NIS2 Compliance Checklist
& Readiness Workbook 2026

Assess Your Readiness Across Governance, Cybersecurity, Suppliers & Resilience

Magic Stone Cyber Security

Note: This workbook does not replace a formal NIS2 assessment. It is designed to help your organisation understand the scope of NIS2 obligations and identify compliance gaps before a formal assessment. For documented compliance evidence, a structured NIS2 Assessment provides the formal gap analysis, prioritised remediation roadmap, and readiness validation that regulators and auditors require. **magicstone.nl/en/nis2-assessment/**

How to Use This Workbook

A complete NIS2 compliance programme addresses the core requirements of the EU's cybersecurity directive: governance and board accountability, cyber risk management, incident response, supply chain security, and business continuity. This workbook translates those obligations into **ten practical sections** — drawn directly from NIS2 Article 21 and Article 20 — so your organisation can assess its current posture, identify gaps, and build a clear remediation plan.

Work through each of the ten sections. For every requirement, mark your current status — **Yes**, **Partial**, or **No**. Every No or Partial is a compliance gap that requires a remediation action.

Organisation Details

Organisation name	
Completed by	
Date	
Review date	
NIS2 entity type	☐ Essential ☐ Important ☐ Not yet determined

Scoring Guide

Status	Meaning
Yes	Requirement fully met — documented evidence available
Partial	Requirement partially met — gaps or documentation missing
No	Requirement not met — remediation action required

Count your **No** and **Partial** responses at the end of each section. Each one is a compliance risk. Prioritise by regulatory exposure — gaps in **Governance, Incident Response, and Supply Chain Security** carry the highest personal liability risk under NIS2 Articles 20 and 21.

1. Governance & Accountability

Requirement	Yes	Partial	No
Cybersecurity roles formally assigned	☐	☐	☐
Board approves cybersecurity strategy	☐	☐	☐
Management receives cyber risk reports	☐	☐	☐
Security policies reviewed annually	☐	☐	☐
Asset inventory maintained	☐	☐	☐
Risk ownership assigned	☐	☐	☐
Compliance ownership defined	☐	☐	☐
Third-party governance established	☐	☐	☐
Executive accountability documented	☐	☐	☐
Cyber budget reviewed annually	☐	☐	☐

2. Cyber Risk Management

Requirement	Yes	Partial	No
Formal risk assessment process in place	☐	☐	☐
Risk register maintained and reviewed	☐	☐	☐
Critical assets identified and classified	☐	☐	☐
Threat landscape assessed regularly	☐	☐	☐
Risk appetite defined and documented	☐	☐	☐
Residual risks accepted by management	☐	☐	☐
Risk treatment plans in place	☐	☐	☐
Risks reviewed after significant changes	☐	☐	☐

3. Technical Security Controls

Requirement	Yes	Partial	No
Multi-factor authentication enforced	☐	☐	☐
Privileged access management in place	☐	☐	☐
Endpoint protection deployed	☐	☐	☐
Email security controls active	☐	☐	☐
Data encryption in place (at rest and in transit)	☐	☐	☐
Patch management process followed	☐	☐	☐
Security hardening standards applied	☐	☐	☐
Software inventory maintained	☐	☐	☐

4. Network Security

Requirement	Yes	Partial	No
Network segmentation implemented	☐	☐	☐
Firewall and perimeter controls in place	☐	☐	☐
Remote access secured (VPN/MFA)	☐	☐	☐
Network traffic monitored and logged	☐	☐	☐
Wireless networks secured and segmented	☐	☐	☐
Intrusion detection/prevention deployed	☐	☐	☐
Network access control (NAC) in place	☐	☐	☐
OT/IoT networks isolated where applicable	☐	☐	☐
Network security reviewed annually	☐	☐	☐

5. Third-Party Risk Management

Requirement	Yes	Partial	No
Critical suppliers identified and documented	☐	☐	☐
Supplier security assessments conducted	☐	☐	☐
Contractual security requirements in place	☐	☐	☐
Supplier access controlled and monitored	☐	☐	☐
Supply chain risk register maintained	☐	☐	☐
Incident notification obligations agreed	☐	☐	☐
Supplier compliance reviewed annually	☐	☐	☐
Fourth-party risks considered	☐	☐	☐

6. Incident Response & Reporting

Requirement	Yes	Partial	No
Incident response plan documented and tested	☐	☐	☐
Incident classification criteria defined	☐	☐	☐
24-hour early warning capability in place	☐	☐	☐
72-hour full notification process defined	☐	☐	☐
Escalation paths documented	☐	☐	☐
Forensic evidence preservation procedures in place	☐	☐	☐
Post-incident review process established	☐	☐	☐
CSIRT/competent authority contacts known	☐	☐	☐

7. Security Awareness & Management Training

Requirement	Yes	Partial	No
Annual security awareness training delivered	☐	☐	☐
Phishing simulation programme in place	☐	☐	☐
Role-based training for high-risk staff	☐	☐	☐
Board and management training delivered	☐	☐	☐
Training completion records maintained	☐	☐	☐
New employee security onboarding in place	☐	☐	☐
Training effectiveness measured	☐	☐	☐

8. Vulnerability Handling & Disclosure

Requirement	Yes	Partial	No
Vulnerability scanning performed regularly	☐	☐	☐
CVE/threat intelligence feeds monitored	☐	☐	☐
Patch prioritisation process in place	☐	☐	☐
Zero-day response procedure defined	☐	☐	☐
Responsible disclosure policy published	☐	☐	☐
Penetration testing conducted annually	☐	☐	☐
Remediation SLAs defined and tracked	☐	☐	☐
Vulnerability register maintained	☐	☐	☐

9. Business Continuity & Recovery

Requirement	Yes	Partial	No
Business continuity plan documented and tested	☐	☐	☐
Recovery time objectives (RTO) defined	☐	☐	☐
Recovery point objectives (RPO) defined	☐	☐	☐
Backups performed and tested regularly	☐	☐	☐
Backups isolated and ransomware-proof	☐	☐	☐
Disaster recovery plan in place	☐	☐	☐
Crisis communication plan documented	☐	☐	☐
BCP reviewed after significant changes	☐	☐	☐

10. Audit & Compliance Evidence

Requirement	Yes	Partial	No
Continuous monitoring in place	☐	☐	☐
Audit evidence maintained	☐	☐	☐
Policy reviews conducted	☐	☐	☐
Control testing performed	☐	☐	☐
Compliance reporting produced	☐	☐	☐
Improvement actions tracked	☐	☐	☐
Metrics reviewed	☐	☐	☐
Management reporting completed	☐	☐	☐

Gaps found? Book a NIS2 assessment with Magic Stone — gap analysis, remediation roadmap, and compliance validation. **magicstone.nl/en/nis2-assessment/**