NIS2 Directive — Scope Determination

trust-center, compliance, nis2, cybersecurity, policies

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

1. Purpose

Directive (EU) 2022/2555 (NIS2) requires “essential” and “important” entities in listed sectors to implement cybersecurity risk-management measures and report significant incidents. This document records whether, and to what extent, Unicis Tech OÜ falls within NIS2 scope as a **direct regulated entity**, what obligations follow indirectly as a **supplier to NIS2-regulated customers**, and the trigger points that would change this determination.

2. Regulatory Basis

- **Directive (EU) 2022/2555** — in force since January 2023; transposition deadline 17 October 2024.
- **Estonia:** transposed via amendments to the Cybersecurity Act (*Küberturvalisuse seadus*), in force **1 January 2026**. No significant deviations from the directive's scope criteria. Self-registration for in-scope entities was due by 1 April 2026. Supervisory authority: **RIA** (Riigi Infosüsteemi Amet), acting as national CSIRT (CERT-EE).
- Scope test is two-part: (1) the entity operates in an Annex I (“essential,” high-criticality) or Annex II (“important,” other critical) sector, **and** (2) the entity meets the size threshold — medium (≥50 employees or >€10M turnover/balance sheet) or large (≥250 employees or >€50M turnover).
- A small set of categories are in scope **regardless of size**: qualified trust service providers, DNS service providers, TLD registries, certain public electronic communications providers, sole providers of a service essential to societal/economic activity in a Member State, and central public administration bodies. **Cloud computing service providers are not in this size-independent list** — they are subject to the standard threshold like other Annex I digital-infrastructure categories.

3. Scope Assessment

3.1 Sector test

The Unicis SaaS platform (platform.unicis.tech) is a cloud-hosted, browser-accessed software service. “Cloud computing service” under the EU's harmonised definition (Recital 33) is broad enough to capture SaaS, not only IaaS/PaaS.

Conclusion: sector test is met. Unicis sits within Annex I, Digital Infrastructure, “cloud computing service providers.”

3.2 Size test

Threshold	Requirement	Unicis Tech OÜ
Essential entity	≥250 employees or >€50M turnover/balance sheet	Not met
Important entity	≥50 employees or >€10M turnover/balance sheet	Not met
Size-independent category	N/A (cloud computing providers excluded from this list)	Not applicable

Unicis Tech OÜ's team consists of a small founder-led group plus part-time contractors engaged per project (technical development, EU-project/stakeholder management, marketing). This is well under both the micro-enterprise ceiling (10 employees / €2M) and the small-enterprise ceiling (50 employees / €10M) used by the size-cap rule.

Conclusion: size test is not met. Unicis Tech OÜ is not currently a directly regulated “important” or “essential” entity under NIS2, in Estonia or elsewhere in the EU.

4. Indirect Obligations (Supply-Chain Pressure)

Direct non-applicability does not mean no practical obligation. Article 21(2)(d) requires every NIS2-obligated entity to manage cybersecurity risk in its supply chain, including “security-related aspects concerning the relationships between each entity and its suppliers.” Since a substantial share of Unicis's own customer base consists of EU SMEs that **are** NIS2-obligated (important or essential entities in their own sectors), those customers are expected to:

- Request evidence of equivalent security practices from Unicis as a supplier (vendor security questionnaires, DPAs, security addenda)
- Factor supplier cybersecurity posture into their own Article 21 risk assessments
- In some cases, contractually require incident-notification cooperation from Unicis if a Unicis-side incident affects their NIS2-relevant data or operations

This is already partially addressed via the existing Vendor Questionnaires page (which covers Unicis's assessment of *its own* vendors) and the TPSRM page. The inbound direction — responding to customer NIS2-driven security questionnaires about Unicis itself — should draw on this document plus Section 5 below.

5. Article 21(2) Minimum Measures — Voluntary Adoption & Gap Check

Even without formal designation, Unicis adopts the Article 21(2) minimum measures voluntarily, both to satisfy indirect customer pressure (Section 4) and because the product's own value proposition depends on credible security practice (“dogfooding”). Status is cross-checked against the existing MVSP Implementation Overview.

#	Article 21(2) Measure	Status	Where evidenced
a	Risk analysis & information system security policies	Covered	MVSP Business Controls; Unicis Cybersecurity Controls module
b	Incident handling	Covered	IRIS incident management; MVSP “Incident handling” row
c	Business continuity, backup, disaster recovery, crisis management	Covered	Weekly encrypted backups, annual restore tests (MVSP Operational Controls)
d	Supply chain security	Partial	Vendor Questionnaires + TPSRM cover outbound vendor risk; inbound (responding to customer NIS2 questionnaires) not yet formalised as a repeatable process

#	Article 21(2) Measure	Status	Where evidenced
e	Security in system acquisition, development, maintenance incl. vulnerability handling/disclosure	Covered	SDLC page; Grype/SBOM scanning workflow; `security.txt` intake tracked in IRIS
f	Policies to assess effectiveness of risk-management measures	Partial	Annual MVSP self-assessment exists; no explicit NIS2-Article-21-mapped internal audit yet
g	Basic cyber hygiene & cybersecurity training	Covered	Unicis Awareness Module; OWASP Top 10 dev training
h	Cryptography and encryption policies	Covered	AES-256 at rest, TLS 1.3 in transit (MVSP Application Design Controls)
i	HR security, access control, asset management	Covered	RBAC + SSO + MFA, quarterly access reviews (MVSP Operational Controls)
j	MFA / continuous authentication, secured voice/video/text and emergency comms	Covered	MFA enforced via SSO (TOTP/YubiKey); Jitsi/Element for internal comms

Open items: formalise (d) an inbound customer-questionnaire response process, and (f) an explicit internal audit cycle mapped to Article 21 line items rather than relying solely on the MVSP annual self-assessment.

6. Incident Reporting Ladder (if ever in scope)

Should Unicis Tech OÜ cross the size threshold (Section 7), Estonia's implementation applies the standard NIS2 ladder via RIA/CERT-EE:

- **24 hours** — early warning
- **72 hours** — notification, including initial assessment and, where applicable, indicators of compromise
- **1 month** — final report

Governance: a management body member (or the full board, if none is designated) must formally approve and oversee the risk-management measures and can be held personally liable for material failures — Estonia's implementation is explicit on this point.

7. Review Triggers

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

- Headcount reaches ~40–50, or annual turnover approaches €10M — reassess against the “important entity” threshold well before crossing it, given the 3-year phase-in window starts from the date the threshold is crossed
- Unicis begins providing managed/outsourced ICT services on customers' behalf (which could additionally trigger the “ICT service management (B2B)” Annex I category)
- A customer or prospect formally requests a NIS2 supplier-risk assessment or security addendum — log the request and confirm the response against Section 5
- RIA publishes further guidance affecting the cloud-computing-provider size-independent question
- At minimum, annually, alongside the existing MVSP/ISO 27001 control review cycle

8. References

- Directive (EU) 2022/2555 (NIS2), Articles 2, 3, 20, 21, 23, Annexes I & II
- Estonian Cybersecurity Act (Küberturvalisuse seadus), as amended, in force 1 January 2026
- Riigi Infosüsteemi Amet (RIA) — national NIS2 competent authority and CSIRT
- CRA Scope Determination

- MVSP Implementation Overview
- Vendor Questionnaires
- TPSRM