NIS2 · SUPPLIER ASSURANCE · PRACTITIONER CHECKLIST

Article 21(2)(d) — the five evidence artefacts

> "supply chain security, including security-related aspects concerning the relationships between each entity and its **direct suppliers or service providers**" — Article 21(2)(d), Directive (EU) 2022/2555

The directive leaves the *how* open — measures "appropriate" to the risk. Across early competent-authority guidance and auditor questions, the operational baseline collapses to five artefacts. For each, the questions an auditor asks. If you can answer all of them without a reconstruction exercise, you hold the defensible core of the clause.

ARTEFACT 01

A maintained supplier inventory, tagged by service and data

- [ ] Can you produce a current list of every supplier touching regulated services — with the service named and the data classification tagged?
- [ ] Are the sub-processors of your top-tier suppliers listed separately?
- [ ] Is there one owner and one system of record — not a CSV in someone's inbox?

Owner ..... System of record ..... Next review .....

ARTEFACT 02

A documented risk classification

- [ ] Does every supplier carry a documented tier — by data sensitivity, service criticality, and replaceability?
- [ ] Is each tier assignment signed and dated by a named reviewer?
- [ ] Does assessment depth scale with tier — and is the lighter touch documented, not absent?

Owner ..... System of record ..... Next review .....

ARTEFACT 03

Per-supplier assessment evidence on a known cadence

- [ ] For each supplier: what did you ask, what did they answer, what evidence did they provide (SOC 2, ISO 27001, sub-processor list, BCP results)?
- [ ] Is each artefact dated, current, and attributed to the reviewer who accepted it?
- [ ] Is the next review date on a calendar someone owns?

Owner ..... System of record ..... Next review .....

ARTEFACT 04

A defensible decision trail

- [ ] Could you show — three years later, after staff turnover — who approved this supplier, on what evidence current at the time, and when?
- [ ] Are decisions timestamped and tamper-evident?
- [ ] Do rejections and escalations leave the same trail as approvals?

Owner ..... System of record ..... Next review .....

ARTEFACT 05

A reaction plan for material change

- [ ] Which events trigger an out-of-cycle review — supplier breach disclosure, certificate expiry, sub-processor addition, change of ownership?
- [ ] Does each trigger have a named owner and a completion target?
- [ ] When did one last actually fire — and is that on record?

Owner ..... System of record ..... Next review .....

____ / 15 **Count your checked boxes.** Anything unchecked is a gap — and each gap needs a named owner and a next review date, not a note to revisit it someday.

Next step: score yourself against all five artefacts in about ten minutes with the readiness check at `shardscybersecurity.io/nis2-readiness-check` — free, no email needed.

Sources: Directive (EU) 2022/2555, Article 21(2)(d) and Recital 85 (EUR-Lex) · ENISA NIS2 Technical Implementation Guidance v1.0. This checklist supports your Article 21(2)(d) work; it is not legal advice, and no tool makes you NIS2 compliant — compliance is the entity's decision and the auditor's judgement.

Vittnor by Shards Cybersecurity
`shardscybersecurity.io/nis2/article-21-2-d`
v1.1 · August 2026