NIS2 compliance checklist

Twenty-eight points to check your compliance with the Belgian NIS2 law: scope, registration, governance, the ten risk-management measures, incident reporting and evidence.

NIS2 Aware · nis2aware.eu · November 2026

1. Scope and registration

- [ ] **Assess whether your organisation is in scope**
  Check your sector (Annex I or II) and size (50+ employees or more than €10M turnover and balance sheet), including partner and linked enterprises. Document the analysis.
- [ ] **Determine your category: essential or important**
  Large organisations in high-criticality sectors are generally essential; the others in scope are generally important. Your supervision regime depends on it.
- [ ] **Register on Safeonweb@Work**
  Registration with the CCB is mandatory. Keep the contact details of your representatives up to date.
- [ ] **Check whether a sectoral authority or other rules apply**
  Some sectors have a sectoral authority alongside the CCB. Financial entities fall mainly under DORA for ICT risk.

2. Governance

- [ ] **The management body has approved the cybersecurity measures**
  Record the approval in the minutes of a board meeting.
- [ ] **The management body oversees implementation**
  Plan regular reporting (for example quarterly) with a few clear indicators.
- [ ] **Members of the management body have followed training**
  This is a legal obligation. Keep attendance records and plan refreshers.
- [ ] **A person is responsible for cybersecurity**
  Name an owner (internal or external) with time, authority and a back-up.
- [ ] **A budget and a 12-month roadmap are approved**
  Set a target, such as a CyberFundamentals assurance level, and the resources to reach it.

3. Risk-management measures

The ten areas the law requires as a minimum, following an all-hazards approach.

- [ ] **Risk analysis and information system security policies**
  Identify your critical assets and risks, and approve a security policy based on them.
- [ ] **Incident handling**
  Detect, analyse, contain and recover from incidents, with defined roles.
- [ ] **Business continuity: backups, disaster recovery, crisis management**
  Keep at least one backup offline or immutable, test restores and write a crisis plan.
- [ ] **Supply chain security**
  Identify critical suppliers and set security requirements in contracts.
- [ ] **Security in acquisition, development and maintenance, including vulnerability handling**
  Patch within defined deadlines, scan for vulnerabilities and handle reports of vulnerabilities.
- [ ] **Assessing the effectiveness of the measures**
  Use audits, tests and indicators to check that the measures work.
- [ ] **Basic cyber hygiene and cybersecurity training**
  Train all staff at least once a year: phishing, passwords, reporting.
- [ ] **Cryptography and encryption**
  Encrypt laptops, sensitive data and communications, and manage keys properly.
- [ ] **Human resources security, access control and asset management**
  Keep an asset inventory, give the least privileges needed, and handle joiners, movers and leavers.
- [ ] **Multi-factor authentication and secured communications**
  MFA on email, remote access, cloud and admin accounts; secured voice, video, text and emergency communications.

4. Incident reporting

- [ ] **Criteria for a significant incident are defined**
  Severe operational disruption, financial loss, or considerable damage to others.
- [ ] **The 24h / 72h / one-month procedure is written down**
  Who decides, who notifies the CCB, with which information. Keep a copy offline.
- [ ] **Notification channels and contacts are known and tested**
  Know how to notify the CCB and keep an up-to-date contact list for the crisis team.
- [ ] **You know when to inform your service recipients**
  Prepare messages to inform clients affected by a significant incident.

- [ ] **Incidents are logged and lessons learned**
  Keep an incident register and update your risk analysis after each incident.

5. Evidence and conformity

- [ ] **A reference framework is chosen**
  CyberFundamentals (Basic, Important, Essential) or ISO/IEC 27001.
- [ ] **A gap analysis has been done and a target level set**
  Measure where you stand against the framework and plan the improvements.
- [ ] **Essential entities: the conformity assessment is planned**
  Plan the verification or certification with an accredited body and check the CCB deadlines that apply to you.
- [ ] **Evidence is kept and organised**
  Board minutes, policies, training records, test and audit reports, incident register.

> **A checklist is not compliance.** NIS2 asks for a risk-based approach that you keep up to date. Use this list to structure the work, not to tick boxes once.

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).