Aona

NIS2 AI supplier dossier

Security leaders, legal teams and procurement at potentially covered EU entities

Read the complete guide on aona.ai

NIS2 is a directive implemented through national law. First establish the entity, sector, size and relevant jurisdiction, then assess the AI supplier's role and risks under the applicable requirements. Article 21 includes direct-supplier security, but a generic AI subscription does not establish the customer's or vendor's legal status.

A fictional manufacturing company evaluates an external drafting service. The dossier keeps the applicability decision separate from supplier-control evidence.

Synthetic company, staffing figures, supplier and proposed use. No actual national-law classification, supplier audit or test result is represented.

Your review

Reviewer: _____ Date: _____

Organisation or team: _____

☐ **Resolve jurisdiction and entity facts**

Identify actual national implementation, sector, size/group and service-specific conditions.

☐ **Evaluate the direct supplier**

Ask for relevant secure-development, vulnerability, incident and access-control evidence.

☐ **Document scope and follow-up**

Separate the legal conclusion, supplier evidence and observed control results with accountable owners.

Checked items record your review, not a compliance approval or an installed-product test result.

Notes and next actions

Decision and scope: _____

Evidence to collect: _____

Owner and next review date: _____

Review matrix

Dossier field	Populated fictional fact	Evidence or decision needed
Entity and establishment	Example Components SAS, established in France, 300 staff in the exercise.	Legal owner verifies the actual sector, size/group rules and French implementing requirements.
Proposed service	External AI drafting for internal support instructions.	Business owner records the task, users and permitted data.

Dossier field	Populated fictional fact	Evidence or decision needed
Connection and data	Initial proposal includes repository access; first evaluation removes that connection.	Security verifies actual permissions and data paths before any real deployment.
Supplier security	No verified development, vulnerability or incident evidence exists in the fictional proposal.	Procurement obtains service-specific evidence and assigns follow-up questions.
Continuity and dependency	Manual drafting is available in the example.	Operational owner assesses real outage effects rather than assuming the fallback settles risk.
Applicable duties	Entity/national-law conclusion is not established by this exercise.	Record the actual legal basis and any sector-specific interaction before claiming compliance.
Interim decision	Use invented instructions only while material questions are resolved.	Do not represent the teaching evaluation as approval for real company data.

Two parallel questions

- **Applicability:** Entity, activities, country and national law
- **Supplier risk:** Service, access, vulnerabilities and dependency
- **Decision:** Actual scope, controls, owners and evidence

Fictional evidence requests

- Legal: which national implementation and entity criteria govern Example Components SAS?
- Procurement: which legal supplier and service terms apply, including onward dependencies?
- Security: what access does the repository connection grant, and can the initial task run without it?
- Operations: what happens if the drafting service becomes unavailable or produces an incorrect result?

Teaching disposition

Restrict this exercise to invented internal instructions with no repository connection. Obtain actual legal and supplier evidence before a real-data decision. No national law or supplier assurance has been invented for the scenario.

Sources and scope

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information, not professional approval or a completed control test. It does not classify an entity under NIS2, certify a supplier or replace the broader risk-management programme.

NIS2: Directive (EU) 2022/2555. Directive scope and Article 21 risk-management and direct-supplier security considerations, implemented through applicable national law.