NIS2 supplier questionnaire

Note
Questions for suppliers and service providers on supply chain security, a measure under Section 30 (2) no. 4 BSIG (Art. 21 (2) (d) NIS2). Question depth: ask every supplier the core questions, add the standard questions for medium criticality and the extended questions for high criticality. Answers: yes / partly / no; for free-text questions a short statement in the comment column. The questionnaire is a working aid; whether it fully covers your duties depends on your company and your suppliers.

Organization and responsibility

No.	Question	Suitable evidence	Answer	Evidence / comment
1	Is your company itself classified as an important or essential entity under NIS2 or the BSIG and registered with the BSI? Art. 3 NIS2 Directive; § 28 BSIG · Core question	No document needed. State the classification in the answer text; on request the BSI registration confirmation without identifiers is enough.		
2	Has your management been trained on cybersecurity risks in the last 24 months? Art. 20(2) NIS2 Directive · Extended question	Attendance confirmation or training record for management with date (at most 24 months) and topic.		
3	Do employees with security tasks receive regular training on cyber hygiene and current threats? Art. 21(2)(g) NIS2 Directive · Standard question	Training record with date (at most 12 months), target group and topic.		
4	Have you accepted our security requirements by contract (for example as an annex or SLA)? Art. 21(2)(d) NIS2 Directive; § 30(2), no. 4 BSIG (German BSI Act) · Core question	Contract or annex extract with our security requirements and signature or acceptance.		
5	Do you grant us or an appointed auditor the right to verify the security requirements? Art. 21(2)(d) NIS2 Directive · Standard question	Contract clause on the audit right.		

Risk and policies

No.	Question	Suitable evidence	Answer	Evidence / comment
6	Have you implemented cybersecurity risk management measures that your management has approved? Art. 20(1) NIS2 Directive; Art. 21(1) NIS2 Directive · Core question	Overview of measures or policy with management approval and date (at most 24 months).		

No.	Question	Suitable evidence	Answer	Evidence / comment
7	Do you check at least annually whether your security measures are effective (for example internal audit or metrics)? Art. 21(2)(f) NIS2 Directive · Standard question	Audit or review report with date (at most 12 months) and result.		

Incidents and reports

No.	Question	Suitable evidence	Answer	Evidence / comment
8	Do you report to us a significant security incident affecting our service within 24 hours of detection? Art. 23(4)(a) NIS2 Directive; § 32 BSIG (German BSI Act) · Core question	Contract clause or SLA with a 24-hour notification deadline and notification route.		
9	Do you provide us with an initial assessment (severity, impact, indicators of an attack) within 72 hours? Art. 23(4)(b) NIS2 Directive; § 32 BSIG (German BSI Act) · Core question	Contract clause with a 72-hour deadline and the content of the initial assessment.		
10	Do we receive a final report with cause and measures taken within one month? Art. 23(4)(d) NIS2 Directive; § 32 BSIG (German BSI Act) · Standard question	Contract clause on the final report within one month.		
11	Is there an emergency contact for security incidents reachable around the clock? Art. 21(2)(b) NIS2 Directive · Extended question	No document needed. State the phone number or address and the availability in the answer text.		

Access and identities

No.	Question	Suitable evidence	Answer	Evidence / comment
12	Is every access to our systems protected by multi-factor authentication and personalized? Art. 21(2)(j) NIS2 Directive · Core question	Screenshot of the MFA requirement for access to our systems (VPN, remote maintenance tool), date visible (at most 12 months).		
13	Does remote access to our systems take place only after our approval, and can we switch it off at any time? Art. 21(2)(i) NIS2 Directive · Standard question	Process description for the approval of remote access with approval date (at most 24 months).		
14	Are administrator accesses to our systems personalized, time-limited and restricted to what is necessary? Art. 21(2)(i) NIS2 Directive · Standard question	Report or screenshot on personalized, time-limited admin accounts with date (at most 12 months).		

No.	Question	Suitable evidence	Answer	Evidence / comment
15	Are persons with access to our systems vetted before deployment and deregistered immediately when they leave? Art. 21(2)(i) NIS2 Directive · Extended question	Policy extract on vetting and leaving with approval date (at most 24 months).		

Operations, patches and vulnerabilities

No.	Question	Suitable evidence	Answer	Evidence / comment
16	Are your accesses to our systems logged, and do you provide us with the logs on request? Art. 21(2)(b) NIS2 Directive · Standard question	Screenshot of session logging with date (at most 12 months).		
17	Is there a procedure for receiving, assessing and remedying vulnerability reports in a coordinated way? Art. 21(2)(e) NIS2 Directive · Core question	Process description with intake, assessment, deadlines and approval date (at most 24 months).		
18	Are security updates prioritized by risk and applied promptly? Art. 21(2)(e) NIS2 Directive · Core question	Patch process with deadlines by severity and a patch status report with date (at most 12 months).		
19	Is our data encrypted in transit and at rest in line with the state of the art? Art. 21(2)(h) NIS2 Directive · Core question	Cryptography policy with methods for transmission and storage and approval date (at most 24 months).		
20	Are the systems in use kept in an inventory and are configurations changed in a controlled way? Art. 21(2)(i) NIS2 Directive · Standard question	Screenshot of the inventory or the change process with date (at most 12 months).		
21	Do you implement basic cyber hygiene (hardening, secure passwords, endpoint protection, secure configuration)? Art. 21(2)(g) NIS2 Directive · Standard question	Policy on hardening, passwords and endpoints with approval date (at most 24 months).		
22	Do you follow warnings from the BSI, CERTs or vendors and act on them? Art. 21(2)(b) NIS2 Directive · Extended question	No document needed. State the sources in the answer text.		

Product and development security

No.	Question	Suitable evidence	Answer	Evidence / comment
23	Do you apply secure development principles when you develop or adapt software or systems for us? Art. 21(2)(e) NIS2 Directive; Art. 21(3) NIS2 Directive · Standard question	Secure development policy with approval date (at most 24 months).		

Continuity and backup

No.	Question	Suitable evidence	Answer	Evidence / comment
24	Is there an emergency and recovery concept specifically for the service provided to us? Art. 21(2)(c) NIS2 Directive · Core question	Emergency or recovery plan for the specific service, version and date (at most 24 months).		
25	Are the availability, maximum downtime and maximum data loss of your service set by contract? Art. 21(2)(c) NIS2 Directive · Standard question	SLA extract with availability, recovery time and maximum data loss.		
26	Is there a secured alternative channel for communicating with us in an emergency (for example if email fails)? Art. 21(2)(j) NIS2 Directive · Extended question	Emergency communication plan with alternative channel and date (at most 24 months).		
27	Do you support us when we exit (data handover in a common format, transition period, help with switching)? Art. 21(2)(d) NIS2 Directive · Extended question	Contract clause on exit, data format and transition period.		

Own supply chain

No.	Question	Suitable evidence	Answer	Evidence / comment
28	Do you assess the security of your own critical suppliers and service providers? Art. 21(2)(d) NIS2 Directive; Art. 21(3) NIS2 Directive · Core question	Report or extract of your own supplier assessment with date (at most 12 months).		
29	Do you announce a change of important subcontractors in advance, giving us the opportunity to object? Art. 21(2)(d) NIS2 Directive · Standard question	Contract clause with notice period and right to object.		
30	Do you take security requirements into account when procuring your own IT (hardware, software, cloud)? Art. 21(2)(e) NIS2 Directive · Extended question	Procurement policy with security requirements and approval date (at most 24 months).		
31	From which countries and which main manufacturers or data centers does your service originate? Art. 22 NIS2 Directive; § 41 BSIG · Extended question	No document needed. State the countries and main providers in the answer text.		

About this template

Template version	2026-11-3-1d7d1915
Content as of	1 November 2026
Published by	Made with Complass, https://complass.eu

Legal basis (as of): Art. 21(2)(d) NIS2 Directive; § 30(2) no. 4 BSIG

This template is not legal advice. It does not replace checking which requirements apply to your company and does not guarantee any audit or certification result.

License: Creative Commons Attribution 4.0 International (CC BY 4.0). You may use, change and pass on the template, also commercially, as long as you name the source. Attribution: "Template: Complass (complass.eu), CC BY 4.0". https://creativecommons.org/licenses/by/4.0/deed.en