NIS2 supply chain security checklist

NIS2 requires essential and important entities to manage the security of their supply chain. Thirteen points to get it under control.

NIS2 Aware · nis2aware.eu · November 2026

Know your suppliers

- [ ] **List your suppliers and ICT service providers**
  IT support, cloud, software, maintenance, logistics, anyone with access to your systems or data.
- [ ] **Identify the critical ones**
  Those whose failure or compromise would disrupt your services.
- [ ] **Know who has access to what**
  Remote access, accounts, data, physical access.

Set requirements

- [ ] **Assess the security of critical suppliers**
  Questionnaire, CyberFundamentals or ISO/IEC 27001 evidence, references.
- [ ] **Include security clauses in contracts**
  Minimum measures, confidentiality, use of subcontractors.
- [ ] **Require notification of incidents within a short delay**
  So you can meet your own 24-hour deadline.
- [ ] **Provide for audit rights and the return or deletion of data at the end**
  Including an exit plan.

Control access

- [ ] **Supplier access uses MFA and personal accounts**
  No shared accounts or passwords.
- [ ] **Access is limited, logged and time-bound**
  Only what is needed, only when needed.

- [ ] **Accounts are removed when the contract ends**
  Check at least once a year.

Monitor

- [ ] **Review critical suppliers at least once a year**
  Changes, incidents, evidence.
- [ ] **Watch the security of the products you buy**
  Updates, end of support, known vulnerabilities.
- [ ] **Have an alternative for each critical supplier**
  Or a plan to keep working without them.

> Are you the supplier? Read our guide “My client asks me for NIS2”.

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).