

FREE CHECKLIST · NIS2 · LUXEMBOURG

NIS2 checklist for companies in Luxembourg

Know where you stand in 10 minutes: 12 checkpoints covering scope, obligations and measures — to tick off with your team.

Legal basis	Directive (EU) 2022/2555 (NIS2), transposed in Luxembourg by the law of 5 May 2026 on measures to ensure a high level of cybersecurity.
Authorities	ILR (Institut Luxembourgeois de Régulation) for most sectors · CSSF for the financial sector.
Registration	Self-registration of affected entities via the ILR portal (guichet.ilr.lu).
Incident reporting	Early warning within 24 hours, notification within 72 hours, final report within one month — via the ILR's SERIMA platform.
Penalties	Up to €10 million or 2% of worldwide annual turnover for essential entities — plus personal accountability of management.

How to use this checklist

Tick every point your company demonstrably fulfils today. “Demonstrably” means: there is a document, a process or a log — not just a good feeling.

At the end, count your ticks and read the evaluation on the last page.

A · Determine whether you are in scope

☐

1. Sector checked

Your activity has been checked against Annexes I/II of the NIS2 directive (energy, transport, health, digital infrastructure, manufacturing, postal services, waste, food, chemicals, and more).

☐

2. Size threshold checked

You know whether you are above the threshold: 50+ employees or more than €10 million in annual turnover or balance-sheet total (exceptions: certain critical services regardless of size).

☐

3. Supply chain checked

You have checked whether customers who are themselves subject to NIS2 pass security requirements on to you by contract — NIS2 often reaches non-covered companies through the supply chain.

B · Governance & obligations

☐

4. Management accountable

Management has approved the cybersecurity measures, oversees their implementation and is trained itself — NIS2 establishes personal accountability here.

☐

5. Registration completed

Your entity is registered as “essential” or “important” with the ILR (guichet.ilr.lu), or with the CSSF if you belong to the financial sector.

☐

6. Reporting process defined

It is defined who reports significant incidents, when and how: early warning within 24 h, notification within 72 h, final report within one month (SERIMA platform).

C · Technical & organisational measures

☐

7. Risk analysis & policies

A documented risk analysis and security policies exist and their effectiveness is reviewed regularly.

☐

8. Backup & contingency plan

A backup concept (e.g. the 3-2-1-1-0 rule) with tested restores plus a business continuity and crisis management plan are in place.

☐

9. Access & encryption

Multi-factor authentication, a clean permissions concept and encryption for sensitive data and communication are in use.

☐

10. Vulnerabilities & detection

Patch management runs systematically and attacks are detected — through monitoring or 24/7 surveillance (SOC/XDR).

D · People & suppliers☐**11. Awareness training**

All employees are trained regularly on phishing and safe behaviour — with evidence.

☐**12. Supplier security governed**

Security requirements for your IT providers and suppliers are fixed contractually and reviewed.

Evaluation: where do you stand?

0–4 ticks	High need for action. The basic obligations are not yet covered — if you are in scope, you risk penalties and long outages. Start with points 1–3 and 8.
5–9 ticks	Solid basis, but with gaps. Typical open points: reporting process, registration and attack detection — exactly what auditors look at first.
10–12 ticks	Well positioned. Now it's about evidence: documentation, restore logs and regular reviews to stay audit-ready.

Next step: free IT check (90 minutes)

You receive a written assessment of your open points from this checklist — on site or remote, without obligation, in English, French or German.

Phone: +352 20 60 12 44 · Email: mail@local-it-partner.lu · Web: local-it-partner.lu

As of August 2026. This checklist is guidance provided by Local-IT-Partner S.à r.l.-S and does not replace legal advice. The NIS2 directive (EU) 2022/2555, the Luxembourg transposition law and the requirements of the ILR and CSSF prevail.