Sern

Stichting Security Expert Register Nederland

SECRETARIAAT SERN
WASSINKBRINKWEG 3
7021 JZ ZELHEM
06 – 3033 9055
SECR-SERN@SERN.NL

De Stichting Security Expert Register Nederland (SERN) is voor haar meer dan 700 geregistreerde physical security professionals dé koepelvertegenwoordiger bij de internetconsultatie inzake de vertaalslag van de CER richtlijn naar de concept Wet weerbaarheid kritieke entiteiten. Hiertoe heeft SERN uit haar midden een Adviescommissie CER ingesteld met als doel de implementatie van bruikbare regelgeving te bewerkstelligen.
De belangenbehartiging vindt plaats vanuit haar statuten met de scope op physical security.

Hieronder treft u de inbreng van de SERN Adviescommissie CER wetgeving

1. **Voor een betere duiding is de opsomming van de Wwke artikelen op één A4 geplaatst en als Bijlage 1 bij deze notitie gevoegd.**

   Wellicht is daarbij ook te overwegen een trefwoordenregister toe te voegen bij zowel de wet als de Memorie van Toelichting

2. **De overheid kondigt 8 AMvB's aan om nadere regels uit te vaardigen.**

   SERN stelt zich hierbij beschikbaar om als platformpartner ondersteuning te bieden bij de totstandkoming van bruikbare en in de markt al gangbare, gedragen nadere regels en vast te leggen in de AMVB's.

   Bijlage 2: de genoemde AMvB's in de Wwke artikelen 3, 10, 14, 16, 18, 31a en 35

3. **In de informatie brochure Wwke staat op bladzijde 6**
   Kritieke entiteiten zijn automatisch ook essentiële entiteiten in de zin van de Cyberbeveiligingswet en moeten – na aanwijzing als kritieke entiteit - ook aan die verplichtingen voldoen.
   In de Wwke is dat in geen enkel artikel opgenomen.
   SERN stelt voor om deze zin ook alsnog in de Wwke op te nemen.

   In bijlage 3 de vermelding van Cbw artikel 8.1.i

   De vraag is dan wel: welke Cbw maatregelen zijn dan voor het uitvoeren ervan van toepassing?
   Is dat de opsomming bij artikel 21 lid 2van de NIS2?

   In bijlage 4 de opsomming bij artikel 21 lid 2van de NIS2

   Voor een betere duiding zijn in bijlage 5 de Cbw artikelen op rij geplaatst

4. Artikel 10 Wwke: Ondersteuning aan kritieke entiteiten

In bijlage 6: in artikel 10 wordt aangegeven het ontwikkelen van richtsnoeren en methodologieën

Wij stellen u voor om in art. 10 vooral aan te sluiten bij de methodologieën, richtsnoeren en instrumenten die ook thans al in de markt aanwezig zijn en breed zijn ingevoerd.

Tekstvoorstel om bestaande richtsnoeren, methodologieën en formats te noemen

Er zijn diverse instrumenten en methodieken al in gebruik waardoor eenvoudig in Art. 10 kan worden voorzien. U kunt hierbij denken aan de verschillende kwaliteitsmeetsystemen waaronder de zogenoemde DHM methodiek, maar ook andere security managementplatformen zoals de meer internationaal georiënteerde ASIS methodieken, de ISO 27001 en ADR kunnen hierbij als gangbaar instrument in verschillende sectoren worden toegepast. Indien gewenst denken we vanuit SERN graag mee om dit artikel te implementeren.

Inzake DHM (*bekend om de unieke gestructureerde aanpak van beleid tot en met uitvoering inclusief kwaliteitsborging)* is het vermeldenswaardig dat dit voor SERN reden is geweest om DHM als aanvaarde opleiding te benoemen als vakbekwaamheidseis om naast de 3 jaar ervaringseis en werkzaam in een HBO physical security functie te kunnen worden opgenomen in het register RSE.

5. Artikel 22 Aanwijzing verbindingsfunctionaris

De kritieke entiteit wijst een verbindingsfunctionaris of een gelijkwaardige functionaris aan als het contactpunt met de bevoegde autoriteiten.

Hierbij overwegen om op te nemen aan welke physical security eisen (opleiding en ervaring e.d.) de verbindingsfunctionaris moet voldoen.

Aanvulling op artikel 22 Aanwijzing verbindingsfunctionaris

- **Voor wat betreft physical security opleidingseisen kan gedacht worden aan het volgende.**

De verbindingsfunctionaris moet inzake physical security tenminste het bezit van:

- een diploma op tenminste HBO niveau, of een tenminste gelijkwaardig niveau, op het vlak van beveiliging en
- minimaal vijf jaar gelijkwaardige werkervaring in een gelijksoortige werkomgeving.

Daarnaast, in het bezit van:

- een diploma van de post HBO Registeropleiding Security Management, zoals gecertificeerd door de Stichting Post HBO Nederland, of een diploma dat ten minste gelijkwaardig is aan laatstgenoemd diploma.
- een diploma van de post HBO Registeropleiding Security Techniek, zoals gecertificeerd door de Stichting Post HBO Nederland, of een diploma dat ten minste gelijkwaardig is aan laatstgenoemd diploma.

- een diploma van de post HBO Registeropleiding Security en Recht, zoals gecertificeerd door de Stichting Post HBO Nederland, of een diploma dat ten minste gelijkwaardig is aan laatstgenoemd diploma.

  De hierboven genoemde post HBO Registeropleidingen zijn door SERN als aanvaardbare physical security opleidingen benoemd om te kunnen worden opgenomen in een van haar physical security registers.

Als verbindingsfunctionaris kan de organisatie ook gebruik maken van tijdelijke inzet van deskundigen die aan bovenstaande eisen voldoen.

Met de hierboven genoemde beroepseisen / vakbekwaamheidseisen worden gelijkgesteld beroepseisen die worden gesteld in een andere lidstaat van de Europese Unie dan wel een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een daartoe strekkend of mede daartoe strekkend Verdrag dat Nederland bindt, en die een beroepsniveau waarborgen dat ten minste gelijkwaardig is aan het niveau dat met de nationale eisen wordt nagestreefd.

De Minister verklaart op verzoek van een kritieke entiteit of een diploma gelijkwaardig is.

6. Artikel 35 Audit

In bijlage 7: in artikel 35 wordt aangegeven waaraan de audit moet voldoen.

Voorstel ter aanvulling artikel 35

Hierbij in te brengen om het gedachtegoed van het Nederlands Securityvalidatie Instituut te institutionaliseren in een Stichting en daarbij de vakbekwaamheidseisen voor de onafhankelijke en gekwalificeerde deskundige benoemen zoals door SERN in haar registers opgenomen: Manager of Security (MSec) én Securityvalideur (Vsec).

Daarnaast adviseren we u te verduidelijken dat audits moeten voorzien in de kwaliteitsborging en kwaliteitsverbetering door aantoonbare verbeterprogramma's op te leveren.

Uiteraard heeft SERN hiermee de blik vooral intern gericht met gebruikmaking van haar eigen methodieken en instrumenten waaronder die van de security validatie, maar zijn we ons er terdege van bewust dat er ook andere inspectiebodies en beroepsgroepen die audits kunnen uitvoeren. Daarvoor adviseren wij deze audits minimaal door een ISO gecertificeerde deskundige te laten uitvoeren.

7. Tijdlijn

Als van de diverse genoemde datums deze worden uitgezet op een tijdlijn, dan gaat het wellicht met elkaar schuren.
Aanbeveling om de datums te heroverwegen

Artikel 7, lid 6:
De eerste aanwijzingen van entiteiten als kritieke entiteit geschieden uiterlijk op **17 juli 2026** en vervolgens telkens indien hiertoe naar het oordeel van de bevoegde autoriteit aanleiding bestaat.

Artikel 9, lid 5:
De eerste risicobeoordeling geschiedt uiterlijk op **17 januari 2026** en vervolgens ten minste elke vier jaar, of eerder indien hiertoe aanleiding bestaat. Dit kan dus 6 maanden zijn vóórdat de vakminister de entiteit als kritieke entiteit heeft aangewezen.

Artikel 13, lid 2:
Onze Minister stelt in overeenstemming met Onze Ministers die het aangaat de eerste strategie uiterlijk op **17 januari 2026** vast en actualiseert de strategie vervolgens ten minste om de vier jaar. Dit is dezelfde datum als dat de vakminister de entiteit als kritieke entiteit aanwijst. Zonder risicobeoordeling dus.

Artikel 14, lid 3:
De risicobeoordeling (door de kritieke entiteit) geschiedt binnen negen maanden na de aanwijzing als kritieke entiteit. Dit kan dus zijn uiterlijk op **17 oktober 2026**.

8. Niet in Wwke verwerkte CER overwegingen en CER artikelen
Er zijn een aantal overwegingen en artikelen uit de CER richtlijn niet opgenomen in de Wwke.
Hebben deze overwegingen dan na 17 oktober 2024 wel van kracht van werking?

9. Stroomlijnen van Wwke en Cbw in het kader van coherentie
Na aanwijzing als kritieke entiteit is dit bedrijf op grond van de Cbw een essentiële entiteit en moet het bestuur van dit bedrijf een security opleiding aantoonbaar met goed gevolg hebben afgerond.
Voorstel om deze opleidingseis ook in de Wwke op te nemen.
Voorts ook de bestuurdersverantwoordelijkheid in de Wwke opnemen zoals in de Cbw is vermeld.

10. Memorie van toelichting versus Wwke zelf
In de memorie van toelichting wordt bij 2.1 expliciet gesproken over fysiek beveiliging, maar in de wettekst zelf niet. Het verdient aanbeveling dit alsnog in te voegen.
Hetzelfde geldt voor dreiging c.q. risico's op het vlak van fysieke beveiliging.

11. Eenduidigheid in het benoemen beveiligingsmaatregelen
Er wordt op verschillende manieren uitdrukking gegeven aan de beveiligingsmaatregelen, te weten:
- OBE mix (Organisatorisch, Bouwkundig, Elektronisch)
- Technische, organisatorische en operationeel
- Passend en evenwichtig

Voorstel: een eenduidige keuze maken. Onze voorkeur: OBE-mix

12. Governance zoals bij Cbw in Wwke
Opnemen wat in de Cbw onder hoofdstuk 8 de Governance beschreven is maar dat een vergelijkbare omschrijving t.a.v. de fysieke dreigingen in de Wwke ontbreekt.
Voorstel om in de Wwke de Governance op een vergelijkbare wijze op te nemen.

==========

BIJLAGE 1

BIJLAGE 2

De genoemde AMvB's in de Wwke artikelen 3, 10, 14, 16, 18, 31a en 35

Artikel 3 (uitvoering uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren)
Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld ter uitvoering van de op grond van de CER-richtlijn vastgestelde uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren.

Artikel 10 (ondersteuning aan kritieke entiteiten)
1. De bevoegde autoriteit ondersteunt en werkt samen met kritieke entiteiten in de betrokken sector en subsector ten behoeve van het vergroten van hun weerbaarheid.

2. De in het eerste lid bedoelde samenwerking en ondersteuning bestaat in ieder geval uit het uitwisselen van informatie en beste praktijken, en kunnen na overleg met Onze Minister voorts bestaan uit:
a. het ontwikkelen van richtsnoeren en methodologieën;
b. het verlenen van bijstand in het geval van crisis- of noodsituaties;
c. het helpen bij de organisatie van oefeningen om de weerbaarheid van de kritieke entiteiten te testen;
d. het verstrekken van advies aan het personeel van kritieke entiteiten; en
e. het geven van opleidingen aan het personeel van kritieke entiteiten.

3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de in het tweede lid bedoelde ondersteuning en samenwerking.

Artikel 14 (risicobeoordeling door de kritieke entiteit)
1. De kritieke entiteit voert een risicobeoordeling uit op basis van de relevante informatie uit de risicobeoordeling van de bevoegde autoriteit, bedoeld in artikel 9, en andere relevante informatiebronnen. De kritieke entiteit beoordeelt in dat kader alle relevante door de natuur en door de mens veroorzaakte risico's die de verlening van haar essentiële dienst of diensten kunnen verstoren, waaronder in ieder geval:
a. risico's van sector overschrijdende of van grensoverschrijdende aard;
b. ongevallen;
c. natuurrampen;
d. noodsituaties op het gebied van volksgezondheid; en
e. hybride dreigingen en andere antagonistische dreigingen, waaronder terroristische misdrijven als bedoeld in Richtlijn (EU) 2017/541.

2. De kritieke entiteit houdt bij het uitvoeren van de risicobeoordeling rekening met de mate waarin andere in de bijlage van de wet genoemde sectoren afhankelijk zijn van de door de kritieke entiteit verleende essentiële dienst, en de mate waarin die kritieke entiteit afhankelijk is van essentiële diensten van andere entiteiten in dergelijke andere sectoren, in voorkomend geval tevens buiten Nederland.

3. De risicobeoordeling geschiedt binnen negen maanden na de aanwijzing als kritieke entiteit. De risicobeoordeling geschiedt vervolgens ten minste elke vier jaar of eerder, indien hiertoe aanleiding bestaat.

4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over de risicobeoordeling.

Artikel 16 (zorgplicht)
1. De kritieke entiteit neemt passende en evenredige technische, beveiligings-, en organisatorische maatregelen om voor haar weerbaarheid te zorgen. Dit doet zij op basis van de door de bevoegde autoriteit verstrekte relevante informatie over de risicobeoordeling, bedoeld in artikel 9, en op basis van de resultaten van de risicobeoordeling van de kritieke entiteit, bedoeld in artikel 14.

2. De kritieke entiteit beschrijft de in het eerste lid bedoelde maatregelen.

3. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de in het eerste lid bedoelde maatregelen, waarbij onderscheid kan worden gemaakt tussen sectoren en subsectoren en type entiteiten.

Artikel 18 (meldplicht)
1. De kritieke entiteit meldt een incident dat de verlening van haar essentiële dienst aanzienlijk verstoort of kan verstoren binnen 24 uur of, indien dat operationeel niet mogelijk is, zo snel mogelijk nadat zij kennis heeft genomen van dat incident bij de bevoegde autoriteit.

2. De melding bevat alle op dat moment beschikbare informatie die de bevoegde autoriteit nodig heeft om te bepalen wat de aard, vermoedelijke oorzaak en mogelijke gevolgen van het incident zijn en of er grensoverschrijdende gevolgen zijn. De melding bevat tevens de contactgegevens van de functionaris die verantwoordelijk is voor de melding.

3. Bij het bepalen of een verstoring aanzienlijk is, wordt in elk geval in aanmerking genomen:
a. het aantal door de verstoring getroffen gebruikers en hun aandeel daarin;
b. de duur van de verstoring;
c. het door de verstoring getroffen geografische gebied, rekening houdend met de vraag of het gebied geografisch geïsoleerd is.

4. De kritieke entiteit brengt binnen een maand na de melding een gedetailleerd verslag uit. Dit verslag bevat een aanvulling van de in het tweede lid bedoelde informatie.

5. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over de wijze waarop een melding als bedoeld in het eerste lid wordt gedaan, aanvullende aspecten en drempelwaarden die in aanmerking worden genomen om te bepalen of een verstoring aanzienlijk is, en de gegevens die ter uitvoering van het derde lid worden verstrekt.

Artikel 31a (bijzondere persoonsgegevens)
1. Gelet op artikel 9, aanhef en tweede lid, onderdeel g, van de Algemene verordening gegevensbescherming, is het verbod om bijzondere categorieën van persoonsgegevens, als bedoeld in artikel 1 van de Uitvoeringswet Algemene verordening gegevensbescherming, te verwerken niet van toepassing indien de verwerking geschiedt door de bevoegde autoriteit, voor zover de verwerking van deze gegevens noodzakelijk is voor de uitoefening van zijn bevoegdheden op grond van deze wet.

2. De bijzondere persoonsgegevens bedoeld in het eerste lid worden niet langer bewaard dan voor de uitoefening van de taken van de bevoegde autoriteit noodzakelijk is. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de verwerking van bijzondere persoonsgegevens.

Artikel 35 (audit)
1. De bevoegde autoriteit kan een kritieke entiteit verplichten om:
a. een onafhankelijke en gekwalificeerde deskundige te laten onderzoeken of de entiteit voldoet aan het bepaalde bij of krachtens deze wet, met uitzondering van artikel 25, tweede lid; of
b. de resultaten van dat onderzoek binnen een bij het besluit gestelde redelijke termijn te verstrekken aan de bevoegde autoriteit.

2. Het onderzoek wordt uitgevoerd op een door de bevoegde autoriteit voorgeschreven wijze.

3. De kritieke entiteit draagt de kosten van het onderzoek, tenzij een bij algemene maatregel van bestuur omschreven geval zich voordoet waarin de betrokken entiteit deze kosten niet hoeft te dragen.

4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het eerste en tweede lid.

BIJLAGE 3

In Cbw staat bij artikel 8.1.i

Artikel 8 (essentiële entiteit van rechtswege)

1. De volgende entiteiten zijn essentiële entiteiten:
a. gekwalificeerde aanbieders van vertrouwensdiensten;
b. aanbieders van registers voor topleveldomeinnamen;
c. DNS-dienstverleners;
d. aanbieders van openbare elektronische communicatienetwerken, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG;
e. aanbieders van openbare elektronische communicatiediensten, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG;
f. andere entiteiten, genoemd in bijlage 1 van deze wet, die de in artikel 2, eerste lid, van de bijlage bij Aanbeveling 2003/361/EG bedoelde drempel voor middelgrote ondernemingen overschrijden;
g. de ministeries met inbegrip van de daartoe behorende dienstonderdelen, onverminderd het bepaalde in artikel 6, en zelfstandige bestuursorganen van de centrale overheid, voor zover deze zelfstandige bestuursorganen kwalificeren als overheidsinstantie;
h. provincies, gemeenten en waterschappen, alsmede gemeenschappelijke regelingen voor zover deze laatste kwalificeren als entiteit van het in bijlage 1 of 2 van de NIS2-richtlijn bedoelde soort en als overheidsinstantie;
i. kritieke entiteiten als bedoeld in artikel 7 van de Wet weerbaarheid kritieke entiteiten.

BIJLAGE 4

De opsomming bij artikel 21 lid 2 van de NIS2

2. De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende:

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b) incidentenbehandeling;
c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

BIJLAGE 5

Voor een betere duiding zijn de Cbw artikelen op rij geplaatst

Hoofdstuk 1. Begripsbepaling
Artikel 1 (begripsbepaling)
Hoofdstuk 2. Algemeen
Artikel 2 (doel van deze wet)
Artikel 3 (uitvoering uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren)
Hoofdstuk 3. Toepassingsbereik
Artikel 4 (jurisdictie en territorialiteit)
Artikel 4a (toepasselijkheid op sector, subsector of type entiteit Wwke)
Artikel 5 (Nederlandse exclusieve economische zone)
Artikel 6 (overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving)
Artikel 7 (instellingen uitgezonderd van Verordening 2022/2554)
Hoofdstuk 4. Essentiële entiteiten en belangrijke entiteiten
§ 4.1 Essentiële entiteiten
Artikel 8 (essentiële entiteit van rechtswege)
Artikel 9 (essentiële entiteit op basis van criteria)
Artikel 10 (essentiële entiteit die aanbieder van een essentiële dienst was)
Artikel 11 (essentiële entiteit na aanwijzing)
§ 4.2 Belangrijke entiteiten
Artikel 12 (belangrijke entiteit van rechtswege)
Artikel 13 (belangrijke entiteit op basis van criteria)
Artikel 14 (belangrijke entiteit na aanwijzing)
Hoofdstuk 5. Aanwijzing en taken van instanties
Artikel 15 (aanwijzing en taken centrale contactpunt)
Artikel 16 (aanwijzing en taken bevoegde autoriteit)
Artikel 17 (aanwijzing en taken CSIRT)
Artikel 18 (aanwijzing en taken coördinator bekendmaking kwetsbaarheden)
Artikel 19 (aanwijzing en taken cybercrisisbeheerautoriteit)
Artikel 19 (aanwijzing en taken cybercrisisbeheerautoriteit)
Hoofdstuk 6. Taken van Onze Minister
Artikel 20 (nationale cyberbeveiligingsstrategie)
Artikel 21 (nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons)
Artikel 22 (nationaal register van entiteiten)
Hoofdstuk 7. Zorgplicht
Artikel 23 (zorgplicht)
Artikel 24 (sectorspecifieke rechtshandelingen)
Artikel 25 (ontheffing zorgplicht)
Hoofdstuk 8. Governance
Artikel 26 (governance)
Hoofdstuk 9. Significante incidenten, incidenten, bijna-incidenten, significante cyberdreigingen, cyberdreigingen en kwetsbaarheden
§ 9.1 Meldplicht
Artikel 27 (meldplicht significante incidenten)
Artikel 28 (vroegtijdige waarschuwing)
Artikel 29 (melding, update en initiële beoordeling)
Artikel 30 (tussentijds verslag)
Artikel 31 (voortgangsverslag en eindverslag)
§ 9.2 Informeren van ontvangers van diensten
Artikel 32 (informeren van ontvangers van diensten)
§ 9.3 Sectorspecifieke rechtshandelingen en vrijstelling
Artikel 33 (sectorspecifieke rechtshandelingen)
Artikel 34 (ontheffing meldplicht)
§ 9.4 Vrijwillige meldingen
Artikel 35 (vrijwillige meldingen van significante incidenten, incidenten, bijna-incidenten en cyberdreigingen)
Artikel 36 (vrijwillige meldingen van kwetsbaarheden)
§ 9.5 Nadere regels
Artikel 37 (nadere regels over meldingen van significante incidenten)
§ 9.6 Taken en bevoegdheden van het CSIRT en de bevoegde autoriteit bij significante incidenten en significante cyberdreigingen
Artikel 38 (taken CSIRT na melding significant incident)
Artikel 39 (openbaarmaking significant incident door CSIRT of bevoegde autoriteit)

BIJLAGE 6

In artikel 10 wordt aangegeven het ontwikkelen van richtsnoeren en methodologieën zie bijlage 6

Artikel 10 (ondersteuning aan kritieke entiteiten)
1. De bevoegde autoriteit ondersteunt en werkt samen met kritieke entiteiten in de betrokken sector en subsector ten behoeve van het vergroten van hun weerbaarheid.
2. De in het eerste lid bedoelde samenwerking en ondersteuning bestaat in ieder geval uit het uitwisselen van informatie en beste praktijken, en kunnen na overleg met Onze Minister voorts bestaan uit:
a. het ontwikkelen van richtsnoeren en methodologieën;
b. het verlenen van bijstand in het geval van crisis- of noodsituaties;
c. het helpen bij de organisatie van oefeningen om de weerbaarheid van de kritieke entiteiten te testen;
d. het verstrekken van advies aan het personeel van kritieke entiteiten; en
e. het geven van opleidingen aan het personeel van kritieke entiteiten.
3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de in het tweede lid bedoelde ondersteuning en samenwerking.

BIJLAGE 7

Artikel 35 (audit)

1. De bevoegde autoriteit kan een kritieke entiteit verplichten om:
a. een onafhankelijke en gekwalificeerde deskundige te laten onderzoeken of de entiteit voldoet aan het bepaalde bij of krachtens deze wet, met uitzondering van artikel 25, tweede lid; of
b. de resultaten van dat onderzoek binnen een bij het besluit gestelde redelijke termijn te verstrekken aan de bevoegde autoriteit.

2. Het onderzoek wordt uitgevoerd op een door de bevoegde autoriteit voorgeschreven wijze.

3. De kritieke entiteit draagt de kosten van het onderzoek, tenzij een bij algemene maatregel van bestuur omschreven geval zich voordoet waarin de betrokken entiteit deze kosten niet hoeft te dragen.

4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het eerste en tweede lid.