07-20 10:20:38	13,912
SentriKat Knowledge Base	Curated	NEVER	—	—

Assessment Sign-off

This report is a self-assessment generated from SentriKat data. To formalise it, an authorised assessor should review the findings above and sign below.

Assessed by (name): _____

Role / title: _____

Signature: _____

Date: _____