cerivo

NIS2 Checklist: Track Your Compliance Progress

Use this NIS2 checklist to keep track of your compliance progress, identify what you already have in place, and see where you still need to act.
Print it, share it with colleagues, or use it as a working document as you move through your NIS2 implementation.

Governance

- [ ] Make sure management defines the company's goals and risk appetite
- [ ] Make sure your NIS2 compliance framework support the company's goals
- [ ] Involve relevant stakeholders, align expectations, and keep everyone with a vested interest in the company's operations and its NIS2 compliance
- [ ] Assign clear compliance responsibilities across the organization
- [ ] Make sure management approves and oversees the implementation of cybersecurity measures
- [ ] Plan regular reviews of your NIS2 framework
- [ ] Use insights from past compliance initiatives in other areas

Security

- [ ] Make sure security levels are appropriate and proportional to manage applicable risks
- [ ] Make sure management and relevant employees complete the required cybersecurity training
- [ ] Make sure the following minimum requirements are implemented (by following national guidance, if published):

    - Policies on risk analysis and information system security
    - Incident handling
    - Business continuity, including backup management and disaster recovery, as well as crisis management
    - Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
    - Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure

- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption
- Human resources security, access control policies and asset management
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

Reporting and communication

- [ ] Be able to detect incidents and analyze their total impact
- [ ] Assess if incidents are significant within the meaning of NIS2
- [ ] Report significant incidents to relevant authorities
- [ ] Communicate significant incidents to recipients of your services
- [ ] Fulfill content requirements and reporting deadlines

Documentation

- [ ] Document your governance process, decisions, and compliance efforts along the way
- [ ] Consider following an ISMS, e.g. based on ISO/IEC 27001:2022, to systematize your cybersecurity
- [ ] Automate as much of the process as possible

Need a more structured way to manage your NIS2 work? If you want to move from checklist to ongoing compliance, our experts can help you set up a NIS2 workflow that keeps track of tasks, documentation, and follow-up.

Get expert help with NIS2