

NIS2 supplier review kit

Four steps to a supplier register you can defend: which suppliers matter, how much risk each one brings, what evidence you hold, and what you decided. One checklist per step, a one-page policy to fill in, and an Excel file for the register itself.

"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 (emphasis added)

1

Tick what you can already show, on this page.

2

Work through steps 1 to 4, on pages 2 to 5; page 7 links an Excel file to record them in.

3

Write your supply chain security policy on page 6, or build it online as a Word file.

4

Come back to this page and count again.

The guide for each step: shardscybersecurity.io/nis2/supplier-review-kit

The five evidence artefacts

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, in our judgement. 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. The four steps in this kit help you build all five.

ARTEFACT 01

Step 1

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 spreadsheet in someone's inbox?

ARTEFACT 02

Step 2

A documented risk classification

- ☐ Does every supplier carry a documented tier, set by its strongest single risk?
- ☐ 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?

ARTEFACT 03

Step 3

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, continuity test results)?
- ☐ Is each artefact dated, current, and attributed to the reviewer who accepted it?
- ☐ Is the next review date on a calendar someone owns?

ARTEFACT 04

Step 4

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?

ARTEFACT 05

Step 4

A reaction plan for material change

- ☐ Which events trigger an out-of-cycle review — an incident the supplier reports, 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?

___ / 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.

Which suppliers matter

Start from the whole list, then keep the suppliers that matter for your cybersecurity. Anything you leave out needs a reason you can show later.

Build the list

- ☐ Every supplier is on it. Good places to look: accounts payable, your contract register, your GDPR processor list, the apps connected to your identity provider, and the accounts used for remote access.
- ☐ Each supplier has one owner on your side.
- ☐ For each one, you know what kind of supplier it is and which services it provides. If one supplier gives you very different services (say, hosting and payroll), treat each service on its own.

Decide what is in scope: five questions

Question	Counts as in scope when...
1. Which of your data can it see or hold?	personal, confidential or internal data
2. Does it have access to your systems?	any access, limited or privileged
3. Would an outage or incident there disrupt your operations or the services you provide?	yes
4. Does it supply software, devices or updates that run in your systems?	yes
5. Does a contract, a customer or another law require you to assess it?	yes, for example as a GDPR processor

One answer that counts as in scope makes the supplier in scope.

Not sure about question 3? On its own, "not sure" doesn't make the supplier in scope. Note it, and find out.

- ☐ All five questions are answered for every supplier, or for every service you treat on its own.
- ☐ Each one is marked in scope or out of scope.
- ☐ Every "out of scope" has a written reason. So does any supplier you mark in or out against what its answers say.

New suppliers too

Run the same four steps before you sign a new supplier, while the contract is still open for discussion.

Notes

How much risk each supplier brings

For each supplier in scope, answer twelve questions, then set a tier: Low, Medium, High or Critical.

Twelve questions in six areas · the choices run from least to most risk, except "Not known yet"

Availability: how much you rely on it

1. How much do your operations, or the services you provide, rely on it?

Not significantly · Low · Material · Full

2. How long could you keep operating if it stopped?

More than a week · 1 to 7 days · Less than a day · Less than 4 hours

Confidentiality: what it can see

3. What is the most sensitive data it can see or hold?

None, or only public · Personal · Confidential business · Special categories of personal data

4. Roughly how many records about people or customers does it hold for you?

None · Fewer than 1,000 · 1,000 to 100,000 · More than 100,000

5. Which of your credentials, keys or secrets does it hold or manage?

None · End-user credentials only · Service credentials with limited scope · Admin credentials or encryption keys

Privileged access: what it can do in your systems

6. What access does it have to your network?

None · Limited or scoped · Privileged or persistent

Privileged access (continued)

7. What access does it have to your identity or cloud administration?

None · Limited, scoped permissions · Admin-level permissions

8. Does it put software, devices, updates or changes into your systems?

No · Yes, you review and install them · Yes, it changes them itself · Yes, automatically and with admin rights

Supply chain: who stands behind it

9. Does it rely on other companies to deliver this service, and do you know who they are?

No · Yes, and we know who · Yes, but we know only some, or it won't say · Not known yet

Jurisdiction: where your data and support sit

10. Where is your data stored or processed, and where is support or admin access provided from?

Only the EU/EEA · Also countries with an EU adequacy decision · Also other countries · Not known yet

Resilience: how replaceable it is

11. How long would it take to replace it?

Less than 3 months · 3 to 12 months · 12 to 24 months · More than 24 months, or no way out

12. Could another supplier take over?

We already use more than one · Yes · Only a few, or switching is hard · No realistic alternative

How to set the tier

The strongest single risk sets the tier, not an average. One serious answer, such as admin rights in your systems or full reliance on the service, is enough for High or Critical, and five good answers don't hide it.

Your tiers depend on your circumstances. The same supplier can be Low for one company and Critical for another, because the tier comes from your answers about your data, your access and how much you rely on it. What has to hold is consistency: the same answers give the same tier across your register, and every tier has its reason on record. A tier is your own risk rating, not a legal category: national law may define its own — check your country's rules (the online guide links them; see page 1). Worked examples, not rules: in the online guide (see page 1).

Checklist

- ☐ The twelve questions are answered for every supplier in scope, using "not known yet" (questions 9 and 10) where you need to find out, rather than guessing. A supplier that refuses to say gives the riskier answer.
- ☐ Every supplier in scope has a tier, set by its strongest single risk, with what set it in one line.
- ☐ Who set each tier, and when, is recorded.

Start with what you already hold

Read the contract first. Then check what is on file and what the supplier publishes. Ask the supplier only for what is still missing.

1. Read the contract against eight terms

These are the contract terms listed in Implementing Regulation (EU) 2024/2690, Annex point 5.1.4. That regulation binds only the provider types it names, such as cloud, data centre, DNS, managed service and trust service providers, and even for them each term applies "where appropriate". Austria goes further: since 2 October 2026, its NISV 2026 ordinance applies the same terms, "where appropriate" included, to every essential and important entity. For everyone else they are a useful reference: NIS2 Recital 85 encourages building security into supplier contracts. Check your national law too (the online guide links your country's rules; see page 1).

- | | |
|--|--|
| ☐ Security requirements for the supplier | ☐ The right to audit, or to receive audit reports |
| ☐ Supplier staff: awareness, skills, training, certifications | ☐ Vulnerability handling by the supplier |
| ☐ Background checks on the supplier's staff | ☐ Subcontracting rules and subcontractor security duties |
| ☐ Incident notification without undue delay | ☐ Exit duties, such as retrieval and disposal of your information |

A current contract may lack some of these. Plan to add them at the next renewal: note the renewal date, and record the fix as a condition of your decision in Step 4.

2. Check what is on file and what the supplier publishes

For every document: does it cover the service you buy, is it current, and who stands behind it?

- | | |
|--|---|
| ☐ ISO/IEC 27001 certificate: does the scope name your service? Is it valid, to the 2022 edition, from an accredited body? Look it up in the certification body's register or in IAF CertSearch, the global database of accredited certificates. | ☐ Penetration test summary: what was tested, when, by an independent tester, and were serious findings fixed and checked again? |
| ☐ Assurance report (SOC 2, ISAE 3000 or 3402, BSI C5): Type 2? An unmodified (clean) opinion? Your service in the description? Read the exceptions, any carved-out sub-suppliers, and the controls it expects you to run. For the months since, a bridge letter. | ☐ Sub-processor list (the sub-suppliers that handle your data): who, what, where, and how you are told about changes. |
| | ☐ Automotive: TISAX labels, shared through the European Network Exchange (ENX) portal. Check the locations, the objectives and the expiry date. |

3. Ask only for what is still missing, and record where each answer came from

- ☐ The contract is read against the eight terms for every supplier in scope, and gaps are noted.
- ☐ What you hold and what the supplier publishes was checked before asking.
- ☐ What you ask for matches the supplier's tier: lighter for Low, fuller for High and Critical.
- ☐ Every answer has a source (your own records, or the supplier), a date, and the name of whoever accepted it.
- ☐ The supplier's security and incident contact is on record.

A decision you can defend later

Three years from now, after staff turnover, the record still has to show who decided, on what evidence current at the time, with what conditions, and when you planned to look again.

Record a decision for every supplier in scope

Decision	When it fits
Approved	The evidence covers what the tier needs.
Approved with risk	You accept a known gap, with conditions, an owner and a date. For a supplier the business depends on and can't drop, approving with conditions and a plan for how you would replace it is a defensible answer.
Rejected	The risk is too high, and there is a way out.

- ☐ Every supplier in scope has a decision for the current period, with the reason in a sentence or two.
- ☐ Each condition has an owner and a date. For example: add the audit clause at the March renewal (owner: IT manager).
- ☐ Who decided, when, and the next review date are recorded.
- ☐ Earlier decisions are kept. Each review adds a new one, so the history stays.

Who may accept risk

Name it in your policy, tier by tier. For High and Critical, we suggest the management body: Article 20 of NIS2 has it approve the cybersecurity risk-management measures and oversee how they are carried out.

When to look again early

- ☐ A security incident at the supplier
- ☐ An expired certificate or audit report
- ☐ A new sub-supplier
- ☐ A change of ownership
- ☐ An EU-level risk assessment of a critical supply chain that covers what it provides (NIS2 Articles 21(3) and 22(1))
- ☐ A contract renewal, or the end of the relationship

Give each trigger an owner, and a date by which the early review is done.

When a supplier leaves

- ☐ Its access is revoked.
- ☐ The retrieval and disposal of your information is confirmed, as the contract's exit term says.
- ☐ The end date is recorded, and its records are kept for the history.

Notes

Supply chain security policy

Organisation _____

Policy owner _____

Approved by (management body) _____

Approved on _____

Next review of this policy _____

Version _____

- 1

Purpose. This policy sets how we manage the cybersecurity of our relationships with our direct suppliers and service providers (NIS2, Article 21(2)(d)).
- 2

Our role in the supply chain. We are _____ *e.g. an important entity in energy, and a supplier to regulated customers.* We tell our direct suppliers about this role by _____ *e.g. a clause in new contracts.*
- 3

Which suppliers are in scope. We keep a register of our direct suppliers and service providers, with a contact point for each and what it provides to us. A supplier is in scope when it can see more than public data, has any access to our systems, our operations depend on it, it supplies software, devices or updates that run in our systems, or a contract, a customer or a law requires an assessment. Every out-of-scope decision is recorded with a reason.
- 4

Choosing new suppliers. Before signing, we look at the supplier's cybersecurity practices (including secure development), its ability to meet our security requirements, the overall quality and resilience of what it supplies (including the security measures built into it), and whether we can avoid depending on it alone. We also check: _____
- 5

How we rate risk. Each supplier in scope gets a tier (Low, Medium, High or Critical) from twelve questions in six areas (availability, confidentiality, privileged access, supply chain, jurisdiction and resilience), with the answers kept in _____ *e.g. our supplier register.* The strongest single risk sets the tier, not an average. We rate each supplier by how we use it, and record the reason for every tier.
- 6

Tier	What we check	Who may accept risk	Review every
Low	<i>e.g. the contract terms</i>		
Medium			
High			
Critical	<i>e.g. the contract terms, certificates, audit reports, a penetration test</i>		
- 7

When we review early. A security incident at the supplier, an expired certificate or audit report, a new sub-supplier, a change of ownership, an EU-level risk assessment of a critical supply chain that covers what it provides, a contract renewal, or the end of the relationship. Each trigger has an owner. Between reviews, we read suppliers' service level reports, where there are any, and look into incidents involving what they provide; we record whether either calls for an early review or a change to this policy.
- 8

Contracts. New and renewed contracts cover the contract terms listed in Implementing Regulation (EU) 2024/2690, Annex point 5.1.4, where appropriate. Gaps in current contracts are fixed at renewal and tracked as conditions.
- 9

When a supplier leaves. We revoke its access, confirm the retrieval and disposal of our information, and record the end date. Records are kept.

About this kit

Made by Shards Cybersecurity, the team behind Vittnor — Supply Chain Assurance for the mid-market.

Version	1.2, last reviewed 20 October 2026
Changes	20 October 2026 · Version 1.2 · Added the policy builder: the policy, filled in for your organisation from four short steps, as a Word file. It replaces the Word file of versions 1.0 and 1.1. 20 October 2026 · Version 1.1 · Added the supplier register as an Excel file. 20 October 2026 · Version 1.0 · First published.
Licence	CC BY 4.0: creativecommons.org/licenses/by/4.0 Free to use inside your organisation, and to show to your auditors and suppliers. If you publish it or hand it out as a template, keep the credit line and say what you changed.
Credit line	Vittnor by Shards Cybersecurity · shardscybersecurity.io · version 1.2 · last reviewed 20 October 2026
Guides and updates	The guide for each step and the latest version of the kit: shardscybersecurity.io/nis2/supplier-review-kit Useful? Follow Shards Cybersecurity on LinkedIn to hear when a new version is out: linkedin.com/company/shardscybersecurity
Other files	The policy on page 6 can also be built online and downloaded as a Word file: shardscybersecurity.io/nis2/supplier-review-kit/policy The register is also available as an Excel file: shardscybersecurity.io/downloads/nis2-supplier-review-kit-register-v1.2.xlsx
Sources	Directive (EU) 2022/2555, Article 21(2)(d) and Recital 85 (EUR-Lex) · European Union Agency for Cybersecurity (ENISA) NIS2 Technical Implementation Guidance v1.0.
Disclaimer	This kit supports your Article 21(2)(d) work; it is not legal advice. It lists contract terms to look for, but doesn't judge whether a contract is adequate. No tool or template makes you NIS2 compliant — compliance is the entity's responsibility, and the competent authority and your auditors judge it.