MK Cloud & IT

NIS2 Readiness & Bewijsrapport

MK Cloud & IT Demo-omgeving

Gegenereerd op 08-08-2026 08:48 UTC

Rapport-ID NIS2-9C7C57E275B3 | Versie 1.0

72

NIS2-GEREEDHEID /100

AANTOONBAAR BEWIJS

Documentbeheer en inhoud

Kenmerk	Vastlegging
Rapport-ID	NIS2-9C7C57E275B3
Versie	1.0
Rapportdatum	08-08-2026 08:48 UTC
Classificatie	Vertrouwelijk
Opsteller	Automatisch gegenereerd door M365 Dashboard
Reviewer	Niet vastgelegd
Reviewdatum	Niet vastgelegd
Volgende review	Niet vastgelegd
Bewijsvingerafdruk (SHA-256)	2baea323997ea04952722d5e831fe72a75673d7ccbc4b0ddb7300bee55be2454

Inhoudsopgave

De uiteindelijke paginanummers hangen af van het aantal maatregelen, bewijsstukken en incidenten. Elke pagina bevat een rapport-ID, versie en paginanummer.

Managementsamenvatting

Dit rapport geeft de actuele NIS2-gereedheid weer over alle 10 zorgplichtgebieden, inclusief technische metingen en handmatig vastgelegd bewijs. Totaalscore: 72/100 (NIS2-maatregelen voor 72% aantoonbaar op basis van beschikbare technische en organisatorische bewijzen.).

CYRA-positionering: dit bewijs kan worden gebruikt bij de voorbereiding van een CYRA-IT-self-assessment. Het dashboard kent geen officieel CYRA-niveau of volwassenheidslevel toe.

De statussen in dit rapport geven aan of bewijs voor een portalcontrole aantoonbaar is. Zij zijn geen definitief juridisch oordeel dat aan een wetsartikel wordt voldaan.

76%	69%	70%	2
ICT/Technisch	Organisatorisch bewijs	Incidentmelding	Kritieke gaps

Bewijsdekking per categorie

Deze vijf categorieën vormen een extra doorsnede naast de tien NIS2-zorgplichtgebieden en zijn geen afzonderlijke wettelijke score.

Categorie	Dekking	Aantoonbaar	Deels	Open	Totaal
Fysiek	0%	0	0	1	1
Organisatorisch	68%	13	2	8	23
Personeel	67%	4	0	2	6
Privacy	100%	4	0	0	4
Technologisch	74%	17	0	6	23

Toepasselijkheid (NIS2 art. 2-3; Cbw toepassingsbereik)

Onderdeel	Vastlegging
Juridische entiteit	MK Cloud & IT Demo-omgeving
KvK-/registratienummer	niet vastgelegd
Sector	ICT service management (B2B)
Subsector/activiteit	niet vastgelegd
Bijlage	I
Omvang	Middelgroot (>= 50 medewerkers of > 10 mln omzet) - 140 medewerkers, 28.5 mln omzet
Kwalificatie	Belangrijke entiteit
Registratieplicht	Ja - geregistreerd op 2026-07-11
Vastgesteld door	Sven de Vries op 2026-06-01

Onderbouwing: Annex I sector 9; middelgroot op basis van 140 medewerkers en 28,5 mln omzet.

Bevoegde instanties en contactpunten

Onderdeel	Vastlegging
Bevoegde toezichthouder	Niet vastgelegd
CSIRT / meldloket	Niet vastgelegd
Nationaal contact / registratieloket	Niet vastgelegd
Intern meldverantwoordelijke	Niet vastgelegd

Registratieplicht: Cbw art. 43-47. De organisatie moet zelf controleren welke toezichthouder, welk CSIRT en welk meldloket voor haar sector gelden.

Bestuurlijke goedkeuring (Art. 20 NIS2)

Aanvullende grondslag: Cbw art. 24 en Cbb art. 20-22; inclusief bestuurlijke opleiding.

Goedgekeurd door Sven de Vries op 2026-05-14.

Bestuurlijk onderdeel	Status / bewijs
Formele goedkeuring maatregelen	Vastgelegd
Toezicht op uitvoering	Niet vastgelegd
Bestuursopleiding gevolgd	Niet vastgelegd
Datum opleiding	Niet vastgelegd
Bewijs / certificaat	Niet vastgelegd
Volgende opleiding	Niet vastgelegd

Kritieke gaps (2)

Zorgplichtgebied	Gap
Incidentafhandeling	Artikel 23 kent drie termijnen: 24 uur vroegtijdige waarschuwing, 72 uur melding en een eindverslag binnen een maand. Leg ook die derde stap vast.
Cyberhygiëne en training	NIS2 Art. 20: bestuur moet cyberbeveiligingstraining volgen.

Verlopend of verlopen bewijs (1)

Maatregel	Bewijsitem	Reden
Jaarlijkse beleidsreview gedocumenteerd	Verslag jaarlijkse beleidsreview	Reviewdatum verloopt of is verstreken

Open acties (0)

Geen openstaande acties vastgelegd.

Actieve incidenten (0)

Geen actieve incidenten.

Methodologie en interpretatie

De portal combineert technische waarnemingen uit Microsoft 365 met handmatig vastgelegd organisatorisch bewijs. Per maatregel wordt beoordeeld of bewijs voor deze portalcontrole aantoonbaar, gedeeltelijk aantoonbaar, niet aantoonbaar of niet van toepassing is. De totaalscore is een gewogen readiness-indicator en geen wettelijke norm, certificeringsniveau of juridisch nalevingsoordeel.

Status	Betekenis
Aantoonbaar	De portal of bewijskluis bevat actueel bewijs voor de uitgevoerde controle.
Gedeeltelijk	Het bewijs is onvolledig, beperkt van scope, verouderd of vereist aanvullende beoordeling.
Niet aantoonbaar	Voor deze controle is geen afdoende bewijs beschikbaar; dit is niet automatisch bewijs van niet-naleving.
N.v.t.	De maatregel is gemotiveerd buiten scope geplaatst; goedkeuring en periodieke herbeoordeling blijven nodig.

Onderzoeksgrenzen

- Primaire technische scope: Microsoft 365 en de databronnen die tijdens de betreffende run beschikbaar waren.
- Niet automatisch onderzocht: overige cloudomgevingen, endpoints buiten gekoppeld beheer, on-premises infrastructuur, fysieke beveiliging, personeel, leveranciers en bedrijfsprocessen.
- Een ontbrekende of niet-beschikbare databron verlaagt de aantoonbaarheid; zij bewijst niet dat een maatregel ontbreekt.
- Handmatig bewijs blijft de verantwoordelijkheid van de organisatie en moet op authenticiteit, actualiteit, volledigheid en toepassingsbereik worden beoordeeld.
- Sectorale en nadere ministeriële regels kunnen aanvullende verplichtingen stellen en moeten afzonderlijk worden vastgesteld.

Beoordelingsmoment

Momentopname: 08-08-2026 08:48 UTC. Bronintegriteit: SHA-256 2baea323997ea04952722d5e831fe72a75673d7ccbc4b0ddb7300bee55be2454. Wijzigingen na dit moment vallen buiten dit rapport.

Risicoregister en scopeverklaring

Formeel risicoregister

Geen formeel risicoregister in de bewijskluis vastgelegd. Voeg minimaal risico-ID, omschrijving, eigenaar, kans, impact, bestaande beheersing, behandeling, restrisico, acceptatie en reviewdatum toe.

Statement of Applicability / scopeverklaring

Geen formele scopeverklaring vastgelegd. Leg systemen, vestigingen, processen, gegevensstromen, leveranciers, uitsluitingen, motivering, eigenaar en bestuurlijke goedkeuring vast.

Incidenten- en meldingsregister

Meldplicht: NIS2 art. 23 en Cbw art. 25-29. Leg per mogelijk significant incident de beoordeling en alle meldmomenten vast, inclusief ontvangst- of referentienummers. De wettelijke beoordeling blijft organisatiespecifiek.

Geen incidenten in het dossier. Dit betekent alleen dat geen incidentregistraties zijn aangetroffen; het bewijst niet dat zich geen incidenten hebben voorgedaan.

Minimale volledigheidscontrole meldingsdossier

- detectie- en classificatietijd, impact, getroffen diensten en significantiebeoordeling;
- vroegtijdige waarschuwing binnen 24 uur waar vereist;
- incidentmelding binnen 72 uur waar vereist;
- tussentijds voortgangsverslag indien gevraagd of noodzakelijk;
- eindverslag uiterlijk een maand na de melding, of voortgang bij een nog lopend incident;
- ontvanger, verzendbewijs, ontvangstbevestiging, referentienummer en verantwoordelijke.

Risicoanalyse en beveiligingsbeleid

NIS2 art. 21 lid 2(a) · Cbw art. 21 lid 3(a) · Cbb art. 6-7

Aantoonbaar · 92%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
Beveiligingsbeleid gedocumenteerd	Aantoonbaar	critical	Michael, Kerker	Handmatig bewijs	
Risicoanalyse uitgevoerd (<=12 maanden)	Aantoonbaar	critical	Michael, Kerker	Handmatig bewijs	
Toegangsbeleid technisch afdwingen (CA)	Niet aantoonbaar	high		Conditional Access	
Jaarlijkse beleidsreview gedocumenteerd	Gedeeltelijk	high	Sven de Vries	Handmatig bewijs	Leg reviewdatum en goedkeuring vast per beleidsdocument.
NIS2-toepassingsbesluit bestuur	Aantoonbaar	critical	Sven de Vries	Handmatig bewijs	

Beveiligingsbeleid gedocumenteerd

- Informatiebeveiligingsbeleid · ref: DOC-A1-POLICY-DOC · datum: 2026-03-03 · geldig tot: 2027-02-26 · bijlage: Informatiebeveiligingsbeleid.docx

Risicoanalyse uitgevoerd (<=12 maanden)

- Risicoanalyse netwerk- en informatiesystemen · ref: DOC-A1-RISK-ANALYSIS · datum: 2026-04-02 · geldig tot: 2027-03-28 · bijlage: Risicoanalyse_netwerk-_en_informatiesystemen.docx

Jaarlijkse beleidsreview gedocumenteerd

- Verslag jaarlijkse beleidsreview · ref: DOC-A1-ANNUAL-REVIEW · datum: 2025-09-04 · geldig tot: 2026-08-30 · bijlage: Verslag_jaarlijkse_beleidsreview.docx

NIS2-toepassingsbesluit bestuur

- Toepassingsbesluit NIS2 · ref: DOC-A1-SCOPE · datum: 2026-05-02 · geldig tot: 2027-04-27 · bijlage: Toepassingsbesluit_NIS2.docx

Incidentafhandeling

NIS2 art. 21 lid 2(b) en art. 23 · Cbw art. 21 lid 3(b) en art. 25-29 · Cbb art. 8

Niet aantoonbaar · 58%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
Auditlog actief en aantoonbaar bewaard	Niet aantoonbaar	critical		Audit Log	
Incidentdetectie actief	Niet aantoonbaar	critical		Security Center	
Incidentrespons-procedures gedocumenteerd	Niet aantoonbaar	high	Noor Jansen	Handmatig bewijs	Leg respons-procedures vast inclusief verantwoordelijken, escalatie en communicatieplan.
24-uurs meldprocedure NCSC/toezichthouder	Aantoonbaar	critical	Noor Jansen	Handmatig bewijs	
72-uurs gedetailleerde melding gedocumenteerd	Gedeeltelijk	critical	Noor Jansen	Handmatig bewijs	Procedure voor gedetailleerde melding binnen 72 uur moet zijn vastgesteld.
Eindverslag binnen 1 maand gedocumenteerd	Niet aantoonbaar	critical		Handmatig bewijs	Artikel 23 kent drie termijnen: 24 uur vroegtijdige waarschuwing, 72 uur melding en een eindverslag binnen een maand. Leg ook die derde stap vast.
Incidentrespons getest (tabel-oefening/drill)	Niet aantoonbaar	medium		Handmatig bewijs	Jaarlijkse test van incidentrespons aantoonbaar maken via oefenrapport.

Incidentrespons-procedures gedocumenteerd

- Incidentresponsprocedure · ref: DOC-A2-SOAR · datum: 2026-02-01 · geldig tot: 2027-01-27 · bijlage: Incidentresponsprocedure.docx

24-uurs meldprocedure NCSC/toezichthouder

- Meldprocedure 24-uurs vroegtijdige waarschuwing · ref: DOC-A2-24H · datum: 2026-05-02 · geldig tot: 2027-04-27 · bijlage: Meldprocedure_24-uurs_vroegtijdige_waarschuwing.docx

72-uurs gedetailleerde melding gedocumenteerd

- Sjabloon 72-uurs incidentmelding · ref: DOC-A2-72H · datum: 2026-06-01 · geldig tot: 2027-05-27 · bijlage: Sjabloon_72-uurs_incidentmelding.docx

Bedrijfscontinuïteit, back-up en crisisbeheer

NIS2 art. 21 lid 2(c) · Cbw art. 21 lid 3(c) · Cbb art. 9

Gedeeltelijk · 67%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
Back-upbeleid gedocumenteerd	Aantoonbaar	critical	Daan Bakker	Handmatig bewijs	
Exchange-archivering actief (>=80% mailboxen)	Niet aantoonbaar	high		Mailbox Health	
DR-procedure en RTO/RPO gedocumenteerd	Aantoonbaar	critical	Daan Bakker	Handmatig bewijs	
Crisismanagementplan aanwezig	Aantoonbaar	high	Sven de Vries	Handmatig bewijs	
Back-upherstel getest (<=12 maanden)	Niet aantoonbaar	high	Daan Bakker	Handmatig bewijs	Hersteltest aantoonbaar maken via testrapport.

Back-upbeleid gedocumenteerd

- Back-up- en herstelbeleid · ref: DOC-A3-BACKUP-POLICY · datum: 2026-01-02 · geldig tot: 2026-12-28 · bijlage: Back-up-_en_herstelbeleid.docx

DR-procedure en RTO/RPO gedocumenteerd

- Uitwijkplan met RTO en RPO · ref: DOC-A3-DR-PLAN · datum: 2026-02-01 · geldig tot: 2027-01-27 · bijlage: Uitwijkplan_met_RTO_en_RPO.docx

Crisismanagementplan aanwezig

- Crisismanagementplan · ref: DOC-A3-CRISIS · datum: 2025-12-03 · geldig tot: 2026-11-28 · bijlage: Crisismanagementplan.docx

Back-upherstel getest (<=12 maanden)

- Rapport hersteltest · ref: DOC-A3-TEST · datum: 2025-10-04 · geldig tot: 2026-09-29 · bijlage: Rapport_hersteltest.docx

Leveranciers- en ketenbeveiliging

NIS2 art. 21 lid 2(d) · Cbw art. 21 lid 3(d) · Cbb art. 10

Gedeeltelijk · 75%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
App-toestemmingen gereviewd (geen kritiek)	Niet aantoonbaar	high		App Consent Health	
Gastgebruikers gereviewd	Niet aantoonbaar	medium		Guest Governance	
Leverancierscontracten met beveiligingseisen	Aantoonbaar	critical	Sven de Vries	Handmatig bewijs	
Jaarlijkse leveranciersbeoordeling	Niet aantoonbaar	high	Sven de Vries	Handmatig bewijs	Periodieke review van leveranciersrisico's documenteren.

Leverancierscontracten met beveiligingseisen

- Beveiligingsbijlage leveranciersovereenkomsten · ref: DOC-A4-VENDOR-CONTRACTS · datum: 2025-11-03 · geldig tot: 2027-10-24 · bijlage: Beveiligingsbijlage_leveranciersovereenkomsten.docx

Jaarlijkse leveranciersbeoordeling

- Jaarlijkse leveranciersbeoordeling · ref: DOC-A4-VENDOR-REVIEW · datum: 2026-03-03 · geldig tot: 2027-02-26 · bijlage: Jaarlijkse_leveranciersbeoordeling.docx

Kwetsbaarhedenbeheer en veilige wijzigingen

NIS2 art. 21 lid 2(e) · Cbw art. 21 lid 3(e) · Cbb art. 11

Gedeeltelijk · 50%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
Legacy-authenticatie geblokkeerd	Niet aantoonbaar	high		Conditional Access	Blokkeer legacy-auth via CA-policy; basisbeveiliging tegen MFA-bypass.
Patch- en updatebeleid gedocumenteerd	Aantoonbaar	high	Daan Bakker	Handmatig bewijs	
Geen verlopen abonnementen (diensten actief)	Niet aantoonbaar	medium		Licentie-kalender	
Threat Intelligence gemonitord	Niet aantoonbaar	medium		Threat Intel	
Wijzigingsbeheer-procedure gedocumenteerd	Aantoonbaar	medium	Daan Bakker	Handmatig bewijs	
Vulnerability Disclosure Policy (VDP) gepubliceerd	Niet aantoonbaar	medium		Handmatig bewijs	Publiceer een proces voor het ontvangen en afhandelen van kwetsbaarheidsmeldingen over eigen systemen (bijv. security.txt of een meldpunt).

Patch- en updatebeleid gedocumenteerd

- Patch- en updatebeleid · ref: DOC-A5-PATCH-POLICY · datum: 2026-02-01 · geldig tot: 2027-01-27 · bijlage: Patch-_en_updatebeleid.docx

Wijzigingsbeheer-procedure gedocumenteerd

- Wijzigingsbeheerprocedure · ref: DOC-A5-CHANGE-MGMT · datum: 2026-01-02 · geldig tot: 2027-12-23 · bijlage: Wijzigingsbeheerprocedure.docx

Effectiviteitscontrole van maatregelen

NIS2 art. 21 lid 2(f) · Cbw art. 21 lid 3(f) · Cbb art. 18

Aantoonbaar · 100%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
Regelmatige security-monitoring aangetoond	Niet aantoonbaar	critical		Run History	
Secure Score trend positief of stabiel	Niet aantoonbaar	medium		Secure Score	
Interne audit uitgevoerd (<=12 maanden)	Aantoonbaar	high	Noor Jansen	Handmatig bewijs	
KPI's / metrics beveiligingspostuur vastgelegd	Aantoonbaar	medium	Noor Jansen	Handmatig bewijs	
Bestuursrapportage cybersecurity	Aantoonbaar	high	Sven de Vries	Handmatig bewijs	

Interne audit uitgevoerd (<=12 maanden)

- Interne auditrapportage beveiligingsmaatregelen · ref: DOC-A6-INTERNAL-AUDIT · datum: 2026-02-01 · geldig tot: 2027-01-27 · bijlage: Interne_auditrapportage_beveiligingsmaatregelen.docx

KPI's / metrics beveiligingspostuur vastgelegd

- Kritieke prestatie-indicatoren beveiliging · ref: DOC-A6-KPIS · datum: 2026-05-02 · geldig tot: 2027-04-27 · bijlage: Kritieke_prestatie-indicatoren_beveiliging.docx

Bestuursrapportage cybersecurity

- Kwartaalrapportage cybersecurity aan de directie · ref: DOC-A6-BOARD-REPORT · datum: 2026-06-01 · geldig tot: 2026-11-28 · bijlage: Kwartaalrapportage_cybersecurity_aan_de_directie.docx

Cyberhygiëne en training

NIS2 art. 20 en art. 21 lid 2(g) · Cbw art. 24 en art. 21 lid 3(g) · Cbb art. 12 en 20-22

Niet aantoonbaar · 60%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
Beveiligingstraining medewerkers (jaarlijks)	Aantoonbaar	critical	Lotte Smit	Handmatig bewijs	
Bewustzijnsprogramma cybersecurity	Aantoonbaar	high	Lotte Smit	Handmatig bewijs	
Phishing-simulatie of social engineering test	Niet aantoonbaar	medium		Handmatig bewijs	Testrapport van phishing-simulatie of vergelijkbare oefening.
Bestuursleden: cybersecurity-kennis aantoonbaar	Niet aantoonbaar	critical		Handmatig bewijs	NIS2 Art. 20: bestuur moet cyberbeveiligingstraining volgen.
Acceptabel gebruik-beleid getekend	Aantoonbaar	medium	Lotte Smit	Handmatig bewijs	

Beveiligingstraining medewerkers (jaarlijks)

- Certificaat beveiligingstraining medewerkers · ref: DOC-A7-TRAINING · datum: 2025-11-03 · geldig tot: 2026-10-29 · bijlage: Certificaat_beveiligingstraining_medewerkers.docx

Bewustzijnsprogramma cybersecurity

- Programma beveiligingsbewustzijn · ref: DOC-A7-AWARENESS · datum: 2026-04-02 · geldig tot: 2027-03-28 · bijlage: Programma_beveiligingsbewustzijn.docx
- Bewustzijnsprogramma cybersecurity

Acceptabel gebruik-beleid getekend

- Gedragsregels acceptabel gebruik · ref: DOC-A7-ACCEPTABLE-USE · datum: 2025-10-04 · geldig tot: 2027-09-24 · bijlage: Gedragsregels_acceptabel_gebruik.docx

Cryptografie en versleuteling

NIS2 art. 21 lid 2(h) · Cbw art. 21 lid 3(h) · Cbb art. 13

Aantoonbaar · 80%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
DMARC p=reject alle domeinen	Niet aantoonbaar	high		Domain Health	Verhoog DMARC naar p=reject; beschermt tegen e-mail-spoofing.
SPF correct geconfigureerd	Niet aantoonbaar	high		Domain Health	
DKIM geconfigureerd op alle domeinen	Niet aantoonbaar	high		Domain Health	
MTA-STS (TLS-afdwinging inkomende e-mail)	Niet aantoonbaar	medium		Domain Health	
Cryptografiebeleid gedocumenteerd	Aantoonbaar	high	Daan Bakker	Handmatig bewijs	
Geen risicovolle transportregels actief	Niet aantoonbaar	medium		Exchange Transport	

Cryptografiebeleid gedocumenteerd

- Cryptografiebeleid · ref: DOC-A8-CRYPTO-POLICY · datum: 2025-12-03 · geldig tot: 2027-11-23 · bijlage: Cryptografiebeleid.docx

Personeelsbeveiliging, toegangsbeheer en assetbeheer

NIS2 art. 21 lid 2(i) · Cbw art. 21 lid 3(i) · Cbb art. 14-16

Gedeeltelijk · 77%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
Alle admins met MFA	Niet aantoonbaar	critical		MFA Coverage	
Global Admins <=4 (least privilege)	Niet aantoonbaar	high		Admin Rollen	
PIM actief (JIT-toegang beheerders)	Niet aantoonbaar	high		Privilege Creep	
Geen ghost admins gevonden	Niet aantoonbaar	high		Ghost Admin	
Offboarding-procedure gedocumenteerd	Aantoonbaar	high	Lotte Smit	Handmatig bewijs	
Assetinventaris ICT-systemen actueel	Niet aantoonbaar	medium		Handmatig bewijs	Bijgewerkte inventaris van hardware, software en cloudservices.
Data-retentie & -vernietigingsbeleid	Aantoonbaar	medium	Sven de Vries	Handmatig bewijs	
Fysieke toegangsbeveiliging	Niet aantoonbaar	low		Handmatig bewijs	Borg fysieke toegang tot kantoor/apparatuur en leg de fysieke beveiliging van de cloud-provider vast (datacenter-certificering).
Geen externe mailbox-forwarding actief	Niet aantoonbaar	high		Mailbox Health	

Offboarding-procedure gedocumenteerd

- Offboardingprocedure · ref: DOC-A9-OFFBOARDING · datum: 2026-03-03 · geldig tot: 2027-02-26 · bijlage: Offboardingprocedure.docx

Data-retentie & -vernietigingsbeleid

- Beleid gegevensbewaring en -vernietiging · ref: DOC-A9-DATA-RETENTION · datum: 2026-01-02 · geldig tot: 2027-12-23 · bijlage: Beleid_gegevensbewaring_en_-vernietiging.docx

MFA en beveiligde communicatie

NIS2 art. 21 lid 2(j) · Cbw art. 21 lid 3(j) · Cbb art. 15

Niet aantoonbaar · 62%

Maatregel	Bewijsstatus	Krit.	Eigenaar	Bron	Gap
MFA-dekking >=95% alle gebruikers	Niet aantoonbaar	critical		MFA Coverage	
100% admins met MFA (dubbele check)	Niet aantoonbaar	critical		MFA Coverage	
CA: MFA afdwingen technisch	Aantoonbaar	critical	MK Cloud & IT	Conditional Access	
Passwordless-methoden aanwezig (FIDO2/WHfB)	Niet aantoonbaar	low		MFA Coverage	
Beleid beveiligde communicatiekanalen	Niet aantoonbaar	medium		Handmatig bewijs	Beleid voor gebruik van beveiligde communicatiemiddelen (versleuteld, geauthenticeerd).

CA: MFA afdwingen technisch

- CA: MFA afdwingen technisch

Bewijsregister en integriteit

Maatregel	Bewijs	Referentie / bestand	Datum	Geldig tot	Hash
a1_policy_doc	Informatiebeveiligingsbeleid	DOC-A1-POLICY-DOC	2026-03-03	2027-02-26	Niet vastgelegd
a1_risk_analysis	Risicoanalyse netwerk- en informatiesystemen	DOC-A1-RISK-ANALYSIS	2026-04-02	2027-03-28	Niet vastgelegd
a1_annual_review	Verslag jaarlijkse beleidsreview	DOC-A1-ANNUAL-REVIEW	2025-09-04	2026-08-30	Niet vastgelegd
a1_scope	Toepassingsbesluit NIS2	DOC-A1-SCOPE	2026-05-02	2027-04-27	Niet vastgelegd
a2_soar	Incidentresponsprocedure	DOC-A2-SOAR	2026-02-01	2027-01-27	Niet vastgelegd
a2_24h	Meldprocedure 24-uurs vroegtijdige waarschuwing	DOC-A2-24H	2026-05-02	2027-04-27	Niet vastgelegd
a2_72h	Sjabloon 72-uurs incidentmelding	DOC-A2-72H	2026-06-01	2027-05-27	Niet vastgelegd
a3_backup_policy	Back-up- en herstelbeleid	DOC-A3-BACKUP-POLICY	2026-01-02	2026-12-28	Niet vastgelegd
a3_dr_plan	Uitwijkplan met RTO en RPO	DOC-A3-DR-PLAN	2026-02-01	2027-01-27	Niet vastgelegd
a3_crisis	Crisismanagementplan	DOC-A3-CRISIS	2025-12-03	2026-11-28	Niet vastgelegd
a3_test	Rapport hersteltest	DOC-A3-TEST	2025-10-04	2026-09-29	Niet vastgelegd
a4_vendor_contracts	Beveiligingsbijlage leveranciersovereenkomsten	DOC-A4-VENDOR-CONTRACTS	2025-11-03	2027-10-24	Niet vastgelegd
a4_vendor_review	Jaarlijkse leveranciersbeoordeling	DOC-A4-VENDOR-REVIEW	2026-03-03	2027-02-26	Niet vastgelegd
a5_patch_policy	Patch- en updatebeleid	DOC-A5-PATCH-POLICY	2026-02-01	2027-01-27	Niet vastgelegd
a5_change_mgmt	Wijzigingsbeheerprocedure	DOC-A5-CHANGE-MGMT	2026-01-02	2027-12-23	Niet vastgelegd
a6_internal_audit	Interne auditrapportage beveiligingsmaatregelen	DOC-A6-INTERNAL-AUDIT	2026-02-01	2027-01-27	Niet vastgelegd
a6_kpis	Kritieke prestatie-indicatoren beveiliging	DOC-A6-KPIS	2026-05-02	2027-04-27	Niet vastgelegd
a6_board_report	Kwartaalrapportage cybersecurity aan de directie	DOC-A6-BOARD-REPORT	2026-06-01	2026-11-28	Niet vastgelegd
a7_training	Certificaat beveiligingstraining medewerkers	DOC-A7-TRAINING	2025-11-03	2026-10-29	Niet vastgelegd
a7_awareness	Programma beveiligingsbewustzijn	DOC-A7-AWARENESS	2026-04-02	2027-03-28	Niet vastgelegd
a7_awareness	Bewustzijnsprogramma cybersecurity	Geen referentie	Niet vastgelegd	Niet vastgelegd	Niet vastgelegd
a7_acceptable_use	Gedragsregels acceptabel gebruik	DOC-A7-ACCEPTABLE-USE	2025-10-04	2027-09-24	Niet vastgelegd
a8_crypto_policy	Cryptografiebeleid	DOC-A8-CRYPTO-POLICY	2025-12-03	2027-11-23	Niet vastgelegd
a9_offboarding	Offboardingprocedure	DOC-A9-OFFBOARDING	2026-03-03	2027-02-26	Niet vastgelegd
a9_data_retention	Beleid gegevensbewaring en -vernietiging	DOC-A9-DATA-RETENTION	2026-01-02	2027-12-23	Niet vastgelegd
a10_ca_mfa	CA: MFA afdwingen technisch	Geen referentie	Niet vastgelegd	Niet vastgelegd	Niet vastgelegd

De rapportvingerafdruk beschermt de samenstelling van de voor dit rapport gebruikte gegevens. Een bestandsspecifieke hash is alleen aantoonbaar wanneer die per bewijsitem is vastgelegd. Bewaar bronbestanden versiebeheerd en wijzigingsbestendig.

Openstaande dossieronderdelen

Dossieronderdeel	Status
Toepasselijkheid formeel vastgesteld	Vastgelegd
Sector en subsector vastgelegd	OPEN - aanvullen
Bevoegde toezichthouder vastgelegd	OPEN - aanvullen
CSIRT / meldloket vastgelegd	OPEN - aanvullen
Registratie afgerond of gemotiveerd niet van toepassing	Vastgelegd
Bestuurlijke goedkeuring vastgelegd	Vastgelegd
Bestuursopleiding aantoonbaar	OPEN - aanvullen
Formeel risicoregister aanwezig	OPEN - aanvullen
Scopeverklaring goedgekeurd	OPEN - aanvullen
Documentreview vastgelegd	OPEN - aanvullen
Formele ondertekening aanwezig	OPEN - aanvullen

8 van de 11 formele dossieronderdelen zijn nog niet volledig vastgelegd. Het rapport is technisch gegenereerd, maar het dossier is pas bestuurlijk gereed nadat deze punten zijn beoordeeld, aangevuld en goedgekeurd.

Deze controle is geen juridisch nalevingsoordeel.

Sectorale en organisatiebrede restcontrole

- Controleer aanvullende sectorale wetgeving, toezichteisen en ministeriële regelingen.
- Bevestig dekking van niet-Microsoft-365-systemen, fysieke beveiliging, personeel, processen en leveranciers.
- Laat toepasselijkheid, uitzonderingen en meldplicht juridisch of door de bevoegde functionaris beoordelen.
- Laat bewijssteekproeven en ontwerp/werking van maatregelen onafhankelijk toetsen waar passend.

Formele vaststelling en ondertekening

Rol / besluit	Vastlegging
Rapporteigenaar	Niet vastgelegd
Beoordeeld door	Niet vastgelegd
Reviewdatum	Niet vastgelegd
Goedgekeurd door bestuur	Niet vastgelegd
Goedkeuringsdatum	Niet vastgelegd
Besluit / opmerkingen	Niet vastgelegd

Naam en functie: _____

Datum: _____ Handtekening: _____

Ondertekening bevestigt beoordeling en bestuurlijke vaststelling van dit dossier; zij verandert de portalmeting niet in een certificering of juridische complianceverklaring.

Bijlage A - Officiële rechtsbronnen

Instrument	Artikelen / onderwerp	Officiële bron
NIS2-richtlijn (EU) 2022/2555	Art. 2-3 toepassingsbereik; art. 20 bestuur; art. 21 risicobeheer; art. 23 meldplicht	https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32022L2555
Cyberbeveiligingswet, Stb. 2026, 187	Art. 21 zorgplicht; art. 24 bestuur; art. 25-29 incidentmelding; art. 43-47 registratie	https://www.officielebekendmakingen.nl/stb-2026-187.html
Cyberbeveiligingsbesluit, Stb. 2026, 189	Art. 6-18 nadere zorgplichtmaatregelen; art. 20-22 bestuursopleiding	https://zoek.officielebekendmakingen.nl/stb-2026-189.html

Juridische disclaimer

Dit rapport ondersteunt ICT-readiness en bewijsvoering voor NIS2 en de Nederlandse Cyberbeveiligingswet. Het is geen formele audit, certificering, CYRA-erkenning, juridisch advies of garantie van naleving. De organisatie blijft verantwoordelijk voor toepasselijkheid, juistheid en volledigheid van gegevens, de volledige organisatiebrede scope, tijdige registraties en meldingen, en beoordeling van sectorale of nadere regels.