“My client asks me for NIS2”: a guide for suppliers

You are not subject to NIS2, but a client sends you a security questionnaire or new contract clauses. Here is why, and how to respond with confidence.

NIS2 Aware · nis2aware.eu · November 2026

Why your client is asking

Organisations subject to NIS2 must manage the security of their **supply chain**. A large share of incidents start at a supplier: a hacked IT provider, a compromised software update, a stolen password of a maintenance company. Your client is therefore required to assess the security of the suppliers it depends on, and you are one of them.

What they may ask for

- A **security questionnaire** (often 20 to 100 questions) on your measures.
- **Contract clauses**: minimum measures, notification of incidents within a short delay, audit rights, confidentiality.
- **Evidence**: a CyberFundamentals self-assessment or verification, an ISO/IEC 27001 certificate, a summary of your security policy.
- Specific measures: **multi-factor authentication**, backups, timely updates, restricted access to their systems.
- A named **security contact** who can be reached in case of an incident.

How to respond

1. **Don't panic and don't overpromise.** Answer honestly: “in place”, “in progress (by date)” or “not applicable”. A credible plan is better than an empty yes.
2. **Read the clauses carefully** before signing: notification delays, liability, audit rights. Have them checked if needed.
3. **Keep your answers in one place**, so you can reuse them for the next client.
4. **Turn it into an advantage:** a supplier who answers clearly and quickly inspires trust and wins contracts.

Your 30-day action plan

Week	Actions
1	Name a security contact. Enable multi-factor authentication on email and remote access.
2	Check your backups: at least one copy offline or immutable, and test a restore. Turn on automatic updates.
3	Remove unnecessary administrator rights. Make sure every device has up-to-date anti-malware.
4	Write a one-page incident procedure, including how you will inform your clients. Brief your staff on phishing.

Next step: show it

The CCB's **CyberFundamentals** framework has a **Basic** level that suits many small companies. A self-assessment against CyFun Basic gives you a structured answer to most questionnaires. You can find the tools on atwork.safeonweb.be.

> **Test yourself first:** our light maturity check shows your gaps in five minutes.

General information on the Belgian NIS2 framework as of November 2026, not legal advice. Always check the latest guidance from the CCB (ccb.belgium.be and atwork.safeonweb.be).