

Where does your organisation stand on NIS2?

Fifteen questions for a quick self-assessment. They are no substitute for a formal review, but they show you where to look first.

Scope and registration

- 01 Have you checked whether your organisation falls within NIS2 scope by sector and size, or receives NIS2 requirements anyway as a supplier to in-scope entities? ☐ Yes ☐ Partly ☐ No
- 02 If you are in scope, is your registration with the national authority (in Italy, the ACN platform) complete and renewed each year, with a designated point of contact? ☐ Yes ☐ Partly ☐ No

Governance

- 03 Has the management body approved the security measures, and does it oversee their implementation? ☐ Yes ☐ Partly ☐ No
- 04 Have senior managers received training on cybersecurity risk management? ☐ Yes ☐ Partly ☐ No
- 05 Are cybersecurity roles and responsibilities assigned and documented? ☐ Yes ☐ Partly ☐ No

Risks and security measures

- 06 Is there a documented, up-to-date risk assessment based on an inventory of systems, data and services? ☐ Yes ☐ Partly ☐ No
- 07 Is multi-factor authentication enabled for email, remote access and administrator accounts? ☐ Yes ☐ Partly ☐ No
- 08 Are backups isolated from the main network, and are restores tested regularly? ☐ Yes ☐ Partly ☐ No
- 09 Are vulnerabilities and security updates handled through a defined process and timescales? ☐ Yes ☐ Partly ☐ No
- 10 Is there a business continuity and crisis management plan? ☐ Yes ☐ Partly ☐ No
- 11 Do all staff receive regular cyber hygiene training? ☐ Yes ☐ Partly ☐ No

Supply chain

- 12 Have critical suppliers been identified and assessed, with security requirements written into contracts? ☐ Yes ☐ Partly ☐ No

Incidents

- 13 Is there an incident management procedure with roles, severity criteria and contacts? ☐ Yes ☐ Partly ☐ No
- 14 Could you report a significant incident to the national CSIRT on time: early warning within 24 hours, notification within 72 hours, final report within one month? ☐ Yes ☐ Partly ☐ No

Assurance

- 15 Is the effectiveness of the measures checked regularly through audits, tests or exercises? ☐ Yes ☐ Partly ☐ No

Score

YES = 2 · PARTLY = 1 · NO
= 0 · MAXIMUM 30

24–30 · A solid base The foundations are in place. Make sure every answer is backed by documented evidence, and keep the system up to date.

12–23 · Work in progress There are gaps on points the law requires. A plan with clear priorities is the next step, starting with governance and incident handling.

0–11 · Still to be set up The risk of non-compliance is high. Start with scope, governance and the risk assessment: everything else builds on them.