PRACTICAL GUIDE · COMPLIANCE

NIS2 checklist: the 10 measures to check

Article 21 of the NIS2 directive lists ten risk-management measures that in-scope entities must implement. For each, ask yourself: does it exist, is it formalised, is it applied?

01 Risk analysis and security policy

Are the risks to your systems identified, assessed and reviewed? Is there a security policy approved by management?

02 Incident handling

Can you detect, qualify and handle an incident? Is the escalation and reporting process written down?

03 Business continuity and crisis management

Isolated and tested backups, a recovery plan, a crisis team: are they in place and rehearsed?

04 Supply-chain security

Are your critical suppliers and providers identified? Do your contracts include security requirements?

05 System security and vulnerability handling

Is security considered in acquisition, development and maintenance? Are patches applied within defined timeframes?

06 Assessing the effectiveness of measures

Do you measure how effective your measures are: indicators, audits, penetration tests?

07 Cyber hygiene and training

Are basic good practices applied? Are employees and executives trained regularly?

08 Cryptography and encryption

Do you have rules for using encryption, for stored data as well as for communications?

09 Human resources, access and assets

Are joiners and leavers managed? Do access rights follow least privilege? Is the asset inventory up to date?

10 Multi-factor authentication and secure communications

Is two-factor authentication deployed, especially for remote access and administrator accounts? Do you have secure means of communication, including in an emergency?

Guide based on Article 21 of Directive (EU) 2022/2555. National transposition laws may specify these requirements further.