Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De Cyberbeveiligingswet

Van regels naar resultaat!

Roel Wijmenga (BZK) &
Edwin Hummel (ADR / NOREA)

Odido: hackers lieten medewerker klantenservice inloggen op phishingsite

woensdag 13 mei 2026, 09:43 door **Redactie**, 2 **reacties**

De hackers die bij Odido de gegevens van ruim zes miljoen mensen wisten te stelen konden toegang krijgen omdat ze een medewerker van de klantenservice lieten inloggen op een phishingsite, waardoor de inloggegevens van het account konden worden gestolen. Het gehackte account, dat toegang gaf tot de werkomgeving, werd binnen een uur geblokkeerd. De klantgegevens waren toen al gedownload, zo laat Odido tegenover de **NOS** weten.

Aandelen West Pharmaceutical dalen nadat cyberaanval wereldwijde activiteiten verstoort

Gepubliceerd op 12-05-2026 om 20:35

MT Newswires - Vertaald door MarketScreener ⓘ - Origineel bekijken

Delen

Live: Universiteit trekt stekker uit Canvas na mogelijk nieuwe hack door ShinyHunters (beëindigd)

Cloudflare-storing die wereldwijd websites lam legde lijkt opgelost

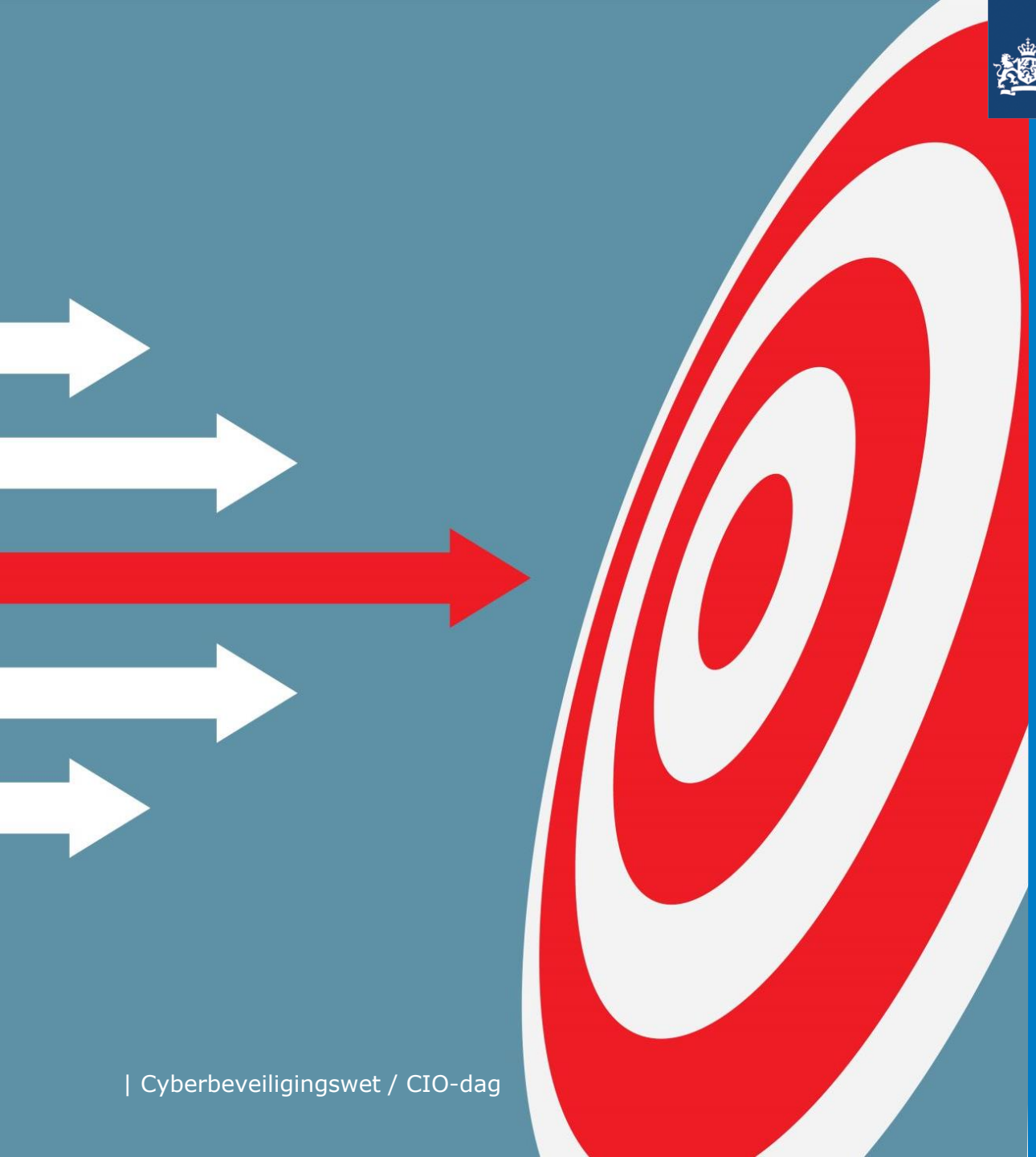
AIVD waarschuwt voor hacks en storingen, want andere landen proberen vaker Nederlandse ICT-systemen binnen te dringen

Inhoud

- Introductie in de CBW
- Wat moet uw organisatie gaan doen?
- Voldoet uw organisatie al aan de CBW?
- CBW-framework als hulpmiddel
- Meer info en vragen?

Inhoud

- **Introductie in de CBW**
- Wat moet uw organisatie gaan doen?
- Voldoet uw organisatie al aan de CBW?
- CBW-framework als hulpmiddel
- Meer info en vragen?



Doel NIS2

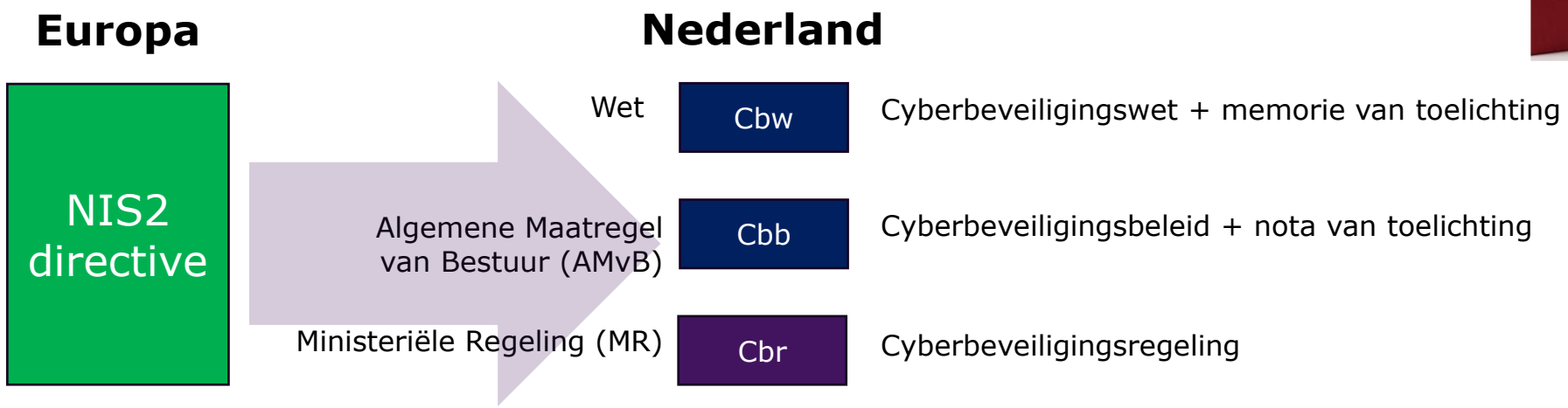
Het doel van NIS2 is om de cyberbeveiliging en de weerbaarheid van essentiële en belangrijke diensten in EU-lidstaten te verbeteren.

Wetgevingstraject (update juni 2026)

	Opstellen	(Internet) consultatie	Raad van state	Tweede kamer	Eerste kamer	Inwerking-treding
Wet (Cbw)	Gereed mei 2024	Gereed juni 2024	Gereed maart 2025	Gereed maart 2026	Q2 2026	Q3 2026
AMvB (Cbb)	Gereed feb 2025	Gereed maart 2025	Gereed mei 2026	→ Verwerking naar finale versie		Q3 2026
MR (Cbr)	Gereed dec 2025	Gereed jan 2026	→			Q3 2026

Behandeling eerste kamer 6 juni 2026

Opbouw van de Cyberbeveiligingswet



De “Network and Information Security 2” (NIS2) directive is een verplichting uit Europa voor een land om een wet te maken. Voor Nederland is dit de Cyberbeveiligingswet (Cbw).

De wet, AMvB en MR zijn gezamenlijk de invulling van de NIS2 directive.

Opbouw van de Cyberbeveiligingswet

- De Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb) gelden voor **alle** sectoren;

- Er komen meerdere Cyberbeveiligingsregelingen
  - Cyberbeveiligingsregeling Overheid
  - Cyberbeveiligingsregeling in de Zorg
  - Cyberbeveiligingsregeling IenW
  - Enz.

Opbouw van de Cyberbeveiligingswet

Gezamenlijk,
voor alle sectoren
onder de Cbw

Wet — Cbw

Algemene Maatregel van Bestuur (AMvB) — Cbb

Ministeriële Regelingen (MR) — CbrO, ..., ...

Per sector, dus ook een regeling voor de overheid

- Cruciale netwerk en informatiesystemen
  - Zorgplicht
    - BIO2
      - NEN 27001
      - NEN 27002/ NEN 7510/CSIR
    - Leidraad TBB
  - Meldplicht
    - Meldcriteria
      - Impacttabel IBD
- CSIRT bepalingen IBD
- Ontheffingen

Nederlandse bedrijven wekenlang ongemerkt gehackt

Nederlandse organisaties hebben gemiddeld 24 dagen lang niet in de gaten dat cybercriminelen toegang hebben tot hun mailboxen. Dat blijkt uit het Incident Response Report 2026 van cybersecuritybedrijf Eye Security. Het onderzoek werpt een licht op de geraffineerde methodes van aanvallers die misbruik maken van het onderlinge vertrouwen binnen bedrijven.

Inhoud

- Introductie in de CBW
- **Wat moet uw organisatie gaan doen?**
- Voldoet uw organisatie al aan de CBW?
- CBW-framework als hulpmiddel
- Meer info en vragen?

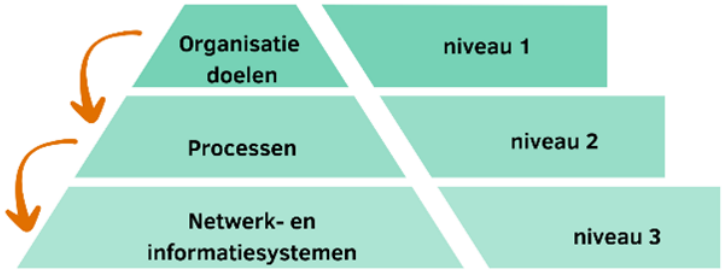
Wat moet uw organisatie gaan doen?

- Hopelijk al gedaan:
  - Bepalen of uw organisatie aan de Overheidscriteria van de Cbw voldoet en zo in de sector overheid valt onder de Cbw;
  - Bepalen of uw organisatie in één van de andere sectoren van de Cbw valt;
    - Een organisatie kan in meerdere sectoren vallen;

Sectoren Cbw (NIS2)	
Energie	Transport
Bankwezen	Infrastructuur financiële markt
Gezondheidszorg	Drinkwater
Digitale infrastructuur	Digitale aanbieders
Afvalwater	**Overheid**
Ruimtevaart	Post- en koeriersdiensten
Afvalstoffen-beheerder	Levensmiddelen
Chemische stoffen	Onderzoek
Vervaardiging/ Manufacturing	

Wat moet uw organisatie gaan doen?

- Implementeren van risicomanagement
  - Bepalen kroonjuwelen
  - Indelen van de kroonjuwelen doormiddel van de TBB systematiek of impact systematiek IBD



Wat moet uw organisatie gaan doen?

- Registreren van de organisatie
  - Zorg dat het Register van Overheidsorganisaties (ROO) up-to-date is.
    - Gegevens uit het ROO worden hergebruikt in de registratie
  - Registreren bij mijn.ncsc.nl
    - Authenticatie SSO-Rijk of E-herkenning
    - Organisatiegegevens
    - Contactgegevens
    - Netwerkgegevens (IP adressen, domeinen en AS nummers)
  - Bepalen
    - Wie gaat registreren
    - Wie gaat melden

Wat moet uw organisatie gaan doen?

- Implementeren van de zorgplicht
  - BIO2
    - (BIO1 al verplicht op basis van zelfregulering voor de rijksoverheid sinds 2019)
    - (BIO2 al verplicht op basis van zelfregulering voor de rijksoverheid sinds september 2025)
    - BIO2 maatregelen nemen op basis van risico’s
      - Inrichten risicomanagement (ISMS)
      - Regelmatig controleren of maatregel nog voldoen (PDCA-cyclus)
      - Calamiteiten plan

Wat moet uw organisatie gaan doen?

- Implementeren van Plan-Do-Check-Act-cyclus
  - Regelmatig niveau van het TBB beoordelen
  - Soort en grote van de dreiging
  - Voldoen genomen maatregelen nog

Wat moet uw organisatie gaan doen?

- Implementeren van de meldplicht
  - Welke systemen zijn meldingsplichtig?
    - Cyberbeveiligingsregeling Overheid (CbrO)
  - Meldproces intern
    - Wie moeten op de hoogte gebracht worden, wie mag beslissen, enz.
    - “Interne” meldingen bijvoorbeeld van agentschap naar ministerie
  - Meldproces richting het meldportaal
    - Wie mag er gaan melden, enz.

Wat moet uw organisatie gaan doen?

- Beleid
  - Leg beleid vast
    - Risicomanagementbeleid
    - Incidentmanagementbeleid
    - Leveranciersmanagementbeleid
    - Enz.
  - Zorg dat het vindbaar is

Wat moet uw organisatie gaan doen?

- Cursus bestuurder
  - Verplicht voor de bestuurder (binnen 2 jaar)
  - Voor anderen niet verplicht wel wenselijk

- “Teach the teacher”
  - Voor pool mensen om intern opleidingen te geven of bij een andere organisatie
  - Presentatie komt beschikbaar voor gehele overheid om zelf aan te vullen met organisatie specifieke onderdelen

Inhoud

- Introductie in de CBW
- Wat moet uw organisatie gaan doen?
- **Voldoet uw organisatie al aan de CBW?**
- CBW-framework als hulpmiddel
- Meer info en vragen?

Waarop gebaseerd?

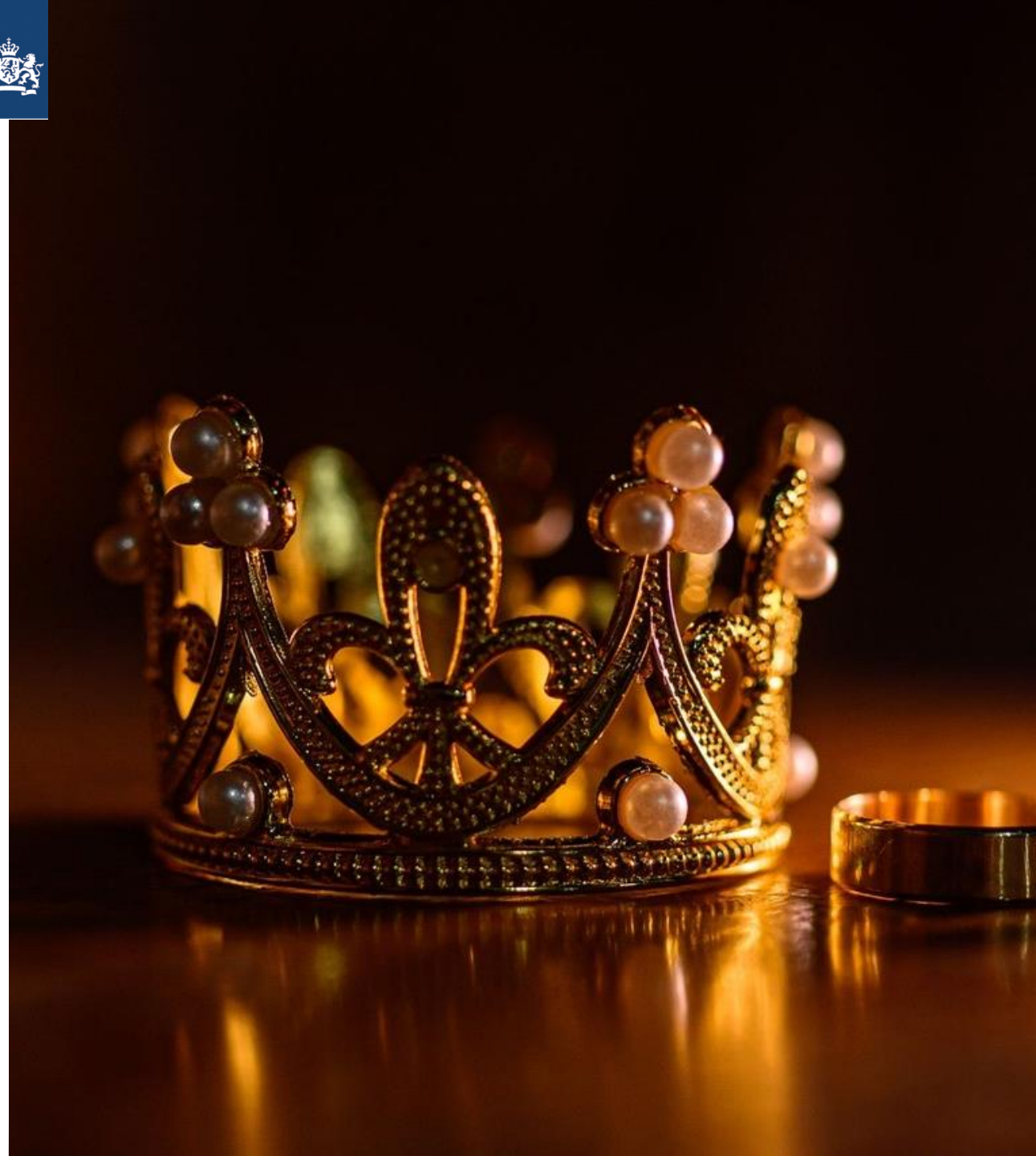
Onderzoeken van de ADR op cyberbeveiliging de afgelopen 3 jaar:

- pentesten
- Digi-D assessments
- GITC-onderzoeken (mn. financiële systemen)
- Diverse red-teaming onderzoeken en micro-aanvalssimulaties
- Beheeronderzoek naar sturing op financiële systemen
- Aangevuld met onze departementale I-scans

Te verschijnen: Publieke management letter Digitale weerbaarheid in verbonden ecosystemen van NOREA

Stand van zaken

- Risico-management
- Bevorderen van veilig gedrag
- Beschermen van systemen
- Toegangsrechten
- Continuiteitsmanagement



Mijn boodschap:

Kwetsbaar opstellen om kwetsbaarheden te voorkomen!

Inhoud

- Introductie in de CBW
- Wat moet uw organisatie gaan doen?
- Voldoet uw organisatie al aan de CBW?
- **CBW-framework als hulpmiddel**
- Meer info en vragen?

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Auditdienst Rijk
Ministerie van Financiën

Studierapport Cbw (NIS2) Control Framework

Een praktisch framework bij de implementatie van de Cyberbeveiligingswet (NIS2-richtlijn), voor het versterken van de digitale operationele weerbaarheid.

Auteurs
L.M. Molewijk, ADR
S. Gangaram Panday, Brightlyn
E. Hummel, ADR
T. Meeuws, ADR

Auditdienst Rijk
Postbus 20201, 2500 EE Den Haag
Telefoon: 088 – 442 80 00
E-mail: adrcommunicatie@minfin.nl

NOREA
Postbus 242, 2130 AE Hoofddorp
Telefoon: 088 – 496 03 80
E-mail: norea@norea.nl

Cbw (NIS2) Control Framework is endorsed by

Statement from the NCSC and the Dutch supervisory authorities

“Het NCSC en de Cbw-toezichthouders hebben kennisgenomen van het kader ontwikkeld door ADR en NOREA, dat erop gericht is de sector een framework te bieden voor de praktische implementatie van de Cbw, Cbb en sectorspecifieke eisen. Hoewel NCSC en de Cbw-toezichthouders niet hebben bijgedragen aan de ontwikkeling ervan of een diepgaande beoordeling hebben uitgevoerd, zien ze de creatie van dergelijke kaders als een goede invulling op hun eerdere oproepen tot sectorbrede samenwerking. Deze samenwerking is cruciaal voor het verbeteren van de algehele cyberweerbaarheid van de sector en, waar gewenst, gezamenlijk ontwikkelen en bijwerken van standaarden die aan dit doel kunnen bijdragen. NCSC en de Cbw-toezichthouders benadrukken dat naleving van de toepasselijke wetten en voorschriften de verantwoordelijkheid blijft van elke organisatie. Het kader kan organisaties helpen hun aanpak te structureren en te versterken, maar het blijft altijd de verantwoordelijkheid van de organisatie zelf om te beoordelen of zij volledig voldoen aan de toepasselijke wet- en regelgeving.”

Key features of the framework


NOREA

Auditdienst Rijk
Ministerie van Financiën

Studierapport Cbw (NIS2)
Control Framework

Een praktisch framework bij de implementatie van de Cyberbeveiligingswet (NIS2-richtlijn), voor het versterken van de digitale operationele weerbaarheid.

Auteurs
L.M. Molewijk, ADR
S. Gangaram Panday, Brightlyn
E. Hummel, ADR
T. Meeuws, ADR

Auditdienst Rijk
Postbus 20201, 2500 EE Den Haag
Telefoon: 088 – 442 80 00

NOREA
Postbus 242, 2130 AE Hoofddorp
Telefoon: 088 – 496 03 80


Actionable controls


Modular

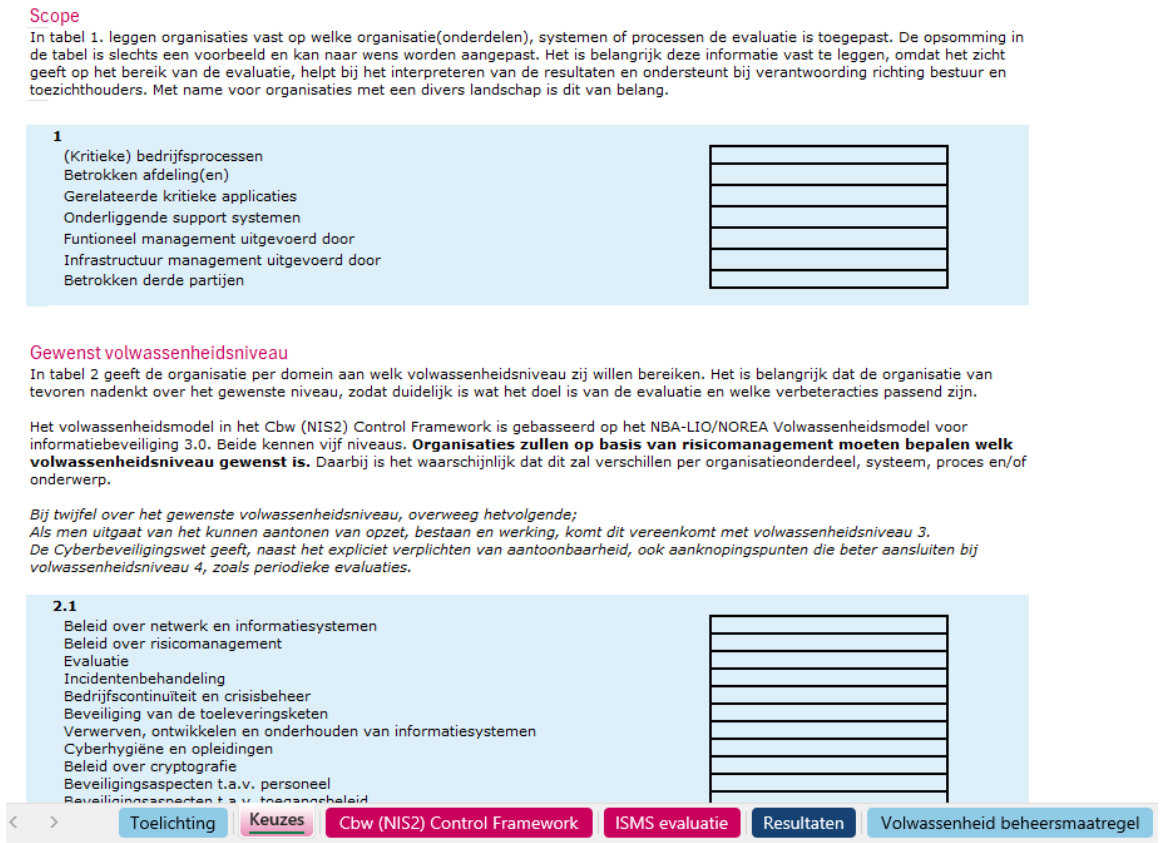

Management system


Maturity model


Management dashboard


Mappings

Scope definition



Scope

In tabel 1. leggen organisaties vast op welke organisatie(onderdelen), systemen of processen de evaluatie is toegepast. De opsomming in de tabel is slechts een voorbeeld en kan naar wens worden aangepast. Het is belangrijk deze informatie vast te leggen, omdat het zicht geeft op het bereik van de evaluatie, helpt bij het interpreteren van de resultaten en ondersteunt bij verantwoording richting bestuur en toezichthouders. Met name voor organisaties met een divers landschap is dit van belang.

1	
(Kritieke) bedrijfsprocessen	
Betrokken afdeling(en)	
Gerelateerde kritieke applicaties	
Onderliggende support systemen	
Funtioneel management uitgevoerd door	
Infrastructuur management uitgevoerd door	
Betrokken derde partijen	

Gewenst volwassenheidsniveau

In tabel 2 geeft de organisatie per domein aan welk volwassenheidsniveau zij willen bereiken. Het is belangrijk dat de organisatie van tevoren nadenkt over het gewenste niveau, zodat duidelijk is wat het doel is van de evaluatie en welke verbeteracties passend zijn.

Het volwassenheidsmodel in het Cbw (NIS2) Control Framework is gebasseerd op het NBA-LIO/NOREA Volwassenheidsmodel voor informatiebeveiliging 3.0. Beide kennen vijf niveaus. **Organisaties zullen op basis van risicomanagement moeten bepalen welk volwassenheidsniveau gewenst is.** Daarbij is het waarschijnlijk dat dit zal verschillen per organisatieonderdeel, systeem, proces en/of onderwerp.

Bij twijfel over het gewenste volwassenheidsniveau, overweeg hetvolgende;
Als men uitgaat van het kunnen aantonen van opzet, bestaan en werking, komt dit vereenkomt met volwassenheidsniveau 3.
De Cyberbeveiligingswet geeft, naast het expliciet verplichten van aantoonbaarheid, ook aanknopingspunten die beter aansluiten bij volwassenheidsniveau 4, zoals periodieke evaluaties.

2.1	
Beleid over netwerk en informatiesystemen	
Beleid over risicomanagement	
Evaluatie	
Incidentenbehandeling	
Bedrijfscontinuïteit en crisisbeheer	
Beveiliging van de toeleveringsketen	
Verwerven, ontwikkelen en onderhouden van informatiesystemen	
Cyberhygiëne en opleidingen	
Beleid over cryptografie	
Beveiligingsaspecten t.a.v. personeel	
Beveiligingsaspecten t.a.v. toegangsbeleid	

Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel

Actionable controls

Thema	Domein	Cbw mapping	Control ID	Beheersmaatregel	Toelichting
Governance (art. 24)	Eisen aan de training, de trainer en het certificaat en doel van de training	Cbw art. 24.2 Cbb art. 21, 22, 23	14.1	informatiesystemen te kunnen identificeren en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen. Daarnaast zorgt de training dat ieder bestuurslid in staat is om risicobeheersmaatregelen op het gebied van cyberbeveiliging en de gevolgen daarvan voor de diensten die door de entiteit worden verleend te kunnen beoordelen.	a. de soorten risico's voor netwerk- en informatiesystemen; b. risicomanagementprocessen; c. risicobeoordelingsmethodiek; d. risicobeheersingsmaatregelen op het gebied van cyberbeveiliging (zoals ook vastgelegd in beveiligingsbeleid). Het certificaat van de training, bevat in ieder geval: a. de naam van het lid van het bestuur van de essentiële entiteit of belangrijke entiteit; b. de datum of data waarop de training is gevolgd; c. de behandelde onderwerpen in de training; en d. de naam van de aanbieder van de training. Het certificaat van de training is opgesteld in de Nederlandse taal of de Engelse taal.
		Cbw art. 24.3, 24.4	14.2	Ieder lid van het bestuur van een entiteit voldoet binnen twee jaar aan de trainingseisen. Daarnaast houdt ieder bestuurslid de kennis aantoonbaar actueel.	
	Meldplicht significante incidenten	Cbw art. 25.1, 25.2, 26.1, 33	15.1	De entiteit meldt ieder significant incident aan haar CSIRT en de bevoegde autoriteit.	Een incident is significant als het: a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Vrijwillige meldplicht: elke entiteit heeft de mogelijke om vrijwillig een melding van een incident, bijna-incident of cyberdreiging te doen bij haar CSIRT of bevoegde autoriteit.

Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel | Template | Mapping Uitvoeringsverordening | Mapping BIO2 | Mapping DORA

Modular

	Toelichting	Mapping per Cbw-sector		
		Beheer van ICT-diensten, digitale infrastructuur en digitale aanbieders	Overheid	Bankwezen en infrastructuur voor de financiële markt
		Uitvoeringsverordening (EU) 2024/2690	BIO2	DORA Control Framework
le entiteit worden diensten die door de	a. de soorten risico's voor netwerk- en informatiesystemen; b. risicomanagementprocessen; c. risicobeoordelingsmethodiek; d. risicobeheersingsmaatregelen op het gebied van cyberbeveiliging (zoals ook vastgelegd in beveiligingsbeleid). Het certificaat van de training, bevat in ieder geval: a. de naam van het lid van het bestuur van de essentiële entiteit of belangrijke entiteit; b. de datum of data waarop de training is gevolgd; c. de behandelde onderwerpen in de training; en d. de naam van de aanbieder van de training. Het certificaat van de training is opgesteld in de Nederlandse taal of de Engelse taal.			
ast houdt ieder		Dit onderwerp valt buiten de scope van de Uitvoeringsverordening, hier dient de Cbb gevolgd te worden.	n.v.t.	1.2
	Een incident is significant als het: a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Vrijwillige meldplicht: elke entiteit heeft de mogelijke om vrijwillig een melding van een incident, bijna-incident of cyberdreiging te doen bij haar CSIRT of bevoegde autoriteit.	Art. 3.1 Een incident wordt voor de toepassing van artikel 23, lid 3, van Richtlijn (EU) 2022/2555 met betrekking tot de relevante entiteiten als significant beschouwd indien aan een of meer van de volgende criteria is voldaan: a) het incident heeft voor de relevante entiteit direct financieel verlies veroorzaakt of kan verlies veroorzaken dat hoger is dan 500 000 EUR of meer dan 5 % van de totale jaaromzet van de relevante entiteit in het voorgaande boekjaar, indien dat lager is; b) het incident heeft het uitlekken van bedrijfsgeheimen als bedoeld in artikel 2, punt 1, van Richtlijn (EU) 2016/943 van de relevante entiteit veroorzaakt of kan dit veroorzaken; c) het incident heeft de dood van een natuurlijke persoon veroorzaakt of kan dit veroorzaken; d) het incident heeft aanzienlijke schade aan de gezondheid van een natuurlijke persoon veroorzaakt of kan dit veroorzaken; e) er heeft een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen plaatsgevonden, die ernstige operationele verstoringen kan veroorzaken; f) het incident voldoet aan de criteria van artikel 4; g) het incident voldoet aan een of meer van de criteria van de artikelen 5 tot en met 14. Art 4. Incidenten die afzonderlijk niet als een significant incident in de zin van artikel 3 worden beschouwd, worden gezamenlijk als één significant incident beschouwd indien zij aan alle volgende criteria voldoen: a) zij hebben zich ten minste tweemaal binnen zes maanden voorgedaan; b) zij hebben dezelfde kennelijk onderliggende oorzaak; c) zij voldoen gezamenlijk aan de criteria van artikel 3, lid 1, punt a).	n.v.t.	11.3

Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel | Template | Mapping Uitvoeringsverordening | Mapping BIO2 | Mapping DORA

Management system

Thema	Domein	Control ID	Beheersmaatregel	VNG IBD vragen ISMS	Score zelf-evaluatie
Plan	Context	P.1	De entiteit heeft inzicht in de eigen organisatie en weet binnen welke context zij hun processen en diensten hebben ingericht. Daarnaast is de entiteit zich bewust van de toepasbaarheid van de wetgeving en de grenzen van de wetgeving binnen de eigen organisatie.	Is er documentatie aanwezig die interne en externe factoren geïdentificeerd? Is er een stakeholderanalyse die de belanghebbenden goed in kaart brengt? Zijn de behoeften van belanghebbenden goed in kaart gebracht? Is de reikwijdte van het ISMS bekend, is dit in een apart document of in de contextanalyse opgenomen? Heeft de organisatie bepaald wat zij wil vastleggen en monitoren in het ISMS? Let op: dit kan zo klein zijn als een spreadsheet en ze groot als een GRC-tool.	
	Leiderschap	P.2	Het bestuur van de entiteit toont leiderschap en betrokkenheid met betrekking tot het Informatiebeveiligingsbeleid.	Zijn verantwoordelijkheden voor informatiebeveiliging beschreven en staat hierin opgenomen dat de directie de uiteindelijke verantwoordelijkheid draagt? Is het beleid voor informatiebeveiliging door de directie goedgekeurd? Heeft de directie op enige wijze het informatiebeveiligingsbeleid kenbaar gemaakt naar de medewerkers en daarbij het belang van informatiebeveiliging uitgesproken? Zijn voor het ISMS en voor informatiebeveiliging benodigde middelen beschikbaar? D.w.z. zijn er budget en personen beschikbaar om uitvoer te geven aan de acties die nodig zijn i.h.k.v. het ISMS en informatiebeveiliging? Worden planningen, acties en bevindingen via de reguliere P&C cyclus gemonitord en bestuurd? Is er een door het (top)management (directie) goedgekeurd informatiebeveiligingsbeleid? Zijn er informatiebeveiligingsdoelstelllingen opgesteld? Stuurt het beleid aan op continue verbetering van het ISMS voor informatiebeveiliging? Is het beleid beschikbaar voor iedereen en wordt hierover gecommuniceerd?	
	Planning	P.3	De entiteit vertaalt strategische-organisatiedoelen, risico's en compliance eisen in een algemeen informatiebeveiligingsplan dat rekening houdt met de IT-infrastructuur en de veiligheidscultuur.	Is er een risicoprocedure welke omschrijft wanneer een risicoanalyse moet plaatsvinden, welke definities voor kans en impact gelden, en hoe en onder welke voorwaarden een risico geaccepteerd mag worden? Zijn de risico's m.b.t. het in stand houden van het ISMS in kaart gebracht en zijn de er maatregelen benoemd en getroffen om deze risico's te beheersen? Zijn de risico's m.b.t. informatie binnen de scope van het ISMS in kaart gebracht en zijn de er maatregelen benoemd en getroffen om deze risico's te beheersen? Hebben alle risico's een eigenaar? Is er een risico behandelplan/ risicoregister? Beschikt de organisatie over een verklaring van toepasselijkheid (VVT)? Wordt in deze VVT minimaal van alle BIO2 maatregelen aangegeven of deze wel of niet in scope zijn met daarbij een onderbouwing van de reden? NB: afhankelijk van het aandachtsgebied kunnen additionele beveiligingsmaatregelen vereist zijn (bijvoorbeeld OT) Zijn er doelstellingen voor informatiebeveiliging opgesteld en geaccordeerd door de directie? Zijn de	
			De entiteit heeft vastgesteld welke middelen nodig zijn en stelt ze dienovereenkomstig beschikbaar voor het inrichten, implementeren, onderhouden en continu verbeteren van informatiebeveiliging.	Zijn er voldoende middelen beschikbaar voor het ISMS en blijkt dit uit budgetten en jaarplannen? Zijn de noodzakelijke competenties vastgesteld van de perso(o)n(en) die onder haar gezag werkzaamheden verricht(en) die de prestaties van de organisatie op het gebied van informatiebeveiliging beïnvloeden? Is vastgesteld dat deze personen competent zijn op basis van de juiste scholing, opleiding of ervaring en worden waar nodig maatregelen genomen om de benodigde competentie te verwerven en worden de doeltreffendheid van de genomen maatregelen geëvalueerd? Zijn de medewerkers binnen de organisatie zich bewust van het informatiebeveiligingsbeleid? Is er bewustzijn bij management en medewerkers voor het naleven van de basis beveiligingsmaatregelen?	

Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel | Template | Mapping Uitvoeringsverordening | Mapping BIO2 | Mapping DORA

Maturity model

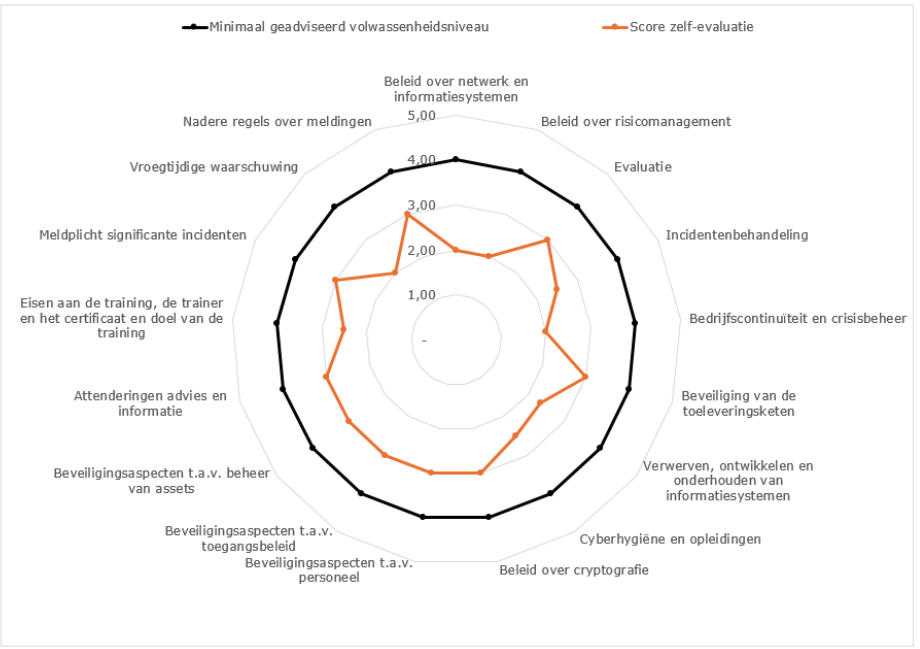
Domein	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Beleid over de toeleveringsketen	Er is geen vastgesteld beleid met betrekking tot de beveiliging van de toeleveringsketen. Afhankelijkheden van leveranciers worden ad hoc benaderd.	Er is een conceptbeleid opgesteld over toeleveringsketenbeveiliging, maar dit is nog niet vastgesteld of organisatiebreed toegepast.	Er is vastgesteld beleid over de toeleveringsketen en afhankelijkheden worden geïnventariseerd. Toepassing vindt aantoonbaar plaats, maar zonder structurele borging of aantoonbaarheid	Het beleid is vastgesteld, breed gecommuniceerd en wordt toegepast binnen relevante processen. Afhankelijkheden worden periodiek geëvalueerd.	Het beleid is volledig geïntegreerd in governance en risicomanagement. Evaluatie en bijstelling vinden cyclisch plaats op basis van risico's en leveranciersontwikkeling. Er is continue monitoring van naleving.
Cyberbeveiligingseisen toeleveringsketen	Er worden geen of slechts incidenteel afspraken gemaakt over cyberbeveiliging met leveranciers.	Er zijn enkele schriftelijke afspraken gemaakt met leveranciers, maar deze zijn niet gebaseerd op uniform beleid. Naleving wordt niet actief bewaakt.	Schriftelijke afspraken over beveiliging worden systematisch gemaakt voor nieuwe contracten, gebaseerd op het beleid. Naleving wordt aantoonbaar reactief gemonitord.	Er is een standaard raamwerk voor beveiligingseisen in contracten. Naleving wordt actief en regelmatig gecontroleerd.	Cyberbeveiligingseisen zijn onderdeel van alle leveranciersrelaties. Er vindt gestructureerde toetsing en auditing plaats. Er is een escalatiemechanisme bij niet-naleving.
Overzicht van de toeleveringsketen	Er is geen centraal of actueel overzicht van leveranciers en bijbehorende afspraken.	Een overzicht wordt handmatig en beperkt bijgehouden, maar is incompleet of verouderd.	Er is een actueel overzicht van leveranciers, producten/diensten en afspraken. Dit wordt periodiek handmatig bijgewerkt.	Het leveranciersoverzicht is volledig, digitaal toegankelijk en geïntegreerd in de beheersprocessen. Wijzigingen worden systematisch verwerkt.	Het overzicht is realtime, gekoppeld aan contractbeheer en risicobeoordeling. Er is inzicht in ketenafhankelijkheden, risico's en beveiligingsafspraken per leverancier.
Ontwikkelen en onderhouden van informatiesystemen	Er zijn geen maatregelen of beleid voor veilige ontwikkeling en onderhoud van informatiesystemen. Kwetsbaarheden worden niet systematisch beheerd.	Er zijn enkele ontwikkel- en onderhoudsactiviteiten, maar zonder formeel beleid of vastgelegde procedures. Beveiligingsmaatregelen worden incidenteel toegepast.	Er is vastgesteld beleid waarin maatregelen zijn opgenomen voor veilige ontwikkeling en onderhoud van informatiesystemen, inclusief rollen, verantwoordelijkheden en basismaatregelen voor het omgaan met kwetsbaarheden. De maatregelen uit het beleid worden aantoonbaar toegepast tijdens ontwikkeling en onderhoud.	Er is structurele aandacht voor kwetsbaarheden, en updates en patches worden volgens vaste processen uitgevoerd.	Beveiliging is geïntegreerd in de gehele levenscyclus van informatiesystemen. Beleid wordt periodiek aangepast op basis van nieuwe kwetsbaarheden, dreigingen en technologische ontwikkelingen. Verbeteringen worden systematisch doorgevoerd.
Cyberhygiene en opleidingen (algemeen)	Er is geen structurele aandacht voor bewustwording of cyberhygiëne.	Er zijn incidentele communicatie- of bewustwordingsacties, zoals een	Er is een basisbewustwordingsprogramma actief.	Cyberbewustwording is geïntegreerd in het onboardingproces, periodieke	Er is een doorlopend en aangepast bewustwordingsprogramma, gebaseerd

Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel | Template | Mapping Uitvoeringsverordening | Mapping BIO2 | Mapping DORA | +

Management dashboard

Resultaten Cbw (NIS2) Control Framework

Thema	Domein	Gewenst volwassenheids-niveau*	GAP	Score zelf-evaluatie	Score reviewer
Zorgplicht	Beleid over netwerk en informatiesystemen	4,00	-2,00	2,00	-
	Beleid over risicomanagement	4,00	-2,00	2,00	-
	Evaluatie	4,00	-1,00	3,00	-
	Incidentenbehandeling	4,00	-1,50	2,50	-
	Bedrijfscontinuïteit en crisisbeheer	4,00	-2,00	2,00	-
	Beveiliging van de toeleveringsketen	4,00	-1,00	3,00	-
	Verwerven, ontwikkelen en onderhouden van informatiesystemen	4,00	-1,67	2,33	-
	Cyberhygiëne en opleidingen	4,00	-1,50	2,50	-
	Beleid over cryptografie	4,00	-1,00	3,00	-
	Beveiligingsaspecten t.a.v. personeel	4,00	-1,00	3,00	-
	Beveiligingsaspecten t.a.v. toegangsbeleid	4,00	-1,00	3,00	-
	Beveiligingsaspecten t.a.v. beheer van assets	4,00	-1,00	3,00	-
	Attenderingen advies en informatie	4,00	-1,00	3,00	-
Goverance	Eisen aan de training, de trainer en het certificaat en doel van de training	4,00	-1,50	2,50	-
Meldplicht	Meldplicht significante incidenten	4,00	-1,00	3,00	-
	Vroegtijdige waarschuwing	4,00	-2,00	2,00	-
	Nadere regels over meldingen	4,00	-1,00	3,00	-



Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel | Template | Mapping Uitvoeringsverordening | Mapping BIO2 | Mapping DORA

Mappings

	Toelichting	Mapping per Cbw-sector		
		Beheer van ICT-diensten, digitale infrastructuur en digitale aanbieders	Overheid	Bankwezen en infrastructuur voor de financiële markt
		Uitvoeringsverordening (EU) 2024/2690	BIO2	DORA Control Framework
le entiteit worden diensten die door de	a. de soorten risico's voor netwerk- en informatiesystemen; b. risicomanagementprocessen; c. risicobeoordelingsmethodiek; d. risicobeheersingsmaatregelen op het gebied van cyberbeveiliging (zoals ook vastgelegd in beveiligingsbeleid). Het certificaat van de training, bevat in ieder geval: a. de naam van het lid van het bestuur van de essentiële entiteit of belangrijke entiteit; b. de datum of data waarop de training is gevolgd; c. de behandelde onderwerpen in de training; en d. de naam van de aanbieder van de training. Het certificaat van de training is opgesteld in de Nederlandse taal of de Engelse taal.			
ast houdt ieder		Dit onderwerp valt buiten de scope van de Uitvoeringsverordening, hier dient de Cbb gevolgd te worden.	n.v.t.	1.2
	Een incident is significant als het: a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Vrijwillige meldplicht: elke entiteit heeft de mogelijke om vrijwillig een melding van een incident, bijna-incident of cyberdreiging te doen bij haar CSIRT of bevoegde autoriteit.	Art. 3.1 Een incident wordt voor de toepassing van artikel 23, lid 3, van Richtlijn (EU) 2022/2555 met betrekking tot de relevante entiteiten als significant beschouwd indien aan een of meer van de volgende criteria is voldaan: a) het incident heeft voor de relevante entiteit direct financieel verlies veroorzaakt of kan verlies veroorzaken dat hoger is dan 500 000 EUR of meer dan 5 % van de totale jaaromzet van de relevante entiteit in het voorgaande boekjaar, indien dat lager is; b) het incident heeft het uitlekken van bedrijfsgeheimen als bedoeld in artikel 2, punt 1, van Richtlijn (EU) 2016/943 van de relevante entiteit veroorzaakt of kan dit veroorzaken; c) het incident heeft de dood van een natuurlijke persoon veroorzaakt of kan dit veroorzaken; d) het incident heeft aanzienlijke schade aan de gezondheid van een natuurlijke persoon veroorzaakt of kan dit veroorzaken; e) er heeft een succesvolle, vermoedelijk kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen plaatsgevonden, die ernstige operationele verstoringen kan veroorzaken; f) het incident voldoet aan de criteria van artikel 4; g) het incident voldoet aan een of meer van de criteria van de artikelen 5 tot en met 14. Art 4. Incidenten die afzonderlijk niet als een significant incident in de zin van artikel 3 worden beschouwd, worden gezamenlijk als één significant incident beschouwd indien zij aan alle volgende criteria voldoen: a) zij hebben zich ten minste tweemaal binnen zes maanden voorgedaan; b) zij hebben dezelfde kennelijk onderliggende oorzaak; c) zij voldoen gezamenlijk aan de criteria van artikel 3, lid 1, punt a).	n.v.t.	11.3

Toelichting | Keuzes | Cbw (NIS2) Control Framework | ISMS evaluatie | Resultaten | Volwassenheid beheersmaatregel | Template | Mapping Uitvoeringsverordening | Mapping BIO2 | Mapping DORA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Auditdienst Rijk
Ministerie van Financiën

Next steps: Upcoming releases

Download de laatste versie via:
www.norea.nl
www.auditdienstrijk.nl

Inhoud

- Introductie in de CBW
- Wat moet uw organisatie gaan doen?
- Voldoet uw organisatie al aan de CBW?
- CBW-framework als hulpmiddel
- **Meer info en vragen?**

Meer informatie

- Te beschermen belangen
  - Leidraad Te beschermen belangen 2015
  - Methodiek Te Beschermen Belangen 10-04-2025 (DepV.)
  - Gereedschap TBB systematiek VIRBI-implementatie (zie linken)

Linken

Baseline Informatiebeveiliging Overheid 2

Github-BZK

NIS2-richtlijn - Digitale Overheid

Mapping NIS2-maatregelen - Digitale Overheid

Veel gestelde vragen over de NIS2-richtlijn Digitale Overheid

Baseline Informatiebeveiliging Overheid 2

Staatscourant

Baseline Informatiebeveiliging Overheid 2

IBD

Cyberbeveiligingswet

IBD

Gereedschapskist implementatie VIRBI 2025 Digitale weerbaarheid - Digitale Overheid

Contactinformatie

Meer weten naar aanleiding van deze presentatie?

BZK:

Cyberbeveiligingswet@minbzk.nl

Auditdienst Rijk / NOREA:

ADRcommunicatie@minfin.nl / norea@norea.nl