

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

Doel

Het Cbw (NIS2) Control Framework is tot stand gekomen in een gezamenlijke inspanning van de Auditdienst Rijk (ADR) en het Ministerie van Binnenlandse Zaken en in samenwerking met de Beroepsorganisatie van IT-Auditors in Nederland (NOREA). Het framework is ontwikkeld om organisaties een handvat te bieden om op effectieve wijze inzicht te krijgen in de mate waarin een organisatie invulling geeft aan de Cyberbeveiligingswet, en daarmee aan de cyberbeveiliging. Ook kan het door IT-auditors worden ingezet als onderdeel van hun auditstrategie.

Het Cbw (NIS2) Control Framework en dit studierapport mogen worden gebruikt en/of ongewijzigd worden gedistribueerd, mits met bronvermelding.

Endorsement

Het Cbw (NIS2) Control Framework en dit studierapport worden ondersteund door de volgende partijen:



Het Cbw (NIS2) Control Framework en dit studierapport zijn gedeeld met het NCSC en de Cbw-toezichthouders. Het NCSC en de Cbw-toezichthouders hebben de volgende gezamenlijke reactie gegeven:

"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."



Het Cbw (NIS2) Control Framework is te downloaden op de websites van de [Auditdienst Rijk](#) en [NOREA](#)

Managementsamenvatting

Aanleiding

De toenemende digitalisering van onze samenleving, in combinatie met groeiende cyberdreigingen en de opkomst van hybride oorlogsvoering, maakt cyberweerbaarheid tot een strategische noodzaak voor organisaties. Met de invoering van de Cyberbeveiligingswet (Cbw, NIS2) wordt de verantwoordelijkheid voor cyberweerbaarheid nadrukkelijk bij organisaties en hun bestuurders neergelegd. Bestuurders zijn juridisch aansprakelijk voor tekortkomingen in cyberbeveiligingsmaatregelen en worden geacht actief invulling te geven aan hun rol door sturing, toezicht en scholing. Tegelijkertijd gelden in diverse sectoren aanvullende normen, zoals de BIO2 voor de overheid en de DORA voor de financiële sector. Het naleven van verplichtingen wordt hierdoor complex en versnipperd, waardoor overzicht en samenhang vaak ontbreekt.

Doel van het framework

Om overzicht te creëren en gericht te kunnen sturen is het Cbw (NIS2) Control Framework ontwikkeld (hierna framework). Dit framework is toepasbaar in zowel publieke als private sectoren. Het maakt gebruik van een volwassenheidsmodel en biedt organisaties de mogelijkheid om snel en gestructureerd inzicht te krijgen in de mate waarin zij invulling geven aan de Cbw (NIS2) en sectorale normen. Daarmee ondersteunt het framework bij het identificeren van verbeterpotentieel en biedt het een basis voor interne en externe verantwoording.

Risico's bij gebrek aan inzicht

Cyberincidenten kunnen leiden tot aanzienlijke financiële schade door verstoringen van bedrijfsprocessen, productieverlies of herstelkosten. Daarnaast kan een incident de reputatie ernstig schaden, wat het vertrouwen van klanten, ketenpartners en toezichthouders ondermijnt. Deze risico's zijn slechts voorbeelden maar benadrukken het belang van een systematische benadering van cyberweerbaarheid. Het fundament voor het beheersen ervan ligt in inzicht: weten waar de organisatie staat, welke risico's relevant zijn en waar verbeterpotentieel ligt. Pas wanneer dit inzicht aanwezig is, kan gericht worden gewerkt aan versterking van de cyberweerbaarheid. Het Cbw (NIS2) Control Framework kan hierin ondersteunen door op een gestructureerde manier inzicht te bieden in de mate waarin een organisatie invulling geeft aan de Cbw (NIS2) en gerelateerde normen. Het framework is geen oplossing op zichzelf, maar is een praktisch hulpmiddel dat helpt bij het verkrijgen van het noodzakelijke inzicht en bij het bepalen van vervolgstappen.

Implicaties en voordelen

Met het gebruik van het Cbw (NIS2) Control Framework wordt door de organisatie (of het bestuur) strategisch inzicht verkregen om te kunnen prioriteren en middelen doelgericht in te zetten. Het vergroot de efficiëntie verder doordat uiteenlopende normenkaders worden samengebracht in één geïntegreerd raamwerk. Daarnaast draagt toepassing bij aan de versterking van de weerbaarheid van de sector en de Europese keten als geheel.

Conclusie

Het Cbw (NIS2) Control Framework vervangt de geldende wet- en regelgeving niet, maar maakt deze inzichtelijk en hanteerbaar. Het ondersteunt organisaties bij het verkrijgen van overzicht, het versterken van hun cyberweerbaarheid en kan helpen bij het voldoen aan wettelijke verplichtingen. Voor bestuurders en toezichthouders vormt dit instrument een waardevolle bron van inzicht en sturing in een complex en veeleisend speelveld.

Inhoud

Managementsamenvatting	3
1. Inleiding	5
1.1 Aanleiding	5
1.2 Beoogd resultaat	5
1.3 Doelgroep	5
1.4 Leeswijzer	5
2. Achtergrond Cbw (NIS2) wetgeving	6
2.1 Overzicht van relevante wet- en regelgeving	6
2.2 NIS2	6
2.3 Cyberbeveiligingswet (Cbw)	7
2.4 Cyberbeveiligingsbesluit (Cbb)	10
2.5 Uitvoeringsverordening (EU) 2024/2690	11
2.6 BIO2	11
2.7 DORA	12
2.8 Compliance vs. digitale weerbaarheid	12
3. Het framework nader bekeken	13
3.1 Een overzicht van het framework	13
3.2 Beheersmaatregelen	13
3.3 Volwassenheidsmodel	14
3.4 Het Control Framework in Excel	14
3.5 ISMS evaluatie	15
3.6 Inzet van het framework bij implementatie Cbw (NIS2)	15
4. Handreiking voor Auditors	17
4.1 Auditgerichte inzet van het framework	17
4.2 Benutting van zelfevaluaties	17
4.3 Scopebepaling en afbakening van systemen	17
4.4 Opdrachtvorm en toepasselijke standaarden	17
5. Conclusie	18

1. Inleiding

1.1 Aanleiding

Het Cbw (NIS2) Control Framework is tot stand gekomen in een gezamenlijke inspanning van de Auditdienst Rijk (ADR) en het Ministerie van Binnenlandse Zaken en in samenwerking met de Beroepsorganisatie van IT-Auditors in Nederland (NOREA). Het framework ondersteunt entiteiten bij het verkrijgen van inzicht in de mate waarin een entiteit invulling geeft aan de Cyberbeveiligingswet en het onderliggende Cyberbeveiligingsbesluit. Het doel is het versterken van de cyberweerbaarheid van entiteiten die als essentiële of belangrijke entiteit zijn aangemerkt en het bieden van handvatten om de naleving van wettelijke verplichtingen te structureren en te evalueren.

1.2 Beoogd resultaat

Het framework is zo opgezet dat het toepasbaar is voor alle sectoren en entiteiten in scope van de wetgeving. Het dient als ondersteunend instrument en niet als normatief kader. Entiteiten blijven zelf verantwoordelijk voor het bepalen welke beveiligingsmaatregelen passend en proportioneel zijn binnen hun specifieke context en risicoprofiel.

Het framework is beschikbaar in Excel. Hiervoor is gekozen vanwege de flexibiliteit van deze software. Niet-relevante sectorspecifieke normen kunnen eenvoudig worden verwijderd, terwijl organisatie-specifieke normen kunnen worden toegevoegd. Excel maakt het bovendien mogelijk om resultaten snel te actualiseren, intern te delen en binnen de eigen entiteiten te bewaren, waardoor het risico op extern opslaan van gevoelige gegevens wordt beperkt.

1.3 Doelgroep

Het framework is bedoeld voor organisaties die als essentiële of belangrijke entiteit onder de Cyberbeveiligingswet vallen, en voor IT-auditors en interne beheerders die betrokken zijn bij het evalueren van cyberweerbaarheid en naleving van wet- en regelgeving. Het biedt een overzicht van de wettelijke vereisten en een praktisch hulpmiddel om verbeterpunten te identificeren.

De Rijksinspectie Digitale Infrastructuur (RDI) heeft een zelfevaluatietool¹ ontwikkeld die organisaties kan helpen om te bepalen of ze een essentiële of belangrijke entiteit zijn onder de Cyberbeveiligingswet.

1.4 Leeswijzer

In dit rapport wordt onderscheid gemaakt tussen de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb). Wanneer beide samen worden bedoeld, wordt de term 'Cbw (NIS2)' gebruikt. Zo is meteen duidelijk welk onderdeel van de wet- en regelgeving van toepassing is.

Het rapport is verder opgebouwd uit drie hoofdstukken:

1. Achtergrond Cbw (NIS2) wetgeving – Bespreekt de relevante wet- en regelgeving, waaronder NIS2, de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit, de Uitvoeringsverordening (EUR) 2024/2690, BIO2 en DORA, en legt uit welke verplichtingen voor organisaties gelden.
2. Het framework nader bekeken – Beschrijft het Cbw (NIS2) Control Framework, inclusief opbouw, stappenplan, concrete beheersmaatregelen en volwassenheidsniveaus, en legt uit hoe het framework kan worden gebruikt. Ook wordt kort de facultatieve ISMS - gebaseerd op ISO/IEC 27001 - evaluatie toegelicht.
3. Handreiking voor auditors – Legt uit hoe het framework kan worden gebruikt bij audits.

¹ <https://regelhulpenvoorbedrijven.nl/NIS-2-NL/>

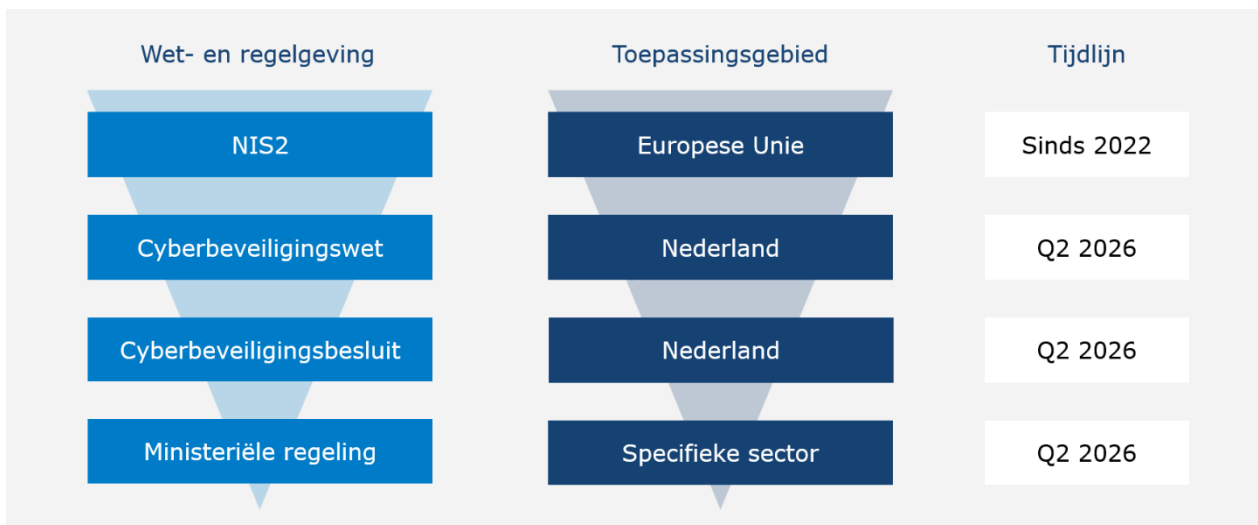
2. Achtergrond Cbw (NIS2) wetgeving

2.1 Overzicht van relevante wet- en regelgeving

Dit hoofdstuk biedt een overzicht van de relevante wet- en regelgeving voor entiteiten die onder de Cbw (NIS2) vallen. Het behandelt de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit, de Uitvoeringsverordening (EUR) 2024/2690, BIO2 en DORA, en verduidelijkt de verplichtingen welke hieruit voortvloeien. Op deze manier wordt de juridische context geschetst die ten grondslag ligt aan het Cbw (NIS2) Control Framework.

De opbouw van deze wetten is hieronder visueel weergegeven. De linker piramide toont de hiërarchie van de EU-wetgeving en de Nederlandse implementatie daarvan. Van boven naar beneden wordt getoond hoe de Europese richtlijn NIS2 wordt vertaald naar nationale wetgeving: via de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit (in een algemene maatregel van bestuur) naar ministeriële regelingen. Deze lagen geven aan hoe abstracte EU-regels concreet worden gemaakt in Nederlandse wet- en regelgeving.

De middelste piramide geeft het toepassingsgebied weer van de brede context van de Europese Unie, via de nationale invulling in Nederland, tot de specifieke essentiële en belangrijke entiteiten (Nederland) en specifieke sectoren. De rechterkolom toont de tijdlijn van invoering. NIS2 is sinds 2022 van kracht, terwijl de nationale implementatie via de Cyberbeveiligingswet en het besluit wordt verwacht in 2026. De Ministeriële regelingen zijn nog in ontwikkeling.



Figuur 1: Overzicht opbouw NIS2 wetgeving

2.2 NIS2

De Europese NIS2-richtlijn (Directive (EU) 2022/2555)² heeft tot doel de fysieke, digitale en economische weerbaarheid van lidstaten te versterken. De NIS2-richtlijn is op 16 januari 2023 in werking getreden en stelt aangescherpte eisen aan de beveiliging van netwerk- en informatiesystemen van entiteiten die essentieel en belangrijk zijn voor het functioneren van de samenleving en economie.

² <https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN>

Lidstaten van de Europese Unie, waaronder Nederland, zijn verplicht om de NIS2-richtlijn om te zetten in nationale wetgeving. Nederland heeft hiervoor de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit opgesteld.

2.3 Cyberbeveiligingswet (Cbw)

De Cyberbeveiligingswet bestaat uit vier kernonderdelen: meldplicht, zorgplicht, registratieplicht en toezicht. Deze kernonderdelen bevatten verplichtingen die gelden voor belangrijke en essentiële entiteiten. Daarnaast worden eventuele sectorspecifieke eisen vastgelegd in ministeriële regelingen.

➤ Essentiële en belangrijke entiteiten

De Cbw (NIS2) maakt onderscheid tussen essentiële entiteiten en belangrijke entiteiten. Het belangrijkste verschil tussen een essentiële entiteit en een belangrijke entiteit onder de NIS2-richtlijn is het toezicht regime en de bijbehorende sancties. Essentiële entiteiten, die cruciaal zijn voor de samenleving, vallen onder intensiever, proactief toezicht (zowel voor als na incidenten) en krijgen hogere boetes, terwijl belangrijke entiteiten reactief toezicht krijgen en lagere sancties riskeren. De cyberbeveiligingsverplichtingen zijn voor beide categorieën gelijk, maar de impact op het toezicht en de boetes verschilt.

In tabel 1 hieronder een overzicht van de criteria die bepalen of een entiteit essentieel of belangrijk is.

Essentiële entiteit	Belangrijke entiteit
Grote organisaties die actief zijn in een van de genoemde sectoren uit bijlage I van de Cyberbeveiligingswet kwalificeren als essentiële entiteit (zie figuur 2).	Middelgrote organisaties die actief zijn in een van de genoemde sectoren uit bijlage 1 (zie figuur 2).
Organisaties die op grond van de Wet weerbaarheid kritieke entiteiten ³ zijn aangewezen als kritieke entiteit.	Middelgrote en grote organisaties die actief zijn in een van de genoemde sectoren uit bijlage 2 (zie figuur 3).
De volgende sectoren vallen direct onder de Cyberbeveiligingswet als essentiële entiteit, ongeacht hun grootte: overheid, gekwalificeerde vertrouwensdienstverleners (QTSP), registers voor topleveldomeinnamen en verleners van DNS-diensten. Ook middelgrote aanbieders van openbare elektronische communicatienetwerken en -diensten.	

³ <https://wetgevingskalender.overheid.nl/Regeling/WGK014624>



Figuur 2: Essentiële entiteiten vastgelegd in bijlage 1 van de Cbw



Figuur 3: Belangrijke entiteiten vastgelegd in bijlage 2 van de Cbw

Naast de sector waar een organisatie actief is, is ook de grootte van de organisatie bepalend voor de bepaling van essentieel of belangrijk. De grootte van een organisatie wordt bepaald aan de hand van twee categorieën. Hiervoor zijn de criteria vastgesteld in figuur 4.



Figuur 4: Grootte criteria uit de Cbw

Uitzonderingen:

- Entiteiten die domeinnaamregistratiediensten aanbieden vallen onder de wet, maar zijn geen essentiële of belangrijke entiteit. Zij zijn een afzonderlijke categorie, omdat voor hen bijzondere verplichtingen gelden; zij hebben geen meldplicht van incidenten en zorgplicht maar moeten een database met domeinnaamregistratiegegevens bijhouden. Hierop vindt ook toezicht plaats.
- Het wetsvoorstel maakt het mogelijk om hogere onderwijsinstellingen onder de Cyberbeveiligingswet te brengen. De Minister van Onderwijs, Cultuur en Wetenschap kan dit bepalen via een ministeriële regeling.
- Micro- en kleinbedrijven vallen in principe niet onder de NIS2-richtlijn. De vakminister die verantwoordelijk is voor een bepaalde sector kan er echter wel voor kiezen om een micro- of kleinbedrijf aan te wijzen op basis van een risicobeoordeling. Bijvoorbeeld als blijkt dat hun dienstverlening van cruciaal belang is voor de Nederlandse economie of maatschappij. In dat geval worden deze bedrijven hierover geïnformeerd door het desbetreffende ministerie. Daarmee kunnen ze alsnog onder de Cyberbeveiligingswet komen te vallen.

Om organisaties te helpen om te bepalen of ze een essentiële of belangrijke entiteit zijn onder de Cbw (NIS2), heeft de Rijksinspectie Digitale Infrastructuur (RDI) een zelfevaluatietool⁴ ontwikkeld. Het is te allen tijde de verantwoordelijkheid van de instelling zelf om te bepalen om na te gaan of ze in scope vallen van de Cbw (NIS2) en in welke categorie.

➤ **Zorgplicht**

Entiteiten die onder de Cbw (NIS2) vallen hebben een zorgplicht (art. 21, Cbw). Dit houdt in dat zij maatregelen moeten nemen om hun netwerk- en informatiesystemen te beschermen tegen significante incidenten (dat zijn incidenten die ernstige verstoringen in de dienstverlening veroorzaken of aanzienlijke materiële of immateriële schade tot gevolg hebben), zoals een cyberaanval.

De wet schrijft tien zorgplichtmaatregelen voor waar entiteiten minimaal aan moeten voldoen:

1. Een risicoanalyse en beveiliging van informatiesystemen.
2. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets.
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningsplannen.
4. Incidentenbehandeling.
5. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging.
6. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief respons op en bekendmaking van kwetsbaarheden.
7. Beveiliging van de toeleveranciersketen.
8. Beleid en procedures over het gebruik van cryptografie en encryptie.
9. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen.
10. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen.

➤ **Meldplicht**

Zodra de Cbw (NIS2) van kracht is, moeten entiteiten significante incidenten melden (art. 25, Cbw) via het NCSC-portaal. Het meldproces bestaat uit drie fasen:

1. Vroegtijdige melding: binnen 24 uur na het incident.
2. Vervolgmelding: binnen 72 uur, met aanvullende informatie.

⁴ <https://regelhulpenvoorbedrijven.nl/NIS-2-NL/>

3. Eindverslag: uiterlijk één maand na de eerste melding, met een gedetailleerde omschrijving van het incident, de ernst en gevolgen.

De melding wordt doorgestuurd naar het sectorale CSIRT en de toezichthouder. Optioneel kan tussentijds aanvullende informatie worden opgevraagd door het CSIRT of de toezichthouder.

Ook organisaties die niet onder de wet vallen kunnen (vrijwillig) meldingen indienen. Daarnaast kunnen alle organisaties niet-significante incidenten op vrijwillige basis melden bij het NCSC.

➤ **Registratieplicht**

Entiteiten die onder de Cbw (NIS2) vallen, moeten zich registreren (art. 44, Cbw) bij de bevoegde autoriteit. Dit loopt via het NCSC-portaal, waar gegevens worden opgenomen in het entiteitenregister. Essentiële en belangrijke entiteiten, en entiteiten die domeinnaamregistratiediensten verlenen, kunnen zich al vanaf 17 oktober 2024 vrijwillig registreren. Na inwerkingtreding van de wet wordt registratie verplicht. Door de registratie ontvangt een entiteit informatie over actuele cyberdreigingen. Registratie is mogelijk via het NCSC-portaal⁵.

➤ **Toezicht**

De toezicht verplichtingen (art. 69, Cbw) richten zich op de rol van de bevoegde autoriteiten en niet op de entiteit. Daarom zijn de toezicht verplichtingen niet opgenomen in het framework. Welke partij de toezichthouder is, verschilt per sector. Van entiteiten wordt verwacht dat zij weten wie voor hun sector de aangewezen toezichthouder is.

➤ **Cbw (NIS2) in het Control Framework**

Het framework richt zich primair op de zorgplicht omdat deze de meeste aanknopingspunten biedt voor een systematische evaluatie van cyberweerbaarheid binnen de entiteit. De meldplicht is eveneens meegenomen, zodat entiteiten inzicht krijgen in hun verplichtingen en verantwoordelijkheden. De registratieplicht is geen onderdeel van het Control Framework en is al hierboven beschreven. In de Excel is een kolom opgenomen waar per thema de Cbw en Cbb artikelen genoemd zijn waar deze uit voort komt. Deze kolom biedt daarmee ook een overzicht van alle artikelen die zijn meegenomen in het framework.

2.4 Cyberbeveiligingsbesluit (Cbb)

Het Cyberbeveiligingsbesluit (Cbb) is een verplicht uitvoeringsbesluit bij de Cyberbeveiligingswet (Cbw). Dit betekent dat entiteiten die onder de wet vallen zich ook aan het besluit moeten houden.

Het Cbb werkt de algemene verplichtingen uit die in de Cbw zijn vastgelegd, zoals de zorgplicht, meldplicht en registratieplicht. Waar de wet het kader bepaalt en de kernprincipes aangeeft, geeft het besluit praktische en juridische details voor de uitvoering. Concreet legt het besluit bijvoorbeeld vast welke technische en organisatorische maatregelen nodig zijn, hoe incidentmeldingen moeten worden gedaan en welke gegevens aangeleverd moeten worden voor de registratie.

Met andere woorden: de wet (Cbw) bepaalt wat entiteiten moeten doen op hoofdlijnen en het besluit (Cbb) vertelt hoe dit in de praktijk moet gebeuren. Entiteiten die onder de Cbw vallen, zijn dus automatisch ook verplicht om de regels uit het Cbb na te leven.

Dit betekent dat het Cbb geldt voor alle essentiële en belangrijke entiteiten die onder de wet vallen. Het besluit ondersteunt entiteiten bij het concreet invullen van de wettelijke verplichtingen en vormt daarmee een belangrijk onderdeel van het wettelijke kader voor cyberweerbaarheid.

⁵ <https://mijn.ncsc.nl/>

Sectorspecifieke eisen

Het is belangrijk te beseffen dat de wet niet alle onderdelen van cyberweerbaarheid op een concreet niveau waarborgt. Naast de generieke normen uit de Cbw en Cbb kunnen ook sectorale eisen van toepassing zijn. Daarom zijn in het Cbw (NIS2) Control Framework aanvullende richtlijnen en standaarden opgenomen, zodat een breed scala aan weerbaarheid wordt geraakt. Zo kennen sectoren zoals de overheid, zorg, financiële dienstverlening, waterschappen en telecom additionele wettelijke verplichtingen en richtlijnen die specifiek zijn toegespitst op hun risico's en afhankelijkheden. Voorbeelden hiervan zijn de Baseline Informatiebeveiliging Overheid (BIO2) voor de sector overheid en de Digital Operational Resilience Act (DORA) voor de financiële dienstverlening. Voor digitale dienstverleners zijn specifieke eisen opgenomen in een Europese uitvoeringsverordening (CIR).

2.5 Uitvoeringsverordening (EU) 2024/2690

De Uitvoeringsverordening (EUR) 2024/2690 is een Europese verordening die direct specifieke eisen stelt aan digitale dienstverleners binnen de scope van de Cbw (NIS2). Net als het Cbb vult deze verordening de algemene verplichtingen van de wet, op Europeesniveau, aan. Let wel, deze verordening is sinds 2024 van toepassing en dient niet in nationale wetgeving vertaald te worden.

De verordening geeft concreet aan welke beveiligingsmaatregelen en rapportageverplichtingen van toepassing zijn op digitale dienstverleners, waaronder Cloud providers, online marktplaatsen en zoekmachines. Organisaties die onder de wet vallen en als digitale dienstverlener actief zijn, moeten zich aan deze verordening houden.

Het verschil tussen wet, besluit en uitvoeringsverordening is als volgt: de wet (Cbw) bepaalt de kernverplichtingen; het besluit (Cbb) geeft nationale praktische invulling; de Uitvoeringsverordening (EUR 2024/2690) specificereert Europese eisen. Samen vormen zij het volledige juridische kader voor naleving en cyberweerbaarheid voor digitale dienstverleners.

2.6 BIO2

De Baseline Informatiebeveiliging Overheid (BIO2) vormt het basisniveau en het gemeenschappelijke normenkader voor informatie(systemen) binnen de overheid. Het biedt richtlijnen en verplichte maatregelen voor overheidsorganisaties, met als doel de informatiebeveiliging op een gemeenschappelijk basisniveau te brengen.

In de ministeriële regeling voor de sector overheid wordt de zorgplicht uit de Cbw (NIS2) uitgewerkt voor overheidsorganisaties. De BIO2 vormt de praktische invulling van deze zorgplicht en biedt daarmee de wettelijke basis voor het normenkader. Hiermee ontstaat een direct verband tussen de wettelijke verplichtingen uit de Cbw en het Cbb, en de maatregelen en richtlijnen die in de BIO2 zijn opgenomen. Organisaties kunnen via de BIO2 aantonen dat zij hun zorgplicht op een systematische en gestructureerde manier invullen.

De BIO bestaat uit twee delen. Deel 1 legt de relatie met ISO/IEC 27001 uit: het managementsysteem van de organisatie moet voldoen aan de eisen zoals in de ISO is beschreven. Beschikbaarheid, integriteit en vertrouwelijkheid van informatie worden geborgd door het managementsysteem te integreren in de organisatieprocessen en de algehele managementstructuur. De BIO2 schrijft voor dat organisaties binnen deze context een risicoanalyse uitvoeren, gebaseerd op een risicomanagementmethodiek waaraan de BIO2 minimeisen stelt. De geïdentificeerde risico's worden vervolgens gemitigeerd door passende beheersmaatregelen vast te stellen.

Deel 2 van de BIO sluit aan bij de beheersmaatregelen uit ISO/IEC 27002 (Appendix A van ISO 27001), die *risico gebaseerd* toegepast dienen te worden. Deze maatregelen worden aangevuld met specifieke overheidseisen die *altijd* geïmplementeerd moeten worden.

2.7 DORA

De Digital Operational Resilience Act (DORA), officieel bekend als Verordening (EU) 2022/2554, is een wetgevingshandeling die ervoor moet zorgen dat financiële entiteiten binnen de EU bestand zijn tegen, kunnen reageren op en kunnen herstellen van alle soorten ICT-gerelateerde verstoringen en bedreigingen. DORA consolideert en verbetert bestaande ICT-vereisten en creëert een uniform kader voor digitale operationele veerkracht in de Europese financiële sector.

NIS2 en DORA delen niet alleen hun doel om de cybersecurity en operationele veerkracht te verbeteren, maar verwijzen ook naar elkaar. DORA heeft een *lex specialis*-status ten opzichte van NIS2, wat betekent dat DORA fungeert als een gespecialiseerde set regels die voorrang heeft op de meer algemene doelen van NIS2.

Voor meer informatie over DORA zie het NOREA DORA studierapport en control framework⁶.

2.8 Compliance vs. digitale weerbaarheid

Entiteiten die onder de Cbw (NIS2) vallen, moeten volledig compliant zijn met zowel de Cbw als het bijbehorende Cbb. Echter, compliance is geen doel op zich. De wettelijke verplichtingen bestaan om de weerbaarheid van entiteiten tegen cyberdreigingen te vergroten en de continuïteit van kritische diensten te waarborgen.

Er bestaan verschillen tussen de wet, het besluit en sectorspecifieke eisen, bijvoorbeeld in terminologie, reikwijdte en mate van detaillering. Voldoen aan één kader betekent daardoor niet dat ook aan andere kaders wordt voldaan. Het is daarom essentieel dat organisaties zowel de generieke als de sectorspecifieke verplichtingen integreren in hun risicobeheersings- en governanceprocessen.

Compliance draagt bij aan een systematische aanpak van informatiebeveiliging. Het helpt risico's te beheersen, beschermt bedrijfsprocessen en ketenpartners, en waarborgt de veiligheid van informatie over medewerkers en afnemers (zoals klanten, patiënten, burgers). Ook draagt het bij aan het afleggen van verantwoording hierover. Organisaties die uitsluitend focussen op het afvinken van wettelijke verplichtingen missen het grotere doel: daadwerkelijk de cyberweerbaarheid verhogen en structureel risico's beheersen.

Hoewel de invoering van de Cbw/NIS2 een belangrijke stap is richting versterkte cyberweerbaarheid, ontbreken er enkele cruciale controls in de Cbw en Cbb die essentieel zijn voor een robuuste beveiligingsstrategie. Denk bijvoorbeeld aan patch management en netwerksegmentatie, beide fundamenteel om veelvoorkomende cyberaanvallen te voorkomen of beperken, maar niet expliciet opgenomen in deze wet- en regelgeving. Organisaties doen er dan ook verstandig aan om niet blind de Cbw en Cbb te implementeren in de veronderstelling dat daarmee de volledige cyberweerbaarheid is afgedekt. Blijf als organisatie zelf nadenken. Kijk kritisch naar je eigen omgeving, bepaal wat je kroonjuwelen zijn, en beoordeel de risico's die specifiek voor jouw organisatie gelden. Cyberweerbaarheid vraagt om maatwerk – wetgeving is slechts het fundament.

⁶ <https://www.norea.nl/uploads/bfile/52ee1e0f-54ae-4157-9a43-524c746c2ff1>

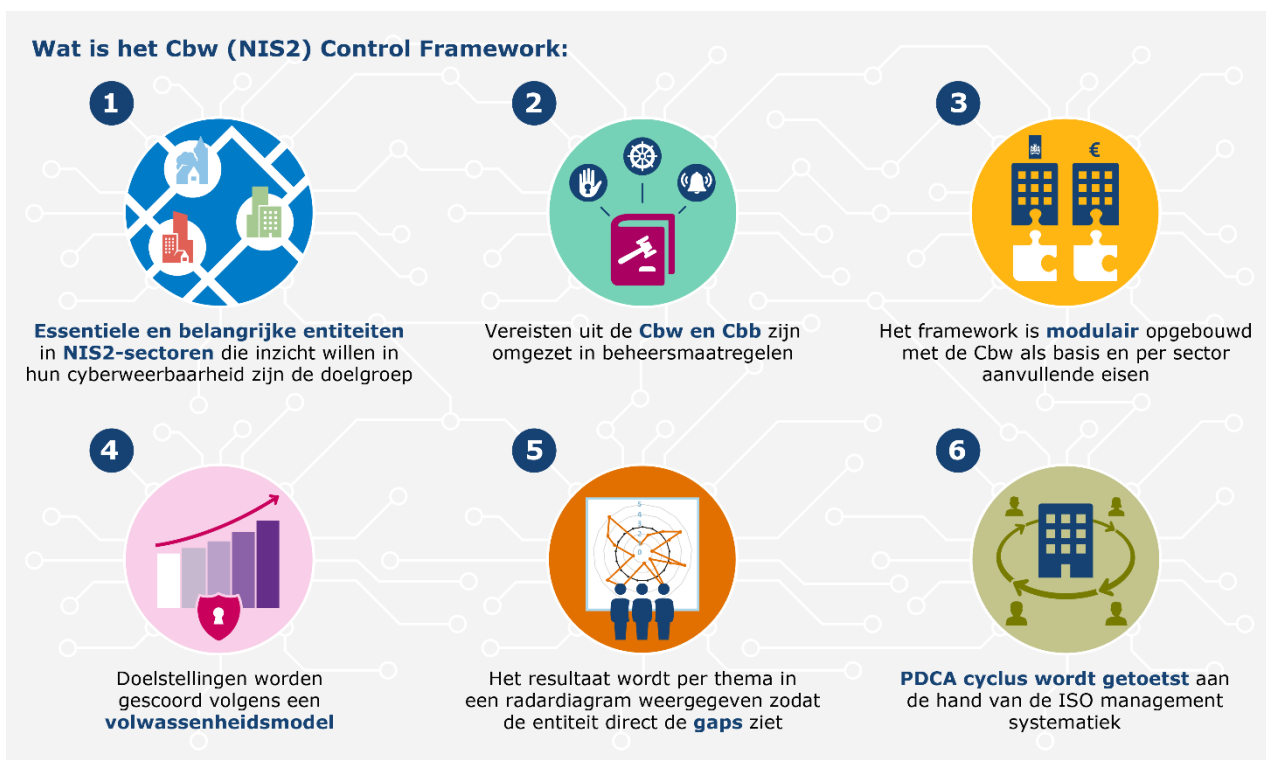
3. Het framework nader bekeken

3.1 Een overzicht van het framework

Het Cbw (NIS2) Control Framework is een praktisch hulpmiddel waarmee entiteiten hun cyberweerbaarheid systematisch in kaart kunnen brengen. Risicomanagement vormt de basis van alle vereisten: elk onderdeel van het framework grijpt terug op het identificeren en beheersen van risico's. De beheersmaatregelen zijn rechtstreeks ontleend aan de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb) met nadruk op de artikelen die de zorgplicht van entiteiten beschrijven.

Deze beheersmaatregelen worden beoordeeld aan de hand van een volwassenheidsmodel, waarmee entiteiten niet alleen kunnen vaststellen of zij aan de vereisten voldoen, maar ook inzicht krijgen in hun groepspad. Het framework is modulair opgebouwd: naast de generieke componenten kunnen per sector aanvullende eisen gelden, zoals de BIO2 voor de overheid of de DORA-verordening voor de financiële sector.

De resultaten worden per thema visueel gepresenteerd in een radardiagram, zodat bestuurders en toezichthouders in één oogopslag zicht hebben op de sterke punten en de huidige gaps. Tot slot wordt de toepassing van de Plan-Do-Check-Act-cyclus desgewenst getoetst, volgens de ISO-management-systematiek, waardoor de continue verbeterloop binnen de organisatie zichtbaar wordt gemaakt.



3.2 Beheersmaatregelen

De beheersmaatregelen in het framework zijn met de wet in acht genomen geformuleerd. De termen uit de wet komen terug in de beheersmaatregelen, en ook de redenatielijn (nl. risico gestuurd) die in de artikelen van de Cbw (NIS2) uiteen wordt gezet. Waar nodig zijn deze maatregelen nader gespecificeerd en/of geoperationaliseerd. Deze nadere concretisering kan entiteiten helpen om de vertaalslag te maken naar concrete acties binnen hun eigen context.

3.3 Volwassenheidsmodel

Hoewel de Cbw en Cbb geen expliciet volwassenheidsmodel voorschrijven, wordt in het framework wel gebruik gemaakt van een volwassenheidsmodel. Dit model maakt het mogelijk om niet alleen de huidige stand van zaken in kaart te brengen, maar ook de voortgang en ontwikkeling van de entiteit over de tijd heen te volgen. Dit bevordert een lerende aanpak en continue verbetering.

In dit framework wordt volwassenheid op dezelfde manier ingedeeld als in het NBA/NOREA volwassenheidsmodel⁷. Dat betekent dat er verschillende niveaus worden onderscheiden per beheersmaatregelen die de mate van volwassenheid van een entiteit weergeven: van een ad-hoc en weinig gestructureerde aanpak, via meer gestandaardiseerde en herhaalbare processen, tot een volwassenheidsniveau waarbij continue verbetering verankerd in de organisatiecultuur centraal staan. Deze indeling maakt het mogelijk om niet alleen de huidige situatie in kaart te brengen, maar ook gericht te bepalen welke stappen nodig zijn om door te groeien naar een hoger volwassenheidsniveau.

De beheersmaatregelen die zijn geformuleerd in het Cbw (NIS2) Control Framework zijn per volwassenheidsniveau uitgewerkt. Deze concretisering van de 5 algemene niveaus biedt entiteiten duidelijkheid over wat er op elk niveau exact verwacht wordt. Dit maakt dat zij beter in staat zijn om te beoordelen waar zij op dit moment staan. Daarnaast biedt het per onderwerp inzicht in de acties die nodig zijn om naar een volgend volwassenheidsniveau te groeien.

3.4 Het Control Framework in Excel

Het Cbw (NIS2) Control Framework is beschikbaar in een Excel-versie die entiteiten houvast biedt bij het invullen, analyseren en presenteren van hun resultaten. Het framework kan zowel op organisatieniveau als op systeemniveau worden toegepast, maar het is van groot belang dat de scope vooraf wordt vastgesteld. Dit gebeurt in het tabblad Keuzes, waarin de gebruiker duidelijk aangeeft op welk domein of welke systemen de evaluatie betrekking heeft.

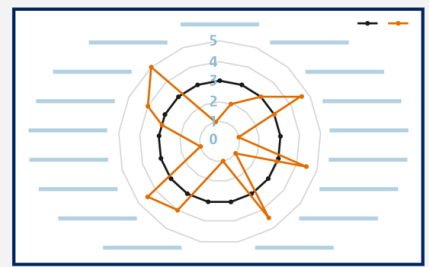
Het tabblad Cbw (NIS2) Control Framework vormt de kern van de Excel: hier zijn alle beheersmaatregelen opgenomen die uit de Cbw en Cbb voortvloeien. De gebruiker vult per beheersmaatregel het volwassenheidsniveau in, waarbij de scores direct aansluiten op de niveaus die in een apart tabblad zijn uitgewerkt. Voor entiteiten die de managementsystematiek aanvullend willen toetsen, is er het tabblad ISMS Evaluatie. Deze evaluatie is facultatief en sluit aan bij de ISO Plan-Do-Check-Act-cyclus. In beide tabbladen kan zowel een score voor de zelfevaluatie worden opgenomen als een score voor de review. Dit laatste kan zowel een interne review zijn, als een externe review (audit of toezichthouder).

De Excel is modulair en flexibel in te zetten. Gebruikers kunnen het framework naar eigen handzetten, door bijvoorbeeld extra velden of tabbladen toe te voegen voor een RACI-matrix, of door een mapping te maken naar een voor de organisatie relevante norm. Standaard bevat het bestand diverse mappings, waaronder de uitvoeringsverordening voor digitale dienstverleners, BIO2 en DORA.

Het tabblad Resultaten biedt een visueel en cijfermatig overzicht. Voor elk thema wordt de score uit de zelfevaluatie vergeleken met het gewenste volwassenheidsniveau, weergegeven in een radardiagram. Daarnaast bevat dit tabblad een tabel met geaggregeerde scores per thema en een tabel met de ruwe scores voor detailinzicht. Voor de ISMS-evaluatie worden de resultaten bovendien weergegeven in een staafdiagram per stap (Plan, Do, Check, Act), eveneens aangevuld met zowel geaggregeerde als ruwe scores. Hierdoor ontstaat een compleet beeld dat zowel op bestuurlijk niveau als in de praktijk houvast biedt.

⁷ [NOREA | Volwassenheidsmodel voor informatiebeveiliging 3.0](#)

Doel Cbw	Sector	Score zelfevaluatie	Toelichting
		2	
		1	
		4	
		3	
		5	



3.5 ISMS evaluatie

Het Cbw (NIS2) Control Framework ondersteunt de evaluatie van de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit en geeft inzicht in de mate waarin een entiteit invulling geeft aan de wettelijke vereisten. De wet stelt dat entiteiten een passende managementsystematiek voor informatiebeveiliging moeten implementeren, maar geeft geen nadere invulling van hoe deze systematiek eruit moet zien (art. 6 lid 4, Cbb).

Om entiteiten een praktische handreiking te bieden, is daarom naast de Cbw evaluatie een facultatieve ISMS evaluatie opgenomen. Deze richt zich specifiek op ISO/IEC 27001 en werkt de normen uit in concrete beheersmaatregelen en volwassenheidsniveaus. Hiermee kan een entiteit op gestructureerde wijze het beleidsproces, het informatiebeveiligingsproces, de borging van maatregelen en de diepgang van controlewerkzaamheden (opzet, bestaan en werking) evalueren.

Het hanteren van een dergelijke systematiek ondersteunt de verantwoordelijkheid van het bestuur, zoals vastgelegd in de Cbw (NIS2): het bestuur moet zorgdragen voor passende beveiligings- en beheersingsmaatregelen en toezien op de implementatie, toetsing en actualisatie ervan (art. 6, Cbb). Entiteiten behouden de vrijheid om een andere systematiek te gebruiken*, mits daarmee aantoonbaar wordt voldaan aan de wettelijke verplichtingen en de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de netwerk- en informatiesystemen wordt gewaarborgd.

* Tenzij zij anderszinds worden verplicht een bepaalde systematiek te volgen, bijvoorbeeld via een ministeriele regeling.

3.6 Inzet van het framework bij implementatie Cbw (NIS2)

Het onderstaande stappenplan laat zien op welke wijze het Cbw (NIS2) Control Framework ingezet kan worden. Voor een succesvolle implementatie van de Cbw, kan dit stappenplan geïntegreerd worden in Cbw programma's bij entiteiten. Het framework kan, in het bijzonder, nuttig zijn bij het analyseren van de gaps (stap 3). Uiteraard is het ook mogelijk het framework op een andere wijze in te zetten.

➤ Stap 1: Asset inventaris

Bij de implementatie van de Cbw (NIS2) is de eerste stap een grondige beoordeling van de kritieke en/of belangrijke processen van de entiteit en de applicaties die deze processen mogelijk maken, vaak de kroonjuwelen genoemd. Voor de kroonjuwelen dienen alle onderliggende assets en hun verhoudingen in kaart gebracht te worden. Betrek hierin de afhankelijkheid van eventuele externe partijen.

➤ Stap 2: Risicoanalyse

De volgende stap is het uitvoeren van een risicoanalyse voor deze assets/ICT-infrastructuur. Deze beoordeling helpt bij het vaststellen van een risicoprofiel en het prioriteren van aandachtsgebieden. Het is van belang dat entiteiten inzicht hebben in hun context en risicoprofiel. De Cbw en Cbb bieden een generiek fundament, maar sluiten niet altijd volledig aan op alle risico's. De evaluatietool biedt daarom ruimte om aanvullende, risicogerichte maatregelen op te nemen die niet expliciet in de Cbw (NIS2) of

sectorale regelgeving zijn benoemd. Dit stelt entiteiten in staat om adequaat in te spelen op eigen dreigingen, afhankelijkheden en kwetsbaarheden.

➤ **Stap 3: Gap analyse**

Na de risicobeoordeling is de volgende stap het uitvoeren van een gapanalyse, op basis van het Cbw (NIS2) control framework. Een dergelijke analyse identificeert waar de entiteit momenteel staat ten opzichte van de vereisten en benadrukt gebieden waar verbeteringen nodig/mogelijk zijn.

➤ **Stap 4: Roadmap**

Op basis van de bevindingen van de gapanalyse moet als laatste stap een plan of routekaart worden ontwikkeld, gericht op oplossingen en mitigerende maatregelen om de geïdentificeerde hiaten en grondoorzaken aan te pakken en naleving van de Cbw (NIS2) te garanderen.



4. Handreiking voor Auditors

4.1 Auditgerichte inzet van het framework

Het framework is ook geschikt voor gebruik door auditors als ondersteuning bij het uitvoeren van audits op het gebied van cyberbeveiliging, of onderdelen daarvan. Het framework kan bijvoorbeeld worden ingezet bij Assurance-opdrachten rond de naleving van de Cbw, specifieke maatregelen uit de Cbb, of bij bredere onderzoeken naar de inrichting en werking van het informatiebeveiligingsbeleid.

4.2 Benutting van zelfevaluaties

In de praktijk verdient het de voorkeur dat de auditor gebruik maakt van een evaluatie die al is uitgevoerd door de organisatie zelf, mits deze voldoende actueel en zorgvuldig is opgesteld. De auditor dient hierbij vanzelfsprekend zelfstandige controlewerkzaamheden uit te voeren om de betrouwbaarheid van de evaluatie te toetsen. Denk hierbij aan documentenanalyse, interviews met sleutelfunctionarissen (zoals de CISO, systeemverantwoordelijken en bestuurders) en waarnemingen ter plaatse. De auditor kan de ingevulde volwassenheidsniveaus en eventuele onderbouwing (zoals opgenomen in het framework) toetsen aan de hand van relevante bewijsstukken en observaties. Een belangrijk aandachtspunt bij het gebruik van het framework is de bepaling van de scope, met name als het gaat om de specifieke systemen of systeemgroepen die onder de beoordeling vallen.

4.3 Scopebepaling en afbakening van systemen

De Cbw (NIS2) stelt in sommige gevallen eisen op systeemniveau, wat betekent dat de auditor kritisch moet nagaan of de opzet van de evaluatie voldoende specifiek en volledig is. Daarnaast is het voor auditors van belang te beseffen dat het framework zich expliciet richt op cyberbeveiliging in het kader van de Cbw (NIS2); andere juridische kaders zoals de AVG (privacywetgeving) vallen buiten de reikwijdte van deze evaluatie en vereisen separate toetsing.

4.4 Opdrachtvorm en toepasselijke standaarden

Afhankelijk van het doel van de audit en de informatiebehoefte van de gebruiker (bijvoorbeeld bestuur, toezichthouder of externe stakeholder), zijn er verschillende typen onderzoeksopdrachten mogelijk, in lijn met de standaarden en richtlijnen van NOREA:

➤ **Standaard 3000A**

Een Assurance-opdracht op basis van Standaard 3000A, waarbij de organisatie een verantwoording opstelt over haar naleving van de Cbw (NIS2) op basis van een zelfevaluatie met het Cbw (NIS2) Control Framework, en de auditor hierop een oordeel formuleert. De zelfevaluatie en bijbehorende onderbouwing kunnen in dat geval dienen als uitgangspunt voor de toetsing.

➤ **Richtlijn 4400**

Een rapport van feitelijke bevindingen (Richtlijn 4400), waarin de auditor objectief vastlegt wat uit de evaluatie en aanvullende controlewerkzaamheden naar voren komt, zonder daar een oordeel over te geven.

➤ **Richtlijnen 210 en 230**

Een overige opdracht, zoals een second opinion of adviesopdracht, waarin het framework wordt gebruikt als leidraad voor analyse of verbetering, zonder dat sprake is van formele Assurance. Hiervoor zullen de richtlijnen 210 en 230 gelden.

Bij de uitvoering van dergelijke opdrachten dienen auditors uiteraard de toepasselijke beroepsregels, standaarden en specifieke NOREA-richtlijnen in acht te nemen. Het is aan de auditor om de opdrachtvorm zorgvuldig te kiezen en deze af te stemmen met de opdrachtgever, mede op basis van het doel van de evaluatie en de mate van zekerheid die gewenst is.

5. Conclusie

De invoering van de Cyberbeveiligingswet (Cbw, NIS2) markeert een nieuwe fase in de aanpak van digitale dreigingen. Entiteiten die onder deze wet vallen, worden niet alleen geconfronteerd met verhoogde eisen op het gebied van cyberweerbaarheid, maar ook met een directe verantwoordelijkheid voor bestuurders om aantoonbaar sturing, toezicht en borging te realiseren. De complexiteit neemt toe doordat naast de generieke verplichtingen uit de Cbw en het Cbb ook sectorspecifieke eisen, zoals BIO2 en DORA, van kracht zijn. Dit maakt een geïntegreerde en systematische benadering onmisbaar.

Het Cbw (NIS2) Control Framework biedt hiervoor een praktisch en flexibel hulpmiddel. Door beheersmaatregelen te koppelen aan concrete volwassenheidsniveaus maakt het framework inzichtelijk wat er van entiteiten verwacht wordt en hoe zij zich kunnen ontwikkelen. De Excel-versie stelt gebruikers in staat het framework naar hun eigen context in te richten, aanvullende normen te integreren en resultaten transparant te visualiseren. Het tabblad Resultaten biedt daarbij overzichtelijke stuurinformatie voor zowel bestuurders als operationele teams, doordat gaps, geaggregeerde scores en detailuitkomsten helder in beeld worden gebracht. De facultatieve ISMS-evaluatie geeft entiteiten bovendien de mogelijkheid om hun managementsystematiek volgens de ISO PDCA-cyclus te toetsen en zo de continue verbeterloop te versterken.

Ook auditors vinden in het framework een waardevol instrument. Het ondersteunt bij het uitvoeren van Assurance-opdrachten, rapportages van feitelijke bevindingen en adviesopdrachten, en sluit aan bij de standaarden en richtlijnen van NOREA. Daarmee vergroot het de consistentie en efficiëntie van audits en draagt het bij aan de betrouwbaarheid van verantwoording richting bestuurders, toezichthouders en ketenpartners.

Het framework vervangt de geldende wet- en regelgeving niet, maar maakt deze inzichtelijk, hanteerbaar en toetsbaar. Het biedt entiteiten de noodzakelijke handvatten om hun verplichtingen te vertalen naar de praktijk, hun cyberweerbaarheid aantoonbaar te versterken en grip te houden in een snel veranderend dreigingslandschap. Daarmee levert het Cbw (NIS2) Control Framework een essentiële bijdrage aan het vergroten van de digitale weerbaarheid van individuele entiteiten, sectoren en de samenleving als geheel.



Het Cbw (NIS2) Control Framework is te downloaden op de websites van de [Auditdienst Rijk](#) en [NOREA](#)