EU Cyber Resilience Act (CRA) — Scope Determination

trust-center, compliance, cra, cybersecurity-resilience-act, nis2, policies

Document owner: Predrag Tasevski (CEO/Founder)
Status: Internal determination — living document, reviewed on regulatory or product changes
Last reviewed: 2026-07-10
Disclaimer: This is an internal compliance determination prepared by Unicis Tech OÜ for its own product portfolio. It is not legal advice. It should be reviewed by qualified external counsel before being relied upon in a contractual, regulatory, or dispute context.

1. Purpose

Regulation (EU) 2024/2847 (the Cyber Resilience Act, “CRA”) imposes cybersecurity obligations on manufacturers, importers, and distributors of **products with digital elements (“PDE”)** placed on the EU market. It does **not** apply to services as such — those are addressed separately, notably by the NIS2 Directive.

This document records Unicis Tech OÜ's assessment of whether, and to what extent, its product portfolio falls within CRA scope, which conformity route applies, and what obligations follow — including the reporting obligations under Article 14, which apply from **11 September 2026**, ahead of full applicability on 11 December 2027.

2. Regulatory Basis

- **Regulation (EU) 2024/2847** — entered into force 10 December 2024.
- Chapter IV (notified body notification) applies from 11 June 2026.
- **Article 14 reporting obligations** (actively exploited vulnerabilities / severe incidents to ENISA and national CSIRTs) apply from **11 September 2026**, and reach products already on the market — not only new ones.
- Full applicability (essential requirements, conformity assessment, CE marking) from **11 December 2027**.
- European Commission draft guidance, Communication Ares(2026)2319816 (3 March 2026), introduces the operative test for “remote data processing solutions” (RDPS) used in Section 3 below.
- Products only require third-party (notified body) conformity assessment if listed in **Annex III** (“important” products, Class I/II) or **Annex IV** (“critical” products). All other in-scope products are **default category** and use **internal control / self-assessment (Module A, Annex VIII)**.

3. Product-by-Product Assessment

Unicis Tech OÜ makes three distinct offerings available. Each is assessed separately, since CRA scope attaches to the product, not the vendor.

Offering	Distribution model	CRA scope view	Rationale
Unicis Platform — Hosted SaaS (platform.unicis.tech)	Browser-accessed only; no client-side download or install	**Out of scope** (services excluded)	Pure cloud-native SaaS consumed via browser, with no software placed on the market for the customer to run. Falls under NIS2 rather than CRA. Confirmed against the Commission's 3-part RDPS test (Section 3.2): the hosted platform is not “remote data processing” that is essential to the function of a separately placed-on-market product — it *is* the service itself.
Unicis Platform — Community Edition (CE) (github.com/UnicisTech/unicis-platform-ce, Apache 2.0)	Distributed as downloadable, installable software; deployed and operated by the recipient on their own infrastructure	**In scope**	Meets the definition of a software product placed on the market: made available to third parties, installed and run outside Unicis's own infrastructure, distributed in the course of a commercial activity (open-core lead generation for the paid SaaS). The non-commercial open-source exemption does not cleanly apply, since distribution sits inside a commercial strategy.
unicis-mcp-server (TypeScript MCP server, 9 tools)	Distributed as downloadable/installable component; run by the recipient (or by AI clients on the recipient's behalf)	**In scope**	Functions as an installable agent/client component per Commission guidance — the kind of downloadable software that pulls an otherwise-service offering back into product scope, independent of the hosted SaaS determination.

3.1 Classification (Annex III / IV check)

Neither CE nor the MCP server appear in Annex III (“important products with digital elements,” e.g. identity/access management software, password managers, standalone/embedded browsers, VPNs, SIEM, network management/configuration/monitoring tools, boot managers, PKI/certificate issuance software, operating systems) or Annex IV (“critical products,” e.g. hardware security modules, smart meter gateways, smartcards). A GRC/compliance task-and-controls platform does not fall within either list.

Conclusion: default (unclassified) category.

3.2 RDPS test applied to the hosted SaaS

Per the Commission's March 2026 draft guidance, a cloud/SaaS component is pulled into a product's conformity scope only if all three conditions of the "remote data processing solution" test are met: (1) the processing is designed and developed by, or under the responsibility of, the manufacturer; (2) it is necessary for the product to perform one of its functions; and (3) its absence would prevent that function. The hosted SaaS platform is not a remote dependency of a separately placed-on-market product — it is the entire offering, delivered as a service with no local install. It therefore does not meet the RDPS test in a way that would pull it into scope, and remains outside the CRA on the "pure SaaS" basis instead.

4. Conformity Route

For **Community Edition** and **unicis-mcp-server** (both default category, no harmonized standards yet cited for GRC-category software):

- **Conformity assessment procedure:** Internal control (Module A, CRA Annex VIII) — self-assessment. No notified body required.
- **Required artifacts:**
    1. Technical documentation per Annex VII (product description, design/development/production information, risk assessment, essential requirements mapping)
    2. EU Declaration of Conformity
    3. CE marking on the product/packaging/accompanying documentation
    4. Retention of documentation for **10 years**
- Once CEN/CENELEC/ETSI harmonized standards under standardisation request M/606 are cited in the Official Journal (horizontal standards expected ~30 August 2026, vertical standards ~30 October 2026), conformity against those standards gives a presumption of conformity under Article 27 and should be adopted where applicable.

Hosted SaaS carries no CRA conformity obligation under the current determination; it is tracked instead under Unicis's NIS2 compliance workstream (see Compliance Framework Roadmap).

5. Article 14 — Reporting Obligations (from 11 September 2026)

Independent of full conformity-assessment readiness, Article 14 reporting applies from 11 September 2026 to any in-scope product already on the market. This means **Community Edition and unicis-mcp-server incident/vulnerability handling must be explicitly covered**, with statutory deadlines:

- **24 hours** — early warning of actively exploited vulnerabilities / severe incidents to ENISA / national CSIRT
- **72 hours** — full notification
- **14 days** after a corrective measure is available — follow-up report (vulnerabilities)
- **1 month** — final report (severe incidents)

This workflow should be integrated with the existing IRIS incident-handling process and Grype/SBOM vulnerability scanning workstream, with CE and MCP-server releases explicitly in scope alongside the hosted platform's own NIS2-driven incident process.

6. Review Triggers

This determination should be re-assessed when any of the following occur:

- A CE or MCP-server release adds functionality that changes the RDPS analysis for the hosted SaaS (e.g. a hosted feature becomes a hard dependency for CE to function)
- Final Commission guidance (beyond the March 2026 draft) is published

- Harmonized standards under M/606 are cited in the Official Journal
- Any new distributable/installable component is introduced (desktop client, browser extension, mobile app, agent)
- At minimum, annually, alongside the existing MVSP/ISO 27001 control review cycle

7. References

- Regulation (EU) 2024/2847 (Cyber Resilience Act)
- European Commission, CRA Summary of the legislative text
- European Commission draft guidance, Communication Ares(2026)2319816 (3 March 2026)
- MVSP Implementation Overview
- Trust Center — Processes and Procedures