

— TEMPLATE · TOMORIS TOOLBOX

Supplier Security Questionnaire: Template for NIS2 and the Supply Chain

Questions on organization, technology, incidents and contract termination, with classification, supplier register and contract points under Implementing Regulation (EU) 2024/2690

UPDATED

Oct 25, 2026

LENGTH

PDF, 8 pages

ONLINE

tomoris.com/en/downloads/lieferanten-sicherheitsfragebogen

AT A GLANCE

point (d)

§ 32 para. 4 NISG 2026:
supply chain security

8

contract points under the
IR, Annex point 5.1.4

22

questions to fill in, in three
parts

annually

review of the policy
according to ENISA
guidance

WHO IT IS FOR

- Procurement and contract management who select IT service providers and suppliers
- Information security officers of essential and important entities
- Management responsible for the risk management measures
- Suppliers who answer such questionnaires and want to prepare

WHAT THIS COVERS

Supply chain security is one of the minimum measures under § 32 NISG 2026 (Austrian Network and Information Systems Security Act 2026), and Implementing Regulation (EU) 2024/2690 describes in detail what entities must regulate when selecting their suppliers, in the contract and in ongoing reviews. This template turns that into a questionnaire you can send to IT service providers, software vendors and suppliers: with questions on organization, technology, incidents and contract termination, a classification of suppliers by criticality, a register to fill in and the eight contract points of the Implementing Regulation. It uses ENISA's implementation guidance of June 2025.

This template must be adapted to your entity, your suppliers and your risks and does not replace legal advice. The questions and the classification are TOMORIS recommendations. The NISG 2026, the NISV 2026 and Implementing Regulation (EU) 2024/2690 as currently in force are authoritative; for data processing agreements (DPAs), also Art. 28 GDPR.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01	What the NISG 2026 and the Implementing Regulation require	2
02	Classifying and recording suppliers	3
03	Questionnaire part 1: organization and evidence	4
04	Questionnaire part 2: technology and operations	5
05	Questionnaire part 3: incidents, audits, contract termination	6
06	Evaluating and following up on answers	7
07	Contract points under IR Annex point 5.1.4	7
08	Sources	8

01 —

What the NISG 2026 and the Implementing Regulation require

The supply chain as a mandatory measure and the details of the Implementing Regulation

Essential and important entities must address supply chain security, including the relationships with their direct suppliers and service providers, taking into account their vulnerabilities, the quality of their products and their cybersecurity practices, including secure development (§ 32 para. 4 lit. d NISG 2026, Art. 21(2)(d) and (3) NIS2 Directive). ENISA points out that NIS2 only covers direct first-tier suppliers.

IR Annex points 5.1.1 to 5.1.3

Establish a supply chain security policy, communicate your own role in the supply chain to suppliers, define selection criteria: cybersecurity practices and secure development, ability to meet requirements, quality and resilience of products, possibility of diversifying sources of supply; where applicable, take into account the EU coordinated risk assessments of critical supply chains.

IR Annex point 5.1.4

Specify eight points in contracts where appropriate, from security requirements through incident reporting and audit rights to obligations at contract termination (see section 07).

IR Annex points 5.1.6 and 5.1.7

Review the policy and assess changes in suppliers' security practices, in case of significant changes or significant incidents; track reports on service level agreements, review incidents involving suppliers' products, document unplanned reviews.

IR Annex point 5.2

Register of direct suppliers with contact points and the ICT products, services and processes provided, kept up to date.

IR Annex point 6.1.2

On acquisition: security requirements, security updates throughout the entire lifetime, information on hardware and software components and security functions, assurance and evidence of compliance.

§ 2 and § 3 NISV 2026 (Austrian NIS Regulation 2026)

The Annex of the Implementing Regulation applies to all essential and important entities; risks in the ICT supply chain are one of the four risk categories that the risk analysis must at least be based on.

Which questions you ask and how you classify suppliers is a TOMORIS recommendation based on the Implementing Regulation and ENISA guidance. The contents of § 32 NISG 2026 and the Implementing Regulation are mandatory to the extent they apply to your entity. Processing personal data on behalf of a controller also requires a contract or other legal act under Art. 28(3) GDPR.

02

Classifying and recording suppliers

Scope of review by supplier criticality, register under IR point 5.2

Not every supplier requires the same effort. Among other criteria, ENISA lists the sensitivity of the products and services procured, the supplier's ability to ensure supply, its history of security incidents and the risk of dependency (lock-in). From this, TOMORIS derives three tiers:

Classification (TOMORIS recommendation)

TIER	TYPICAL SUPPLIERS	SCOPE OF REVIEW
High	Remote access to your systems, operation of important services, cloud with sensitive data, IT service providers with administrator rights	Full questionnaire with evidence, contract points under point 5.1.4, annual review

Medium	Software and devices for important processes without permanent access	Parts 1 and 2 plus incident reporting and contract termination
Low	Standard products without access and without sensitive data	Basic details in the register, review when there is cause

Register of direct suppliers (IR Annex point 5.2, to fill in)

SUPPLIER	CONTACT POINT	PRODUCTS, SERVICES	TIER
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

03 —

Questionnaire part 1: organization and evidence

Who is responsible at the supplier and what they can prove

Questionnaire from [company] to [supplier], completed by [name, function] on [MM/DD/YYYY]. Please answer every question and provide evidence, such as a document, certificate or audit report.

Part 1: Organization

NO.	QUESTION	ANSWER	EVIDENCE
1.1	Who is responsible for information security at your company (name, function, contact)?	_____	_____
1.2	Do you have a documented security policy or management system? Which certifications do you hold, with what scope and valid until when?	_____	_____
1.3	Are you yourself an essential or important entity under NIS2, or do your products fall under the Cyber Resilience Act?	_____	_____
1.4	Who owns your company, and which jurisdiction are you subject to?	_____	_____
1.5	Have you had security incidents affecting customers in the last three years? What did you change as a result?	_____	_____
1.6	How do you train your employees in security, and what qualifications do the people working for us have?	_____	_____
1.7	Do you screen the employees who have access to our systems or data?	_____	_____
1.8	Do you use subcontractors? Which ones, where, and do the same security requirements apply to them?	_____	_____

Basis: selection criteria and certifications, training and background checks, subcontractors (IR Annex points 5.1.2 and 5.1.4(b), (c), (g)); ENISA lists jurisdiction, ownership, incident history and regulation under NIS2 or the Cyber Resilience Act as criteria.

04

Questionnaire part 2: technology and operations

Access, vulnerabilities, development, data and resilience

Part 2: Technology and operations

NO.	QUESTION	ANSWER	EVIDENCE
2.1	How do you access our systems? With personal accounts, multifactor authentication and logging?	_____	_____
2.2	How do you learn about vulnerabilities in your products or services, and within what time frame do you fix them?	_____	_____
2.3	How long do you provide security updates, and how do you announce the end of support?	_____	_____
2.4	Do you develop software? Following which rules for secure development and testing?	_____	_____
2.5	Can you disclose the hardware and software components used, for example as a software bill of materials (SBOM)?	_____	_____
2.6	What security functions does your product have, and is the secure configuration documented?	_____	_____
2.7	Where is our data stored and processed? Will you notify us in advance if this changes?	_____	_____
2.8	How do you encrypt data in transit and at rest?	_____	_____
2.9	How do you back up data, how often do you test restores, and is there a contingency plan for your service?	_____	_____

Basis: security requirements, updates throughout the lifetime, components and security functions on acquisition (IR Annex point 6.1.2), remediation of vulnerabilities (point 5.1.4(f)), remote access by service providers (point 6.7.2(d)), multifactor authentication, cryptography and business continuity (§ 32 para. 4 lit. j, h and c NISG 2026); ENISA recommends storage and processing locations as contract content.

05 —

Questionnaire part 3: incidents, audits, contract termination

What applies in an emergency and how the collaboration ends

Part 3: Incidents and contract

NO.	QUESTION	ANSWER	EVIDENCE
3.1	Will you report security incidents that endanger our systems to us without undue delay? Through which channel and to whom?	_____	_____
3.2	Will you support us in an incident caused by your product or service, and on what terms?	_____	_____
3.3	Do you grant an audit right, or do you provide audit reports?	_____	_____
3.4	Will you inform us about developments that could significantly impair your service?	_____	_____
3.5	What happens to our data when the contract ends: return, deletion, confirmation? How do you support the transition?	_____	_____

Confirmation

FIELD	ENTRY
Completed by (name, function)	_____
Date, signature	_____
Contact person for questions	_____

Basis: incident reporting, audit rights and obligations at contract termination (IR Annex point 5.1.4(d), (e), (h)); ENISA lists support during incidents, notification of significant changes and exit as additional contract content.

06 —

Evaluating and following up on answers

From the completed questionnaire to a documented decision

1

Check plausibility

Compare answers with the evidence; check certificates for scope and validity. Request missing answers.

2

Assess the risk

Take the selection criteria into account in selection and contract award (IR point 5.1.5); where appropriate, carry out and record a risk analysis before concluding the contract (ENISA on 5.1.5).

3

Close gaps

Address deviations through contract clauses, service level agreements or your own safeguards, such as restricted access. If that is not possible, consider alternatives.

4

Decide and document

Record approval, conditions or rejection with reasons and the people responsible; enter the supplier in the register.

5

Monitor continuously

Track performance reports, review incidents involving the supplier's products, assess the need for unplanned reviews (IR Annex point 5.1.7), for example after incidents, significant changes or contract breaches (ENISA); according to ENISA, review the policy at least annually.

For the self-declaration to the cybersecurity authority, information on supply chain security in particular must be submitted (§ 33 para. 1 NISG 2026). Completed questionnaires, assessments and the register provide a good basis for this.

07 —

Contract points under IR Annex point 5.1.4

What contracts with suppliers should specify where appropriate

- ☐ a) Cybersecurity requirements for the supplier, including the requirements on acquisition under point 6.1.
- ☐ b) Requirements for awareness, skills and training and, where appropriate, certifications of the supplier's employees.
- ☐ c) Requirements for background checks of the supplier's employees.
- ☐ d) Obligation to report without undue delay security incidents that present a risk to your systems.

- ☐ e) Right to audit or to receive audit reports.
- ☐ f) Obligation to remediate vulnerabilities that present a risk to your systems.
- ☐ g) Rules on subcontracting; where permitted, security requirements for subcontractors.
- ☐ h) Obligations at contract termination, such as the return and disposal of information obtained.

For large suppliers whose contracts can hardly be negotiated, ENISA suggests alternatives: joint procurement with similar organizations, representation through an industry association, suppliers with published security commitments or recognized certifications, model contracts from public bodies and a short list of alternatives.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)

tomoris.com/tools/nis2-check

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

08

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **NISG 2026, BGBl. I No. 94/2025, version in force in the RIS**
§ 32 para. 4 lit. c, d, h, j and § 33 para. 1, accessed October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=105061000
- 2 **Directive (EU) 2022/2555 (NIS2 Directive), German version on EUR-Lex**
Art. 21(2)(d) and (3), accessed October 25, 2026
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- 3 **Implementing Regulation (EU) 2024/2690, German version on EUR-Lex**
Annex points 5.1, 5.2, 6.1.2 and 6.7.2, accessed October 25, 2026
eur-lex.europa.eu/eli/reg/2024/2690/oj/deu
- 4 **NISV 2026, BGBl. II No. 290/2026**
§ 2 applicability of the IR, § 3 risk categories, accessed October 25, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 5 **GDPR, German version on EUR-Lex**
Art. 28(3), accessed October 25, 2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 6 **ENISA: Technical Implementation Guidance, Version 1.0 (June 2025)**
Chapter 5 Supply Chain Security, accessed October 25, 2026
www.enisa.europa.eu/publications/nis2-technical-implementation-...
- 7 **ENISA: Good Practices for Supply Chain Cybersecurity (June 2023)**
Executive Summary and Section 2.1, accessed October 25, 2026
www.enisa.europa.eu/publications/good-practices-for-supply-chain-...