Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Briefnummer
25-123277

Onderwerp
Reactie internetconsultatie Cbb

Den Haag
21 maart 2025

Telefoonnummer
+31620319264

E-Mail
gielens@vnoncw-mkb.nl

Geachte heer, mevrouw,

Met veel belangstelling hebben VNO-NCW en MKB-Nederland kennisgenomen van het concept Cyberbeveiligingsbesluit (Cbb), ter uitwerking van het voorstel voor de Cyberbeveiligingswet (Cbw). De Cbw strekt op haar beurt tot implementatie van de Europese Network and Information Security Directive (NIS2-richtlijn). Wij maken graag gebruik van de mogelijkheid op de consultatie van het Cbb te reageren.

VNO-NCW en MKB-Nederland staan in beginsel positief tegenover de doelen uit de NIS2-richtlijn, namelijk versterking van de digitale en economische weerbaarheid van Europese lidstaten. Vooral in een tijd waarin de digitale dreiging onverminderd groot is, is dit van groot belang.

Echter, kijkend naar de opzet en invulling de nadere regels in voorliggend concept Cbb, vragen wij ons af of deze daadwerkelijk zullen bijdragen aan versterking van de digitale weerbaarheid. Zo komt de risico gebaseerde benadering die centraal staat in de NIS2-richtlijn onvoldoende tot uiting in het Cbb. Die benadering is essentieel omdat het bedrijven/organisaties in staat stelt en stimuleert hun cyberbeveiligingsmaatregelen af te stemmen op hún specifieke risico's. Dit leidt tot gerichter investeren in benodigde cybersecuritymaatregelen én daarmee betere bescherming tegen relevante dreigingen en gevaren.

Daarnaast zien wij een disbalans tussen compliancy en de praktische werkbaarheid en uitvoerbaarheid van de eisen. Het Cbb vraagt om het veelvuldig opstellen en invullen van diverse documenten (beleid, procedures en planvorming). Dit leidt tot een behoorlijke toename van de administratieve regeldruk terwijl de NIS2-richtlijn juist stelt dat er een billijk evenwicht moet zijn tussen de op risico gebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds. De regeldruk ingevolge de Cbb zal veel capaciteit en middelen van bedrijven/organisaties vergen terwijl die juist vooral nodig zijn voor het investeren in noodzakelijke cybersecurity maatregelen en het toetsen van de effectiviteit ervan.

Wij pleiten dan ook richting het coördinerend ministerie van Justitie en Veiligheid, als ook richting de betrokken vakdepartementen, voor het volgende:

1. Herzie de huidige opzet van het Cbb en stel het besluit op aan de hand van duidelijke doelvoorschriften waarbij de invulling in termen van risico gebaseerde en proportionele maatregelen aan bedrijven/organisaties zelf is, en beperk de administratieve belasting
2. Houd vast aan het doel van de NIS2-richtlijn (minimumharmonisatie binnen de EU) en laat conform het Hoofdlijnenakkoord 2024-2028 aanvullende dan wel zwaardere eisen via lagere regelgeving achterwege
3. Houd nadrukkelijk rekening met resources van het mkb en voorzie het mkb van de nodige ondersteuning bij de implementatie van de eisen
4. Zorg ervoor dat de eisen die uit EU-uitvoeringsverordening (voor de digitale sector) worden overgenomen in het Cbb dan wel ministeriele regeling met elkaar in lijn zijn
5. Zorg voor een goede samenloop tussen de Cbw en Wet weerbaarheid kritieke entiteiten ten einde de toezichtslaten voor alle betrokkenen te beperken. Dit betekent: één centraal meldloket; één toezichthouder voor beide wetten; en mogelijkheid dat bedrijven/organisatie via één integrale risicoanalyse en één maatregelenpakket de naleving van hun zorgplicht uit de Cbw én Wwke kunnen aantonen.
6. Leg bij het opstellen van de drempelwaarden voor de meldplicht de focus op continuïteit van de dienstverlening, en voorkom een stapeling van drempelwaarden
7. Leg de focus van het toezicht op de Cbw en Cbb op lerend vermogen
8. Geef z.s.m. inzicht in hoe bedrijven/organisaties met complexe bedrijfsmodellen zich verhouden tot de Cbw zodat zij weten of ze onder de reikwijdte van Cbw vallen
9. Kom daadwerkelijk tot een afgestemde aanpak in het toezicht en handhaving om de toezichtslasten voor alle betrokkenen zoveel als mogelijk te beperken
10. Houd rekening met de complexiteit van bedrijven/organisaties met meerdere entiteiten, en bezie hoe voor hen de lastendruk kan worden gereduceerd

In de bijlage worden bovenstaande zorgpunten nader belicht, gevolgd door een artikelsgewijze reactie.

Uiteraard zijn wij bereid een nadere toelichting te geven op onze reactie. Hiervoor kunt u contact opnemen met Sabine Gielens (zie boven voor de contactgegevens).

Wij wensen u veel succes met de verwerking van de reactie op de internetconsultatie.

Met vriendelijke groet,

Erik te Brake
Manager Fysieke omgeving en markten

Bijlage met reactie van VNO-NCW en MKB-Nederland op het concept Cyberbeveiligingsbesluit (Cbb)

Algemene opmerkingen / aandachtspunten

1. **Herzie de huidige opzet van het Cbb en stel het besluit op aan de hand van duidelijke doelvoorschriften waarbij de invulling in termen van risico gebaseerde en proportionele maatregelen aan bedrijven/organisaties zelf is, en beperk de administratieve belasting**
   Het concept Cbb bevat een veelvoud aan voorgeschreven procedures, beleid en planvormingen. In nagenoeg elk artikel én sub artikel van hoofdstuk 4 (zorgplicht) van het Cbb wordt van bedrijven/organisaties geëist dat zij over vastgesteld beleid, procedures dan wel planvorming moeten beschikken, gevolgd door een uiteenzetting van wat het beleid, procedures en planvorming moet omvatten. Met deze opzet wordt de focus van het Cbb gelegd op *compliancy*. In de regel moet er een goede balans zijn tussen compliancy en praktische werkbaarheid en uitvoerbaarheid. Die balans ontbreekt nagenoeg volledig in voorliggend concept besluit.
   De huidige opzet van het Cbb is volgens ons ook niet in lijn met de *Network and Information Security Directive* (NIS2-richtlijn). In de NIS2-richtlijn staat de risico gebaseerde benadering centraal, waarbij het aan bedrijven/organisaties zélf is om passende en evenredige maatregelen te treffen om de geïdentificeerde risico's voor de beveiliging van de netwerk- en informatiesystemen te beheren. In het verlengde daarvan, hebben wij in overleggen met het coördinerende ministerie van Justitie en Veiligheid (JenV) aangegeven dat de overheid zich zou moeten beperken tot het stellen van duidelijk omschreven *doelvoorschriften* waarbij de invulling aan bedrijven/organisaties zélf is. Deze werkwijze zou niet alleen in lijn zijn met de NIS2-richtlijn, maar dwingt bedrijven/organisaties bovenal om zélf op een risico gebaseerde wijze na te denken over wat nodig is en daadwerkelijk bijdraagt aan de beveiliging en continuïteit van hun netwerk- en informatiesystemen die randvoorwaardelijk/kritisch zijn voor hun essentiële- dan wel belangrijke dienstverlening.
   De huidige opzet van het concept Cbb leidt vooral tot het veelvuldig opstellen en invullen van diverse documenten. Dit betekent voor bedrijven/organisaties een enorme toename in de administratieve lasten dat zeer veel capaciteit - in mensen en middelen - vergt waarbij wij ons ten zeerste afvragen of dit de cyberveiligheid en weerbaarheid ten goede komt.
   VNO-NCW en MKB-Nederland doen via deze weg de dringende oproep om de opzet van voorliggend Cbb te herzien en op te stellen aan de hand van duidelijk omschreven doelvoorschriften waarbij bedrijven/organisaties zelf evenredige maatregelen identificeren en treffen die passend zijn bij de risico's, aard en omvang van het bedrijf/organisatie.

2. **Houd vast aan het doel van de NIS2-richtlijn (minimumharmonisatie) en laat aanvullende dan wel zwaardere eisen via lagere regelgeving achterwege**
   Eén van de doelen achter de NIS2-richtlijn is om de bij de NIS1-richtlijn geconstateerde verschillen t.a.v. de uitvoering van de verplichtingen op nationaal niveau - zoals het soort cyberbeveiligingseisen en de mate van gedetailleerdheid - weg te nemen. Deze verschillen kunnen nl. nadelige effecten hebben op de werking van de interne markt en kunnen sommige lidstaten meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele EU. VNO-NCW en MKB-Nederland onderschrijven de noodzaak van harmonisatie van harte.
   Echter, wanneer lidstaten via lagere regelgeving (besluiten en regelingen) alsnog aanvullende eisen gaan stellen, wordt dit beoogde doel niet bereikt en ontstaat een toename van de lastendruk als gevolg van divergerende regelgeving.

VNO-NCW en MKB-Nederland doen dan ook de dringende oproep om conform
- het Hoofdlijnenakkoord 2024-2028 (waarin is afgesproken geen nationale koppen op Europese regelgeving te zetten) en
- de MvT bij het wetsvoorstel Cbw (waarin staat dat er niet wordt gekozen voor zwaardere eisen dan de minimumeisen van de NIS2-richtlijn)

via lagere regelgeving géén aanvullende / zwaardere eisen te stellen dan de minimumeisen uit de NIS2-richtlijn, en voorliggend concept Cbb daarop te herzien. Hierbij gaat het o.a. om de extra eisen die aan de training van bestuurders wordt gesteld (art. 22), maar ook t.a.v. noodcommunicatiesystemen (art. 9), het omgaan met informatie (art. 16) en het verstrekken van gegevens (art. 25).

3. **Houd nadrukkelijk rekening met resources van het mkb en voorzie het mkb van ondersteuning bij de implementatie van de eisen**
De NIS2-richtlijn bevat ten opzichte van de NIS1-richtlijn een forse doelgroep uitbreiding. Hiermee zullen er ook meer mkb-bedrijven onder de Cyberbeveiligingswet (Cbw) en Cbb komen te vallen. Dit zal de eerder door de Cyber Security Raad geconstateerde weerbaarheidskloof doen verkleinen en de (waarde)ketens versterken.
VNO-NCW en MKB-Nederland onderschrijven dit belang ten zeerste. Tegelijkertijd pleiten wij ervoor om bij de implementatie van de NIS2-richtlijn via de Cbw en Cbb als ook in het toezicht rekening te houden met de resources van mkb-bedrijven. In lijn met de uitkomsten van het MKB-panel (blz. 4 van de Nota van toelichting, Nvt), dienen de vereisten haalbaar en proportioneel te zijn. Zo wordt bv. in artikel 6 van het concept Cbb om een managementsystematiek gevraagd. Het is van belang dat deze systematiek past bij de aard en omvang van mkb-bedrijven. Voorkomen moet worden dat de wetgever en de toezichthouder van mkb bedrijven een vergelijkbaar en omvangrijk managementsysteem wordt verwacht, zoals bij grote (internationale) bedrijven.
Daarnaast pleiten wij voor gerichte overheidsondersteuning aan het mkb, in de vorm van tools, sjablonen en handreikingen, onder meer gericht op het opstellen van risicoanalyses en de te nemen maatregelen. Welke algemene risico's moeten bv. betrokken worden in de risicoanalyse etc. Maak daarbij gebruik van bestaande mkb-kanalen en aanwezige kennis, zoals bv. ons platform Samen Digitaal Veilig en het Digital Trust Center.

4. **Zorg ervoor dat de eisen die uit EU-uitvoeringsverordening worden overgenomen in het Cbb dan wel MR met elkaar in lijn zijn**
In het concept Cbb en geconsulteerde concept ministeriële regeling (MR) worden bepaalde zorgplichteisen uit de Europese uitvoeringsverordening voor de digitale sector (EU) 2024/2690) overgenomen. Door aanpassing van bewoordingen dan wel een net iets andere weergave, is niet altijd duidelijk of hetgeen gevraagd wordt, overeen komt met de eisen uit de uitvoeringsverordening en/of dat er via het Cbb dan wel MR aanvullende eisen worden gesteld. Voor bedrijven/organisaties die onder beide regimes vallen (de Cbw én de uitvoeringsverordening) maakt dit de implementatie onnodig complex.
VNO-NCW en MKB-Nederland pleiten ervoor dat verplichtingen die overgenomen worden uit de uitvoeringsverordening in de Cbb en/of MR één-op-één op elkaar aansluiten, dan wel wordt toegelicht hoe deze beide regelgevingen zich tot elkaar verhouden in geval van verschillen. Dit uitgangspunt zien we graag in artikel 4 en 19 van het Cbb, dan wel in de Nvt terug.

5. **Zorg voor een goede samenloop tussen de Cbw en Wwke ten einde de toezichtslaten voor alle betrokkenen te beperken**
   Om dubbele lasten aan de zijde van zowel bedrijven/organisaties als ook de overheid te voorkomen, is het van belang dat de samenloop tussen de Cbw en Wet weerbaarheid kritieke entiteiten (Wwke) goed geregeld wordt. Dit betekent:
   - Één centraal meldloket voor meldingen onder de Cbw en Wwke (en idealiter ook voor meldingen onder sectorale wetgeving);
   - Één en dezelfde toezichthouder voor beide wetten die integraal toezicht houdt;
   - De mogelijkheid dat entiteiten via één integrale risicoanalyse en één pakket aan (aanvullende) maatregelen de naleving van hun zorgplicht uit de Cbw én Wwke aan de toezichthouder kunnen aantonen. Zoals vorig jaar aangegeven in onze reactie op de wetsvoorstellen Cbw en Wwke, werken bedrijven/organisaties veelal op basis van een all hazards benadering waarbij fysieke en digitale beveiliging en weerbaarheid integraal worden bezien en beoordeeld. Opname van deze mogelijkheid in de Nvt geeft bedrijven/organisaties houvast en voorkomt evt. discussies met de toezichthouder(s).

6. **Leg bij het opstellen van de drempelwaarden voor de meldplicht de focus op continuïteit van de dienstverlening en voorkom stapeling van drempelwaarden**

   - VNO-NCW en MKB-Nederland zijn blij om te lezen dat in de Nvt staat aangegeven dat sectoren worden betrokken bij het opstellen van de drempelwaarden. Bij sectoren zit immers de benodigde kennis en expertise die nodig is om te komen tot proportionele en bovenal zinvolle drempelwaarden.
   - Hetgeen wij ons echter afvragen is of het verstandig is om deze drempelwaarden in een openbare MR vast te leggen. De drempelwaarden houden - als het goed is - verband met de continuïteit van het essentiële / belangrijke proces en kunnen daarmee gevoelige informatie bevatten. Wij willen graag ter overweging meegeven om de uitgewerkte sectorale drempelwaarden als vertrouwelijk te behandelen en niet in een MR op te nemen.
   - Hierop vooruitlopend pleiten wij ervoor dat bij het opstellen van drempelwaarden de focus ligt op continuïteit van de essentiële of belangrijke dienstverlening / borging van de leveringszekerheid (ofwel op die dienstverlening op basis waarvan de entiteiten als essentieel of belangrijk zijn aangemerkt). Temeer gezien de administratieve lastendruk die de meldplicht met zich meebrengt voor entiteiten.
   - Voor bedrijven/organisaties die onder meerdere sectoren vallen, is het van belang dat de drempelwaarden door de betrokken vakdepartementen en toezichthouders op elkaar worden afgestemd. Uiteraard weer in samenspraak met de betrokken bedrijven/ organisaties. Een ‘simpele stapeling’ van drempelwaarden leidt tot onduidelijkheid, misverstanden en verhoging van de toezichtslasten.
   - Tevens doen wij de oproep aan alle betrokken vakdepartementen om op korte termijn (en dus in overleg met de sectoren) tot uitwerking van de drempelwaarden te komen zodat bedrijven/organisaties de tijd hebben om deze correct te implementeren.
   - Tot slot pleiten wij (nogmaals) voor het het op- en inrichten van één centraal meldportaal voor meldingen die entiteiten moeten doen op grond van verschillende wetgeving. Dit zou de toezichtslasten voor bedrijven/organisaties aanzienlijk verminderen, met name op die momenten waarin zij zich bezig zouden moeten houden met het oplossen/verhelpen van het (mogelijke / dreigende) incident in plaats van het doen van meldingen bij verschillende overheidsportalen.

7. **Leg de focus van het toezicht op lerend vermogen**
   Ambitie van het Rijk is dat de Cbw in Q3 2025 van kracht gaat. Dit betekent dat bedrijven/organisaties vanaf dat moment ook compliant moeten zijn. Wij begrijpen dat dit

ingegeven de NIS2-richtlijn is. De NIS2-richtlijn bevat in tegenstelling tot bv. de Wwke geen implementatietermijn. Echter, tussen de consultatie van onderhavige AMvB en ministeriële regeling (MR) - waarmee bedrijven/organisaties pas echt inzicht krijgen in de exacte eisen die aan hen gesteld worden - en Q3 van dit jaar, zit zeer weinig tijd en ruimte om 100% compliant te worden. Zoals hierboven reeds aangegeven, schrijven het Cbb en onderliggende MR een veelvoud aan beleid, procedures en planvormingen voor. Met name voor bedrijven/organisaties die tot de nieuwe doelgroep onder de NIS2-richtlijn horen, zal dit behoorlijk veel capaciteit, tijd en inspanning vergen. Daarnaast bestaat er bij een aantal bedrijven/organisaties nog altijd onduidelijkheid of zij überhaupt onder de Cbw vallen (zie punt 8).
Bij de invulling van het toezicht op de Cbw, Cbb en MR, pleiten wij dan ook - met name voor bedrijven/organisaties onder de nieuwe doelgroep - voor een ingroeiperiode. Daarnaast dient voor alle bedrijven/organisaties onder de Cbw het toezicht in eerste instantie vooral gericht te zijn op lerend vermogen waarbij gekeken wordt naar maximale effort vanuit bedrijven/organisaties.

8. **Geef z.s.m. inzicht in hoe bedrijven/organisaties met complexe bedrijfsmodellen zich verhouden tot de Cbw zodat zij weten of ze onder de reikwijdte van Cbw vallen**
VNO-NCW en MKB-Nederland pleiten sinds geruime tijd voor duidelijkheid over de reikwijdte van de Cbw voor bedrijven/organisaties met complexe bedrijfsmodellen en/of samengestelde bedrijven. Vanuit JenV/NCTV wordt i.s.m. de vakdepartementen gewerkt aan een schriftelijke uitwerking van complexe bedrijfsmodellen / samengestelde bedrijven in relatie tot de Cbw maar die is nog altijd niet voor handen. Hierdoor is het voor een aantal bedrijven/organisaties nog altijd niet helder in hoeverre zij onder de Cbw vallen en straks te maken krijgen met een wettelijke zorg- en meldplicht. Uiteraard is het treffen van de nodige cybersecurity-maatregelen voor elke bedrijf/organisatie een no-regret maatregel, echter, dat is nog iets anders dan straks onder wettelijke toezicht te staan. Via deze weg doen wij nogmaals de oproep om z.s.m. met de schriftelijke uitwerking te komen.

9. **Kom daadwerkelijk tot een afgestemde aanpak in het toezicht en handhaving om de toezichtslasten voor alle betrokkenen zoveel als mogelijk te beperken**
In de MvT bij de Cbw staat opgenomen dat voor borging van een doeltreffende en doelmatige uitvoering van de Cbw, de toezichthoudende instanties onderling afspraken maken over gemeenschappelijke aangelegenheden. Hier zijn wij erg blij mee, en via deze weg willen wij nogmaals het belang benadrukken van een transparante- en op elkaar afgestemde aanpak in het toezicht en handhaving om de toezichtslasten voor álle betrokken (bedrijfsleven én overheid) partijen zoveel mogelijk te beperken.
Voor bedrijven/organisatie die onder meerdere sectoren vallen en daarmee meerdere toezichthouders hebben, dienen heel duidelijke afspraken gemaakt te worden wie van de toezichthouders de coördinatie - en bij voorkeur regie - neemt in het toezicht met daarbij goede afspraken over wederzijdse informatievoorziening i.v.m. de politieke verantwoordelijkheden.
Naar verluidt wordt de samenloop met de Wwke ook betrokken bij de afspraken. Ook dat ondersteunen we zeer, temeer wanneer bedrijven/organisaties voor de Cbw en Wwke met verschillende toezichthouders te maken krijgen.
Idealiter zou (in de nabije toekomst) via deze weg ook de samenwerking en afstemming met andere toezichthouders vorm moeten krijgen, zoals met de Omgevingsdienst.

10. **Houd rekening met de complexiteit van bedrijven/organisaties met meerdere entiteiten, en bezie hoe voor hen de lastendruk kan worden gereduceerd**
    Er zijn bedrijven/organisaties die uit meerdere juridische entiteiten bestaan. Denk bv. aan gecombineerde energiebedrijven, met onder andere opwek (zoals windparken, zonneparken, centrales, warmte), levering (bijv. administratie, marketing, retail), handel (o.a. inkoop, verkoop, balancering), advies en diensten (laadparken, congestie, isolatie). In veel gevallen is elke activiteit (en dus ook elk windpark, zonnepark, etc.) in een aparte juridische entiteit ondergebracht. Zowel het hoofdbedrijf als de juridische entiteiten vallen in het voorbeeld hierboven veelal onder de reikwijdte van de Cbw. Deze inrichting brengt met oog op de eisen uit de Cbw en Cbb behoorlijk wat administratieve lasten met zich mee. Zo moet elke juridische entiteit binnen het hoofdbedrijf zich separaat registeren in het nationaal register. Bij bepaalde bedrijven gaat het om meer dan 100 juridische entiteiten die zich allen moeten registeren.
    VNO-NCW en MKB-Nederland pleiten ervoor dat in bovengenoemde gevallen, het hoofdbedrijf de mogelijkheid krijgt om via een volmacht vanuit de betrokken juridische entiteiten zich éénmaal middels eHerkenning registreert namens het hoofdbedrijf én de betrokken juridische entiteiten.
    Ook in relatie tot de zorg- en meldplicht van deze individuele juridische entiteiten, vragen VNO-NCW en MKB-Nederland de wetgever als ook de toezichthouders (meer) rekenschap te geven van de operationele uitdagingen die dit met zich mee brengt. Wij pleiten ervoor dat deze problematiek en de mogelijkheden om hier op een meer pragmatische wijze mee om te gaan, expliciet aan de orde komt in de bij punt 9 genoemde aanpak in het toezicht en handhaving. Vanuit VNO-NCW en MKB-Nederland zijn wij, alsmede onze leden, uiteraard graag bereid hierover mee te denken.

Artikelsgewijze opmerkingen

11. **Dubbelingen**
    De regels in voorliggend concept Cbb lijken in een aantal gevallen herhalingen te zijn:
    - De verplichting om rollen en verantwoordelijkheden vast te stellen staat in art. 6.2, maar komt terug in art. 8.1 en art. 14.1.
    - Art. 7.1 vraagt om vastgesteld beleid over risicomanagement voor de beveiliging van netwerk- en informatiesystemen. Vervolgens vraagt art. 16.2 om beleid voor het beheer van assets om systemen op verschillende risico niveaus te kunnen classificeren.
    - Art. 10 vraagt om schriftelijke afspraken te maken met leveranciers inzake cyberbeveiligingseisen. In art. 11 lid 1 komt dit vervolgens terug: “deze eisen maken waar mogelijk deel uit van de overeenkomsten”.

    Oproep is om herhalingen te voorkomen en om tot meer samenhang tussen de artikelen in het Cbb te komen.

12. **Artikel 5 (uitvoering van art. 21 van de wet)**
    Ter verduidelijking van de reikwijdte van de artikelen 6 tot en met 18 (en overeenkomstig de NIS2-richtlijn), zouden wij in artikel 5 graag toegevoegd willen zien dat het hier gaat om maatregelen om de risico’s voor de beveiliging van de netwerk- en informatiesystemen, die entiteiten voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te beheersen.

13. **Artikel 6 (beleid over beveiliging van netwerk- en informatiesystemen)**
    In dit artikel ontbreekt de belangrijke notie dat het beveiligingsniveau van de netwerk- en informatiesystemen dient te zijn afgestemd op de risico’s die zich voordoen. Verzoek is om dit toe te voegen.

14. **Artikel 7 (beleid over risicomanagement)**
    Artikel 7 stelt dat entiteiten over risicomanagement-beleid moeten beschikken en op basis daarvan maatregelen moeten treffen. Hetgeen waaraan voorbij wordt gegaan zijn de processtappen van risico's inventariseren en risico's kwantificeren en analyseren. Op basis van het laatste worden beheersmaatregelen geformuleerd, en niet op beleid.
    VNO-NCW pleiten ervoor dit artikel aan te passen naar het reguliere proces van risicomanagement.

15. **Artikel 9 (bedrijfscontinuïteit en crisisbeheer)**
    Lid 1 gaat uit van de vooronderstelling dat een incident zal leiden tot het in werking treden van het bedrijfscontinuïteitsplan. Sommige incidenten zullen echter een beperkte impact hebben en niet resulteren in het in werking stellen van het plan. Verzoek is om deze notie te betrekken bij de formulering van lid 1.

16. **Artikel 9 (bedrijfscontinuïteit en crisisbeheer)**
    - In dit artikel ontbreekt de risico gebaseerde benadering. Verzoek is om dit toe te voegen.
    - In lid 3 sub b wordt in relatie tot het gebruik van beveiligde noodcommunicatiesystemen de term 'ten tijde van crisis' geïntroduceerd. In de NIS2-richtlijn wordt niet over crisis gesproken. Ten tijd van een crisis is het beschikken over communicatie al een hele opgave, laat staan beveiligde communicatie. VNO-NCW en MKB-Nederland pleiten ervoor om de term 'crisis' hier achterwege te laten.

17. **Artikel 10 (beveiliging van de toeleveringsketen)**
    - In lid 2 wordt gesproken over 'het waar mogelijk' afspraken maken met leveranciers en dienstverleners. Hieruit kan worden afgeleid dat het maken van afspraken geen harde eis is. Is dat correct? Graag verduidelijking op dit punt.
    - VNO-NCW en MKB-Nederland zouden in lid 2 graag expliciet de risico gebaseerde benadering willen terugzien daar waar het gaat om het stellen van cyberbeveiligingseisen aan leveranciers en dienstverleners. Het is van belang dat de eisen die door NIS2-bedrijven en organisaties aan toeleveranciers en dienstverleners (veelal mkb) worden gesteld proportioneel en risicogericht zijn teneinde onnodige administratieve lasten en investeringen te voorkomen. Tekstvoorstel: *De essentiële entiteit of belangrijke entiteit maakt waar mogelijk schriftelijke afspraken met haar rechtstreekse leveranciers en rechtstreekse dienstverleners van de producten en diensten, bedoeld in het eerste lid, over de aan die rechtstreekse leveranciers en rechtstreekse dienstverleners te stellen* ***risico gebaseerde*** *cyberbeveiligingseisen en borgt dat deze afspraken worden nagekomen. De entiteit houdt de afspraken actueel.* Hetzelfde zouden we ook graag terug zien in de Nvt. Nu staat daar dat bij het maken van afspraken rekening kán worden gehouden met de geïdentificeerde risico's. Die kán-bepaling dient vervangen te worden door een moet-bepaling.
    - Tevens pleiten we in lid 2 ervoor dat waar het gaat om borging van het nakomen van de afspraken met leveranciers en dienstverleners, de principes *haalbaarheid* en *evenredigheid* worden toegevoegd. Zoals ook staat uiteengezet in de Nvt, zijn bedrijven/organisatie niet altijd in de positie om over cyberbeveiligingseisen te onderhandelen, met name waar het grote leveranciers of dienstverleners betreffen.
    - Tot slot, in de Nvt staat over dit laatste dat bedrijven/organisaties, wanneer zij niet in de positie zijn om over cyberbeveiligingseisen te onderhandelen, moeten beoordelen of het cyberbeveiligingsniveau dat de betreffende leverancier aanbiedt passend is gezien de risico's. Vervolgens staat er dat de entiteit ook moet beoordelen of er aanvullende maatregelen getroffen moeten worden of dat er voor een andere leverancier moet worden gekozen.

Het in de Nvt opnemen van de overweging om van leverancier te veranderen, vinden VNO-NCW en MKB-Nederland om meerdere redenen té ver gaan. Eén, invulling van noodzakelijke maatregelen is aan bedrijven/organisaties zelf. Ten tweede, het wordt uit de Nvt niet duidelijk of het veranderen van leverancier terugslaat op de eerder genoemde grote leveranciers/dienstverleners of over álle mogelijke leveranciers/dienstverleners gaat. Daar waar het gaat om mkb als leverancier of dienstverlener, is het des te meer ongewenst om vanuit de overheid te pleiten voor een verandering van leverancier/dienstverlener. Juist mkb-leveranciers/dienstverleners hebben ruimte nodig om hun beveiligingsniveau te verhogen en zich aan te passen aan de nieuwe normen. De overheid zou juist moeten inzetten op ondersteuning en samenwerking, niet op directe vervanging. Daarnaast kan het verlies aan mkb-leveranciers/dienstverleners leiden tot verstoringen in productie- en datastromen.
VNO-NCW en MKB-Nederland dringen erop aan om de zinsnede rondom het kiezen voor een andere leverancier achterwege te laten.

18. **Artikel 11 (beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen)**
Bij artikel 11 dient (evt. via de Nvt) een koppeling gemaakt te worden met de Cyber Resilience Act (CRA) die bindende eisen stelt aan de cyberveiligheid van digitale producten. Bedrijven/organisaties moeten controleren of leveranciers de juiste waarborgen heeft maar niet zelf de eisen voor haar producten ontwikkelen. Dat laatste vindt op Europees niveau plaats, op basis van de CRA.

19. **Artikel 12 (basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging)**
In lid 2 pleiten wij ervoor dat de term opleiding wordt vervangen door cursus of training. Een opleiding is van lange duur en impliceert dat een erkend diploma behaald dient te worden terwijl – kijkende naar de Nvt – het hier veel meer gaat om het actueel houden van kennis of kunde en/of het bijleren ervan. De termen cursus of training die kortdurend maar wel frequent zijn, sluiten hier beter bij aan.

20. **Artikel 13 (beleid over het gebruik van cryptografie)**
In lid 1 ontbreekt de risico gebaseerde benadering. Verzoek is om dit toe te voegen.

21. **Artikel 16 (beveiligingsaspecten t.a.v. beheer van assets)**
    - Wat wordt in lid 1 bedoeld met ‘beleid voor de werking van netwerk- en informatiesystemen’? Moet in beleid worden vastgelegd hoe de werking van het stelsel van maatregelen wordt geëvalueerd of getoetst? Graag verduidelijking op dit punt.
    - In lid 2 wordt de eis gesteld dat er regels moeten zijn voor ‘het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en gerelateerde netwerk- en informatiesystemen’. Restricties t.a.v. het gebruik van informatie worden gesteld in andere wetgeving, zoals bv. data privacy wetgeving. Vraag is wat wordt hier exact bedoeld, en de wijze waarop het nu staat weer gegeven lijkt dit op een nationale kop op de NIS2 en gaat verder dan cyberbeveiliging.
    - Lid 3 vervolgens ‘een inventaris van informatie en andere gerelateerde netwerk- en informatiesystemen’. Door om een inventaris van informatie te vragen, lijkt dit opnieuw op een nationale kop op de NIS2-richtlijn. Niet elk bedrijf/organisatie dat NIS2-plichtig is zal een inventaris van informatie nodig hebben om management van cyberbeveiliging te ondersteunen. Daarnaast hebben bedrijven/organisaties niet noodzakelijkerwijs één geïntegreerd inventaris van informatie en systemen.

22. **Artikel 17 (attenderingen, adviezen en informatie)**
De strekking van dit artikel is veel te breed, en leidt tot onnodige administratieve lasten. VNO-NCW en MKB-Nederland pleiten ervoor het artikel op een tweetal aspecten in te perken. Bij 'relevante kwetsbaarheden en cyberdreigingen' dient een bepaalde mate aan criticaliteit worden toegevoegd, denk aan inperking tot *high-high alerts* zoals we die kunnen vanuit het Nationaal Cyber Security Centrum (NCSC).
Daarnaast dienen de relevante partijen te worden ingeperkt naar enkel overheidspartijen (CSIRT's, bevoegde autoriteiten en andere betrokken overheidsinstanties). Daarbij moet in ogenschouw worden genomen dat gerubriceerde informatie vanuit de inlichtingen- en veiligheidsdiensten veelal niet mag worden vastgelegd. Uiteraard wordt in de praktijk ook gekeken naar- en geacteerd op meldingen vanuit leveranciers e.d. maar het is ondoenlijk om voor álle meldingen een schriftelijke beoordeling vast te leggen. Vandaar het voorstel om dit te beperken tot meldingen vanuit overheidspartijen.

23. **Artikel 20 (doel van de training)**
In de NIS2-richtlijn, art. 20, staat dat leden van bestuursorganen een opleiding moeten volgen zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.
Dit artikel uit de NIS2-richtlijn is in de Cbw én Cbb niet juist overgenomen. In de Cbw en Cbb wordt nl. niet gesproken over risicobeheerspraktijken maar over risicobeheersmaatregelen. Dit zijn twee verschillende zaken. Waar het bij risicobeheerspraktijken veel meer gaat over de algemene aanpak, methoden en strategieën, gaat het bij risicobeheersmaatregelen om concrete acties die worden getroffen om geïdentificeerde risico's te beperken. Het niveau waarop de governance eisen nu in de Cbw en Cbb zijn geformuleerd, is niet correct en sluit niet aan bij wat van een bestuurder mag worden verwacht.
VNO-NCW en MKB-Nederland dringen erop aan om het voorstel voor de Cbw hierop aan te passen (artikel 24, lid 2 sub b), alsmede het voorliggend Cbb (artikel 20 én artikel 21 lid 2).

24. **Artikel 22 (eisen aan de trainer)**
Wij zijn verbaasd door de aanvullende eisen die aan de opleiding van leden van het bestuur worden gesteld. VNO-NCW en MKB-Nederland onderschrijven uiteraard de nut en noodzaak van een goede scholing voor bestuurders op het gebied van cybersecurity. Wij hebben echter bezwaren tegen de eis dat deze scholing door een onafhankelijke trainer gegeven moet worden. Vooral in organisaties waar reeds diepgaande cybersecurity expertise aanwezig is werkt deze eis contraproductief. Een externe trainer kent de specifieke context en risico's van de organisatie veel minder goed dan interne experts, waardoor de training minder effectief wordt.
Daarnaast gaat Nederland met deze eis verder dan de NIS2-richtlijn voorschrijft, waarin alleen het voltooien van een training en opdoen van noodzakelijke kennis voorgeschreven is. Het stellen van extra eisen leidt binnen de EU tot een ongelijk speelveld, en administratieve complicaties voor bedrijven die in meerdere lidstaten actief zijn. Daarnaast staat – in reactie op vragen vanuit het Adviescollege toetsing regeldruk – in de MvT bij de Cbw dat er op dit moment geen aanleiding is om te kiezen voor zwaardere eisen dan de

minimumeisen van de richtlijn. De inhoud van artikel 22 is daar naar onze mening niet mee in lijn.
Tot slot brengt deze eis aanzienlijke kosten met zich mee die niet per definitie noodzakelijk zijn en/of tot een beter eindresultaat zal leiden. Bovendien zal de aanvullende eis leiden tot een wildgroei aan opleidingsprogramma's en certificaten.
Ons voorstel is om de nadere eisen achterwege te laten en - aan de hand van een duidelijke doelomschrijving van de training en beoogde uitkomst - de invulling aan bedrijven/organisaties over te laten, passend bij hun aard, omvang en bestaande werkwijzen. Een overweging is om vanuit de overheid een handreiking op te stellen over de opzet en invulling van de training, maar laat de primaire verantwoordelijkheid waar deze hoort, nl. bij bedrijven/organisaties zelf. Mocht vanuit het toezicht worden gesignaleerd dat aanscherping nodig is, kan dat altijd nog.

25. **Artikel 25 (gegevens waar een vroegtijdige waarschuwing uit moet bestaan)**
Artikel 25 schrijft ten opzichte van de NIS2-richtlijn en artikel 26 uit de Cbw aanvullende eisen voor t.a.v. de gegevens die verstrekt moeten worden bij een vroegtijdige waarschuwing. Insteek van de Cbb zou nadere uitwerking moeten zijn (o.a. ter verduidelijking), en niet aanvullende eisen.
Bij de in artikel 25 gevraagde gegevens is het de vraag of bedrijven/organisaties deze gelet op de extreem korte doorlooptijd om zaken te verifiëren en te beoordelen, überhaupt kunnen verstrekken.
VNO-NCW en MKB-Nederland dringen er allereerst op aan om het stellen van aanvullende eisen, bovenop de NIS2-richtlijn, via de Cbb achterwege te laten.
Indien het Rijk bepaalt dat zij de eisen zoals opgenomen in artikel 25 toch wil behouden, pleiten wij ervoor om voorafgaande aan de opsomming a-c het volgende de woorden ‘zo mogelijk’ op te nemen.

26. **2.4 van de Nvt (Aanwijzing CSIRT)**
In de Nvt staat dat het CSIRT onder meer tot taak om entiteiten in geval van dreigingen, kwetsbaarheden en incidenten vroegtijdig te waarschuwen en bijstand te verlenen. Vraag is: wanneer en wat kunnen entiteiten als het gaat om bijstand van het CSIRT verwachten? In het kader van verwachtingenmanagement is het van belang dat dit op voorhand richting entiteiten wordt verduidelijkt. Wat kan het NCSC bieden, en bovenal, kan zij dit ten tijde van een (grootschalige) dreiging of crisis ook daadwerkelijk waarmaken qua capaciteit?