NIS2 Compliance Checklist
& Gereedheidswerkboek 2026

Beoordeel uw gereedheid op het gebied van governance, cybersecurity, leveranciersbeheer en operationele weerbaarheid

Magic Stone Cyber Security

Opmerking: Dit werkboek vervangt geen formele NIS2-assessment. Het is ontworpen om uw organisatie te helpen de reikwijdte van de NIS2-verplichtingen te begrijpen en mogelijke compliance-hiaten te identificeren voordat een formele beoordeling wordt uitgevoerd.

Voor aantoonbaar compliance-bewijs biedt een gestructureerde NIS2 Assessment de formele gap-analyse, een geprioriteerde verbeterroadmap en een validatie van uw gereedheid die toezichthouders en auditors verwachten. **https://magicstone.nl/nis2-assessment/**

Hoe gebruikt u dit werkboek?

Een volledig NIS2-complianceprogramma behandelt de belangrijkste vereisten van de Europese cybersecurityrichtlijn: governance en bestuurlijke verantwoordelijkheid, cyberrisicobeheer, incidentrespons, beveiliging van de toeleveringsketen en bedrijfscontinuïteit.

Dit werkboek vertaalt deze verplichtingen naar tien praktische onderdelen, rechtstreeks gebaseerd op NIS2 Artikel 20 en Artikel 21, zodat uw organisatie haar huidige situatie kan beoordelen, hiaten kan identificeren en een duidelijke verbeter- en herstelroadmap kan opstellen.

Doorloop elk van de tien onderdelen. Markeer voor iedere vereiste uw huidige status: Ja, Gedeeltelijk of Nee.

Elke "Nee" of "Gedeeltelijk" vertegenwoordigt een compliancehiaat waarvoor een verbetermaatregel Neeodzakelijk is.

Organisation Details

Organisatienaam	
Ingevuld door	
Datum	
Herzieningsdatum	
NIS2-entiteitstype	☐ Essentiële entiteit ☐ Belangrijke entiteit ☐ Neeg niet vastgesteld

Scoregids

Status	Meaning
Ja	Vereiste fully met — documented evidence available
Gedeeltelijk	Vereiste Gedeeltelijkly met — gaps or documentation missing
Nee	Vereiste Neet met — remediation action required

Tel aan het einde van elke sectie het aantal antwoorden " **Nee** " en " **Gedeeltelijk** ". Elk daarvan vertegenwoordigt een compliance-risico.
Prioriteer op basis van wettelijke blootstelling. Hiaten in **Governance**, **Incidentrespons** en **Leveranciersbeveiliging** brengen onder NIS2 Artikel 20 en 21 de grootste bestuurlijke aansprakelijkheid met zich mee.
.

1. Governance & Verantwoordelijkheid

Vereiste	Ja	Gedeeltelijk	Nee
Cybersecurityrollen zijn formeel toegewezen	☐	☐	☐
Het bestuur keurt de cybersecuritystrategie goed	☐	☐	☐
Management ontvangt cyberrisicorapportages	☐	☐	☐
Beveiligingsbeleid wordt jaarlijks herzien	☐	☐	☐
Activa-inventaris wordt bijgehouden	☐	☐	☐
Risico-eigenaarschap is toegewezen	☐	☐	☐
Compliance-verantwoordelijkheden zijn vastgesteld	☐	☐	☐
Governance voor derde partijen is ingericht	☐	☐	☐
Bestuurlijke verantwoordelijkheid is gedocumenteerd	☐	☐	☐
Cybersecuritybudget wordt jaarlijks geëvalueerd	☐	☐	☐

2. Cyberrisicobeheer

Vereiste	Ja	Gedeeltelijk	Nee
Formeel proces voor risicobeoordeling aanwezig	☐	☐	☐
Risicoregister wordt onderhouden en beoordeeld	☐	☐	☐
Kritieke bedrijfsmiddelen zijn geïdentificeerd en geclassificeerd	☐	☐	☐
Dreigingslandschap wordt regelmatig beoordeeld	☐	☐	☐
Risicobereidheid is vastgesteld en gedocumenteerd	☐	☐	☐
Rest-risico's worden door management geaccepteerd	☐	☐	☐
Risicobehandelingsplannen zijn aanwezig	☐	☐	☐
Risico's worden beoordeeld na significante wijzigingen	☐	☐	☐

3. Technische Beveiligingsmaatregelen

Vereiste	Ja	Gedeeltelijk	Nee
Multi-factor authenticatie (MFA) is verplicht gesteld	☐	☐	☐
Privileged Access Management is geïmplementeerd	☐	☐	☐
Endpointbeveiliging is uitgerold	☐	☐	☐
E-mailbeveiligingsmaatregelen zijn actief	☐	☐	☐
Gegevens zijn versleuteld tijdens opslag en transport	☐	☐	☐
Patchmanagementproces wordt gevolgd	☐	☐	☐
Security hardening-standaarden zijn toegepast	☐	☐	☐
Software-inventaris wordt bijgehouden	☐	☐	☐

4. Netwerkbeveiliging

Vereiste	Ja	Gedeeltelijk	Nee
Netwerksegmentatie is geïmplementeerd	☐	☐	☐
Firewall- en perimeterbeveiliging zijn aanwezig	☐	☐	☐
Externe toegang is beveiligd (VPN/MFA)	☐	☐	☐
Netwerkverkeer wordt gemonitord en gelogd	☐	☐	☐
Draadloze netwerken zijn beveiligd en gesegmenteerd	☐	☐	☐
Intrusion Detection/Prevention is geïmplementeerd	☐	☐	☐
Network Access Control (NAC) is aanwezig	☐	☐	☐
OT/IoT-netwerken zijn waar nodig gescheiden	☐	☐	☐
Netwerkbeveiliging wordt jaarlijks geëvalueerd	☐	☐	☐

5. Leveranciersrisicobeheer (TPRM)

Vereiste	Ja	Gedeeltelijk	Nee
Kritieke leveranciers zijn geïdentificeerd en gedocumenteerd	☐	☐	☐
Leveranciersbeoordelingen op beveiliging worden uitgevoerd	☐	☐	☐
Contractuele beveiligingseisen zijn vastgelegd	☐	☐	☐
Leverancierstoegang wordt gecontroleerd en gemonitord	☐	☐	☐
Risicoregister voor de supply chain wordt bijgehouden	☐	☐	☐
Meldingsverplichtingen voor incidenten zijn overeengekomen	☐	☐	☐
Leverancierscompliance wordt jaarlijks beoordeeld	☐	☐	☐
Vierde-partijrisico's worden meegenomen	☐	☐	☐
Kritieke leveranciers zijn geïdentificeerd en gedocumenteerd	☐	☐	☐

6. Incidentrespons & Meldingen

Vereiste	Ja	Gedeeltelijk	Nee
Incidentresponsplan is gedocumenteerd en getest	☐	☐	☐
Criteria voor incidentclassificatie zijn vastgesteld	☐	☐	☐
Mogelijkheid voor melding binnen 24 uur aanwezig	☐	☐	☐
Proces voor volledige melding binnen 72 uur vastgesteld	☐	☐	☐
Escalatieprocedures zijn gedocumenteerd	☐	☐	☐
Procedures voor veiligstellen van forensisch bewijs zijn aanwezig	☐	☐	☐
Post-incident reviewproces is ingericht	☐	☐	☐
Contactgegevens van CSIRT en bevoegde autoriteiten zijn bekend	☐	☐	☐

7. Security Awareness & Management Training

Vereiste	Ja	Gedeeltelijk	Nee
Jaarlijkse security awareness-training wordt gegeven	☐	☐	☐
Phishingsimulatieprogramma is aanwezig	☐	☐	☐
Rolgebaseerde training voor risicofuncties wordt uitgevoerd	☐	☐	☐
Training voor bestuur en management wordt verzorgd	☐	☐	☐
Trainingsregistraties worden bijgehouden	☐	☐	☐
Security onboarding voor nieuwe medewerkers is aanwezig	☐	☐	☐
Effectiviteit van trainingen wordt gemeten	☐	☐	☐

8. Kwetsbaarhedenbeheer & Responsible Disclosure

Vereiste	Ja	Gedeeltelijk	Nee
Kwetsbaarheidsscans worden regelmatig uitgevoerd	☐	☐	☐
CVE- en threat-intelligencefeeds worden gemonitord	☐	☐	☐
Proces voor prioritering van patches is aanwezig	☐	☐	☐
Procedure voor zero-day kwetsbaarheden is vastgesteld	☐	☐	☐
Responsible Disclosure-beleid is gepubliceerd	☐	☐	☐
Penetratietesten worden jaarlijks uitgevoerd	☐	☐	☐
Remediation-SLA's zijn vastgesteld en worden gevolgd	☐	☐	☐
Kwetsbaarhedenregister wordt bijgehouden	☐	☐	☐

9. Bedrijfscontinuïteit & Herstel

Vereiste	Ja	Gedeeltelijk	Nee
Bedrijfscontinuïteitsplan is gedocumenteerd en getest	☐	☐	☐
Recovery Time Objectives (RTO) zijn vastgesteld	☐	☐	☐
Recovery Point Objectives (RPO) zijn vastgesteld	☐	☐	☐
Back-ups worden regelmatig uitgevoerd en getest	☐	☐	☐
Back-ups zijn geïsoleerd en ransomwarebestendig	☐	☐	☐
Disaster Recovery-plan is aanwezig	☐	☐	☐
Crisiscommunicatieplan is gedocumenteerd	☐	☐	☐
BCP wordt beoordeeld na significante wijzigingen	☐	☐	☐

10. Audit & Compliance-bewijs

Vereiste	Ja	Gedeeltelijk	Nee
Continue monitoring is ingericht	☐	☐	☐
Auditbewijzen worden bijgehouden	☐	☐	☐
Beleidsbeoordelingen worden uitgevoerd	☐	☐	☐
Controltests worden uitgevoerd	☐	☐	☐
Compliancerapportages worden opgesteld	☐	☐	☐
Verbeteracties worden gevolgd	☐	☐	☐
KPI's en meetwaarden worden beoordeeld	☐	☐	☐
Managementrapportages worden afgerond	☐	☐	☐

Gaps found? Plan een NIS2 Assessment met Magic Stone Cyber Security voor een professionele gap-analyse, verbeterroadmap en validatie van uw NIS2-gereedheid. **magicstone.nl/nis2-assessment/**