NIS2 compliance checklist

Knowing what NIS2 requires is one thing; knowing whether you already comply is another. This checklist goes block by block through what the IT department should be able to show in an audit.

Tick each item once it is in place.

Before you start: are you in scope?

- [ ] Check with your legal advisers whether your organization is an essential entity, an important entity or neither.
- [ ] Review what your customers require: many ask their suppliers for these measures even when the law does not.
- [ ] Appoint one person to coordinate compliance.

1. Governance and responsibilities

- [ ] Management has approved the security policy and the risk management measures.
- [ ] There is a security lead with responsibilities defined in writing.
- [ ] Management has received cybersecurity training, and there is a record of it.
- [ ] There is a review schedule for the measures, at least once a year.

2. Inventory and risk analysis

- [ ] An up-to-date inventory of devices, servers, cloud services and applications.
- [ ] An inventory of licenses and who they are assigned to.
- [ ] A list of user accounts and who can access what, including privileged accounts.
- [ ] A documented risk analysis that identifies critical assets.
- [ ] A treatment plan: which risk is accepted, which is reduced and with which measure.

3. Technical measures

- [ ] Multi-factor authentication for email, remote access and privileged accounts.
- [ ] System and application patches up to date, with a defined deadline for critical ones.
- [ ] Device protection and threat detection.
- [ ] Encryption of laptops and sensitive data.
- [ ] Automatic backups, with at least one copy outside the main network, and regular restore tests.
- [ ] A business continuity and disaster recovery plan.
- [ ] Secure communications for emergencies.

4. Incident management and reporting

24 h
Early warning
A first notice that something has happened.

72 h
Incident notification
An initial assessment of severity and impact.

1 month
Final report
One month after the notification: description, root cause, mitigation measures and cross-border impact.

- [ ] A written procedure to detect, classify and handle incidents.
- [ ] Clear criteria for deciding whether an incident is significant.
- [ ] Owners and deputies for reporting, with their contact details at hand.
- [ ] Templates ready for the three notifications the directive requires
- [ ] A log of every incident, with its timeline and the actions taken.
- [ ] One drill a year to check that the procedure works.

5. Suppliers and supply chain

- [ ] A list of suppliers with access to systems or data, and the critical services they provide.
- [ ] Security and incident reporting clauses in their contracts.
- [ ] Regular reviews of their security, proportionate to the risk.
- [ ] Renewal dates under control, so you can review terms before contracts renew automatically.

6. Training and awareness

- [ ] Basic cybersecurity training for all staff, at least once a year.
- [ ] Specific training for those who administer systems or handle incidents.
- [ ] Phishing simulations, with follow-up on the results.
- [ ] Written cyber hygiene practices: passwords, devices, email and remote work.
- [ ] Onboarding and offboarding with access reviewed: nobody keeps permissions after they leave.

7. Evidence: how to prove it

- [ ] Approved policies, dated and signed.
- [ ] The inventory and the risk analysis, with their latest review.
- [ ] Incident and drill records.
- [ ] Restore test results.
- [ ] Training records for staff and management.
- [ ] Supplier contracts with their security clauses.

This checklist is for guidance only and is not a substitute for legal advice. Full guide:
monkinet.ai/en/blog/nis2-compliance-checklist