NIS2 checklist for the board

Under NIS2, the management body approves the cybersecurity measures, oversees them and can be held liable. Thirteen points for directors.

NIS2 Aware · nis2aware.eu · November 2026

Understand

- [ ] **We know whether we are in scope and in which category**
  Essential or important entity, documented.
- [ ] **Each board member has followed cybersecurity training**
  A legal obligation for members of the management body. Keep evidence.
- [ ] **We understand the board's liability**
  The management body can be held liable for breaches of the risk-management obligations.
- [ ] **Our top cyber risks are expressed in business terms**
  Impact on operations, revenue, reputation and clients.

Decide

- [ ] **The board has formally approved the cybersecurity measures**
  The decision is recorded in the minutes.
- [ ] **A budget and a roadmap are approved**
  With a clear target, for example a CyberFundamentals level.
- [ ] **Responsibilities are assigned**
  A named owner for cybersecurity, and decision rights in a crisis.
- [ ] **Risk appetite is defined**
  Which risks we accept, reduce, transfer (insurance) or avoid.

Oversee

- [ ] **Cybersecurity is on the board agenda at least every quarter**
  With short written reporting.
- [ ] **We follow a few clear indicators**
  For example MFA coverage, patching delays, backup tests, training completion, incidents.

- [ ] **Critical suppliers are monitored**
  The board knows which suppliers could stop the business.
- [ ] **Incident reports reach the board**
  Including near misses and lessons learned.
- [ ] **The measures are reviewed every year**
  And whenever the organisation or the threats change.

> Go further with the 10 questions your board should ask.

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).