Waterschap Rijn en IJssel
Ingekomen
10 SEP. 2026

Ministerie van Infrastructuur en Waterstaat

beschikking

DG Water en Bodem
Dir. Waterveiligheid, Rivieren en Zee

Contactpersoon
T. Nguyen
Team Coördinator
M 06 52485802
thy.nguyen@minienw.nl

Datum
8 september 2026

Bijlagen
- Wet weerbaarheid kritieke entiteiten - Handreiking voor kritieke entiteiten
- Cyberbeveiligingswet - Informatiebrochure.

Datum	8 september 2026
Nummer	IENW/BSK-2026/171648
Betreft	aanwijzing als kritieke entiteit

Aan: Waterschap Rijn en Ijssel
Ter attentie van drs. H.Th.M. Pieper
Adres: Postbus 148, 7000 AC Doetinchem

Geachte meneer Pieper,

Hierbij informeer ik u dat ik uw organisatie aanwijs als kritieke entiteit als bedoeld in de Wet weerbaarheid kritieke entiteiten. Uw organisatie is bij brief van 6 juli 2026 geïnformeerd over het voornemen uw organisatie aan te wijzen. Uw organisatie heeft daarop geen zienswijze ingediend.

Uw organisatie is:
Waterschap Rijn en Ijssel
KvK-nummer: 9212548

Aanwijzing als kritieke entiteit
Uw organisatie is met ingang van 14 september 2026 aangewezen als kritieke entiteit in de sector Keren en Beheren van Waterkwantiteit en de sector Afvalwater. De Wet weerbaarheid kritieke entiteiten (hierna: Wwke) bepaalt dat kritieke entiteiten worden aangewezen als deze organisaties voldoen aan de in die wet opgenomen criteria.[1] De aanwijzing van uw organisatie als kritieke entiteit in deze sectoren is naar aanleiding van de specifieke rol die zij vervult in het leveren van een essentiële dienst volgens de Wwke en de Regeling weerbaarheid kritieke entiteiten IenW (Rwke)[2].

In de sector Keren en Beheren Waterkwantiteit biedt uw organisatie de volgende essentiële dienst aan: het keren en beheren van de waterkwantiteit.

In de sector Afvalwater biedt uw organisatie de volgende essentiële dienst aan: het behandelen en lozen van stedelijk, huishoudelijk en industrieel afvalwater.

Uw organisatie is verder actief op Nederlands grondgebied en heeft op dat grondgebied kritieke infrastructuur.

Hieronder wordt per sector verder uitgewerkt of een incident bij uw organisatie een aanzienlijk verstorend effect heeft, volgens de definitie van de Wwke.

[1] Artikel 6 van de Wwke.
[2] Essentiële diensten zijn diensten die zijn opgenomen in de bijlage bij de Wwke of genoemd in artikel 3 van de Regeling weerbaarheid kritieke entiteiten (Rwke)

Afvalwater
Voor de beoordeling of een incident bij uw organisatie een aanzienlijk verstorend effect heeft, heb ik in Q3 2025 een vitaalbeoordeling uitgevoerd als onderdeel van de Aanpak Vitaal. Deze aanpak wordt grotendeels vervangen met de inwerkingtreding van de Wet weerbaarheid kritieke entiteiten. Uit deze beoordeling blijkt dat een incident bij uw organisatie een aanzienlijk verstorend effect heeft als bedoeld in de Wwke.[3]

Ik kom tot dat oordeel op grond van:

a. Het aantal gebruikers dat afhankelijk is van de verleende dienst;
b. De mate waarin andere sectoren afhankelijk zijn van de verleende dienst
c. De ernst en duur van de gevolgen van incidenten voor economische en maatschappelijke activiteiten, het milieu, de openbare veiligheid en beveiliging of de volksgezondheid.
d. Het marktaandeel;
e. Het belang van de essentiële dienst en eventuele alternatieven.

Bij de vitaalbeoordeling is de methodiek van de NCTV gebruikt. Deze methodiek kijkt naar de fysieke, economische, maatschappelijke, ecologische schade als gevolg van een aantal worst-case scenario's, waaronder grootschalige elektriciteitsuitval, alsmede de gevolgen van dit scenario voor de territoriale veiligheid, internationale rechtsorde en de cascade-effecten voor andere sectoren.

Uw organisatie scoort als volgt:
Ad a. Aantal gebruikers: Hoog
De 21 waterschappen nemen gezamenlijk de reiniging voor het gros van het stedelijk afvalwater in Nederland voor hun rekening. Dit betekent dat een groot aantal gebruikers afhankelijk is van de dienst die uw waterschap levert voor het zuiveren en lozen van hun afvalwater. Dit wordt versterkt door het feit dat sommige individuele Rioolwaterzuiveringsinstallaties (RWZI) op zichzelf al een groot aantal gebruikers bedienen.

Ad b. Afhankelijkheid: Hoog
Tijdens het uitwerken van de scenario's gaven andere kritieke entiteiten aan dat hun essentiële dienst afhankelijk is van de afvalwater diensten van uw organisatie. Specifiek, een incident in de afvalwaterverwerking bij uw organisatie zou verstoringen kunnen veroorzaken voor kritieke entiteiten in de sectoren Chemie, Elektriciteit, Drinkwater en Scheepvaartafwikkeling. Bij een verstoring van de essentiële zuiveringsdienst die uw waterschap levert waarbij de RWZI tijdelijk stopt of ongezuiverd afvalwater geloosd wordt op oppervlaktewater zou dit kunnen betekenen dat deze andere kritieke entiteiten geen gebruik meer kunnen maken van dit water en/of hun productieproces moeten staken. Dit zou kunnen leiden tot een verstoring in hun mogelijkheid om hun essentiële dienst te leveren.

Ad c. Ernst en duur van incident: Hoog
In één of meer scenario's komt naar voren dat een verstoring bij uw organisatie de volgende gevolgen zouden kunnen hebben:

- Ecologische schade: >3% van Natura 2000 gebieden of NNN gebied wordt >10 jaar aangetast en/of een gebied van >30 km2 wordt >10 jaar aangetast.

[3] Als bedoeld in artikel 6, eerste lid, onderdeel d, van de Wwke.

- Economische schade: >5 miljard euro als cumulatieve kosten van het herstellen van ecologische schade en de gederfde omzet van kritieke bedrijven door het stilzetten van hun productieproces door het uitvallen van de afvalwaterzuivering bij de RWZI.

Ad d. uw marktaandeel: Hoog
Als decentrale overheid met de wettelijke taak voor het zuiveren en lozen van stedelijke afvalwater hebben waterschappen vrijwel een monopolie in hun leveringsgebied op de infrastructuur om deze taken uit te voeren.[4] Uw marktaandeel voor deze dienst in uw zuiveringskringen is dan ook bijna 100%, en alle eindgebruikers (burgers en veelal bedrijven) zijn volledig afhankelijk van deze infrastructuur.

Ad e. Belang van essentiële dienst en alternatieven: Hoog
Door bovengenoemd wettelijk monopolie is er geen alternatief voor de dienst die uw waterschap levert in uw verantwoordelijke leveringsgebied. Het is mogelijk dat specifieke zuiveringskringen onder uw beheer verbindingen hebben met andere zuiveringskringen, en dat in het geval van een incident de afvoer en zuivering van afvalwater (deels) voortgang kan vinden. Echter, deze onderlinge verbindingen zijn een uitzondering. Er is (normaliter) dus geen alternatieve infrastructuur aanwezig waarop burgers hun lozingen kunnen doen wanneer de RWZI niet operationeel is. Er zijn derhalve geen reële alternatieven voor de zuiveringskring en in de meeste gevallen zijn gebruikers afhankelijk van de geleverde dienst van het waterschap.

Keren en Beheren
In 2021 is een herbeoordeling uitgevoerd van de eerdere vitaalbeoordeling van de sector Keren en Beheren Waterkwantiteit. Hierbij is gekeken of een incident bij uw organisatie een aanzienlijk verstorend effect heeft. De conclusies volgend uit deze herbeoordeling zijn ter kennisname voorgelegd tijdens het Bestuurlijk Overleg Water van 12 april 2023. De herbeoordeling is gedaan als onderdeel van de Aanpak Vitaal. Deze aanpak zal grotendeels worden vervangen door de Wwke bij de inwerkingtreding. Uit deze beoordeling blijkt dat een incident bij uw organisatie een aanzienlijk verstorend effect heeft als bedoeld in de Wwke.[5]

Ik kom tot dat oordeel op grond van:
a. Het aantal gebruikers dat afhankelijk is van de verleende dienst;
b. De mate waarin andere sectoren afhankelijk zijn van de verleende dienst
c. De ernst en duur van de gevolgen van incidenten voor economische en maatschappelijke activiteiten, het milieu, de openbare veiligheid en beveiliging of de volksgezondheid.
d. Het marktaandeel;
e. Het belang van de essentiële dienst en eventuele alternatieven.

Bij de herbeoordeling en eerdere vitaalbeoordeling van de sector Keren en Beheren Waterkwantiteit is dezelfde methodiek van de NCTV gebruikt als bij de sector Afvalwater.

[4] Dit geldt voor bijna al het huishoudelijk afvalwater en een deel van het industrieel afvalwater. Enkel het afvalwater dat behandeld wordt door specifieke bedrijven in hun eigen afvalwaterzuiveringsinstallaties of door een handvol wijken in hun eigen decentrale afvalwaterzuivering valt hier niet onder.
[5] Als bedoeld in artikel 6, eerste lid, onderdeel d, van de Wwke.

Uw organisatie scoort als volgt:
Ad a. Aantal gebruikers: Hoog
De 21 waterschappen zijn gezamenlijk primair verantwoordelijk voor de continuïteit en weerbaarheid van een aanzienlijk deel van de Nederlandse waterkerende en waterbeherende infrastructuur. In Nederland wonen 9 miljoen mensen in gebieden die gevoelig zijn voor overstromingen. Zonder uw diensten zouden deze gebieden kunnen overstromen. Dit betekent dat een groot aantal inwoners van Nederland in zeer hoge mate afhankelijk is van de door u geleverde diensten.

Ad b. Afhankelijkheid: Hoog
De sector keren en beheren heeft in hoge mate effect op andere sectoren. Falen van waterkerende en -beherende infrastructuur kan cascade-effecten veroorzaken met gevolgen voor een groot aantal andere processen. Andere infrastructuur is dus in hoge mate afhankelijk van de door u geleverde diensten. Enkele voorstelbare voorbeelden van gevolgen bij falen zijn:

- Drinkwatervoorziening: bij grote overstromingen moeten drinkwaterbedrijven hun productie (tijdelijk) staken. Dit kan leiden tot tekorten, ook in niet overstroomde gebieden die geëvacueerde personen opvangen.
- Transport over de weg en het spoor: bij overstromingen kunnen vervoer over (hoofd)wegennet en (hoofd)spoorwegennet stil komen te liggen. Dit kan bijvoorbeeld gebeuren door het onderlopen van tunnels en het verzakken van (spoor)wegen.
- Transport door de lucht: bij overstromingen kunnen start- en landingsbanen onder water komen te staan. Hierdoor is vliegverkeer niet langer mogelijk.

Ad c. Ernst en duur van incident: Hoog
In een of meer scenario's komt naar voren dat een verstoring bij uw organisatie de volgende gevolgen zouden kunnen hebben:

- Economische schade: afhankelijk van de aard en locatie van het falen betreft dit tientallen miljoenen tot tientallen miljarden Euro's schade.
- Fysieke schade: afhankelijk van de aard en locatie van het falen betreft dit enkele tot duizenden (dodelijke) slachtoffers en vele malen zovelen getroffenen.
- Maatschappelijke schade: afhankelijk van de aard en locatie van het falen betreft dit grote provincie overstijgende sociaal-maatschappelijke schade die meer dan 1 miljoen personen kan raken.

Ad d. Uw marktaandeel: Hoog
De waterschappen hebben een monopolie binnen hun eigen werkgebied. Uw marktaandeel voor het keren en beheren van water in het werkgebied van uw waterschap is dan ook 100%. Alle eindgebruikers (burgers en veelal bedrijven) zijn volledig afhankelijk van de door u geleverde dienst.

Ad e. Belang van essentiële dienst en alternatieven: Hoog
De door uw Waterschap geleverde essentiële diensten op het gebied van het keren en beheren van water zijn uniek en alternatieve, door andere partijen geleverde, voorzieningen in het bediende geografisch gebied zijn niet voorhanden. Gebruikers zijn daardoor afhankelijk van de geleverde dienst van uw Waterschap.

Relevante informatie uit sectorale risicobeoordeling

Het ministerie van Infrastructuur en Waterstaat voert momenteel een sectorale risicobeoordeling uit in de sectoren Afvalwater en Keren en Beheren. Deze sectorale risicobeoordeling bevat mogelijk voor uw organisatie relevante informatie en kan als input dienen voor de entiteit-specifieke risicobeoordeling die u als kritieke entiteit opstelt. Deze informatie wordt zodra deze beschikbaar is met u gedeeld op basis van vertrouwelijkheid.

Rechten en plichten
Op https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur en op www.versterkenweerbaarheid.nl kunt u voor u relevante informatie vinden. Ook is bij deze beschikking gevoegd de handreiking 'Wet weerbaarheid kritieke entiteiten – Handreiking voor kritieke entiteiten'. In deze handreiking staat informatie over de Wwke en de rechten en plichten die voortvloeien uit de Wwke.

Via www.wetten.nl kunt u de regelgeving raadplegen. Het gaat om:
- Wet weerbaarheid kritieke entiteiten;
- Besluit weerbaarheid kritieke entiteiten;
- Regeling weerbaarheid kritieke entiteiten IenW.

Contact
Uw organisatie heeft als contactpersoon dhr. Alexander Mastenbroek (alexander.mastenbroek@minienw.nl), Senior Beleidsmedewerker Cyber & Vitaal, Afdeling Waterveiligheid, Directie Waterveiligheid, Rivieren en Zee, Directoraat-Generaal Water en Bodem.

Bezwaarclausule
Als u het niet eens bent met dit besluit, kunt u daartegen binnen zes weken na de verzenddatum van deze brief een bezwaarschrift indienen. Het bezwaarschrift kunt u sturen naar: Minister van Infrastructuur en Waterstaat, ter attentie van Hoofddirectie Bestuurlijke en Juridische Zaken, afdeling Algemeen Bestuurlijk-Juridische Zaken, postbus 20901, 2500 EX Den Haag.

Als u uw bezwaarschrift te laat indient, kan dit in de meeste gevallen niet meer in behandeling worden genomen.

Uw bezwaarschrift moet in ieder geval de volgende gegevens bevatten:
- uw naam en adres;
- de datum waarop u het bezwaarschrift schrijft;
- een omschrijving en het kenmerk van het besluit waar het bezwaar tegen is gericht;
- de reden waarom u het er niet mee eens bent;
- uw handtekening.

Hoogachtend,

DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT,

Namens deze,
Directeur-Generaal Water en Bodem,

Drs. J.H. Slootmaker

N Network

I Information

S Security

Cyberbeveiligingswet

Informatiebrochure

augustus 2026

Inleiding

Veel van ons leven en werk speelt zich af in de digitale wereld. Omdat de digitale veiligheid van onze samenleving en economie steeds vaker onder druk staat, heeft de Europese Unie (EU) de NIS2-richtlijn vastgesteld. Deze richtlijn is de opvolger van de NIS1-richtlijn. De NIS2-richtlijn heeft tot doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de EU te bereiken. In Nederland is de NIS2-richtlijn geïmplementeerd in de Cyberbeveiligingswet. Met de inwerkingtreding van de Cyberbeveiligingswet is de Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangen. Tegelijkertijd is ook de Critical Entities Resilience Directive (CER-richtlijn) geïmplementeerd in de Wet weerbaarheid kritieke entiteiten (Wwke). Beide wetten zijn op 15 augustus 2026 in werking getreden.

De Cyberbeveiligingswet heeft gevolgen voor organisaties die onder de wet vallen. Daarbij gaat het om veel meer organisaties dan voorheen onder de Wbni vielen. Voor organisaties die onder de Cyberbeveiligingswet vallen, gelden onder meer een registratieplicht, zorgplicht, meldplicht en bestuurlijke verantwoordelijkheid. Ook is het toezicht op de naleving van deze verplichtingen ingericht.

Wat zijn de belangrijkste onderdelen van de Cyberbeveiligingswet?



Disclaimer

Deze informatiebrochure bevat basisinformatie over de Cyberbeveiligingswet. Aan de inhoud van deze informatiebrochure kunnen geen rechten worden ontleend. Deze informatiebrochure is niet juridisch bindend. Organisaties zijn zelf verantwoordelijk voor het voldoen aan de eisen in de Cyberbeveiligingswet. Deze informatiebrochure is voor het laatst geactualiseerd in augustus 2026 en wordt indien nodig hierna opnieuw geactualiseerd.

Inhoud

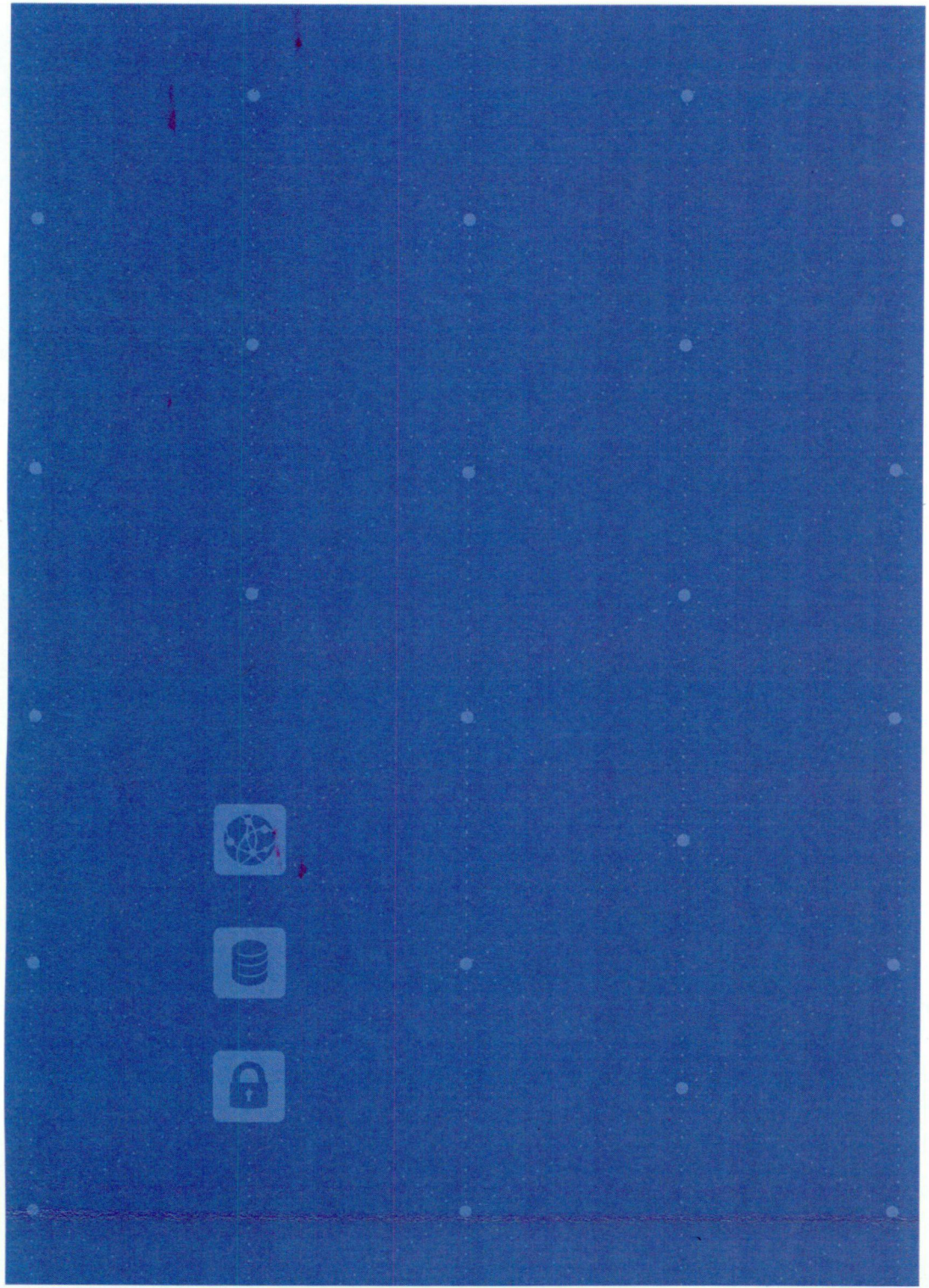
Inleiding 2

1. Valt jouw organisatie onder de Cyberbeveiligingswet? 4

2. Wat betekent de Cyberbeveiligingswet voor jouw organisatie? 11

3. Wat kunnen organisaties van de Rijksoverheid verwachten? 16

4. Meer weten? 19



1.

Valt jouw organisatie onder de Cyberbeveiligingswet?

Valt jouw organisatie onder de Cyberbeveiligingswet?

Veel organisaties vallen van rechtswege onder de Cyberbeveiligingswet. Organisaties zijn zelf verantwoordelijk om te bepalen of zij onder deze wet vallen.

Zelfevaluatietool

Organisaties kunnen met de zelfevaluatietool beoordelen of ze onder de Cyberbeveiligingswet vallen en, indien dat het geval is, of zij kwalificeren als essentiële entiteit of belangrijke entiteit. Daarnaast kunnen onderstaande stappen worden doorlopen om te bepalen of een organisatie onder de Cyberbeveiligingswet valt.

Stap 1: Controleer of jouw organisatie behoort tot een van onderstaande sectoren

De Cyberbeveiligingswet is van toepassing op de onderstaande sectoren. Zie bijlage 1 en 2 van de Cyberbeveiligingswet voor een gedetailleerd overzicht van deze sectoren en daaronder vallende soorten entiteiten.

Organisaties die domeinnaamregistratiediensten verlenen staan niet vermeld in bijlage 1 of 2 van de Cyberbeveiligingswet. Op deze organisaties zijn niet alle verplichtingen uit de Cyberbeveiligingswet van toepassing.



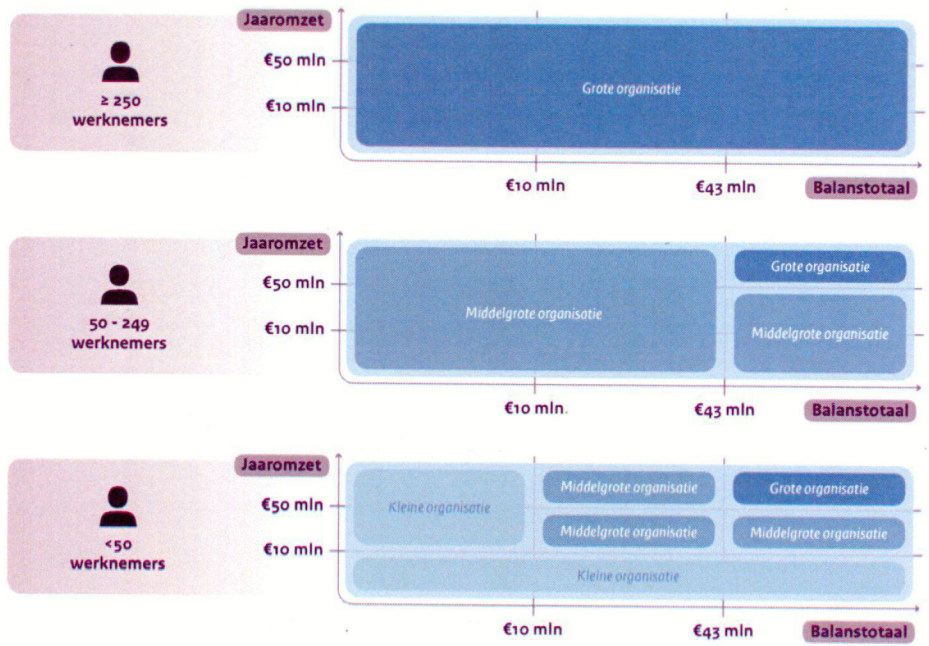
Stap 2: Controleer of jouw organisatie voldoet aan de omvangscriteria

Nadat is vastgesteld dat jouw organisatie behoort tot een soort entiteit die is opgenomen in bijlage 1 of bijlage 2 van de Cyberbeveiligingswet, moet worden beoordeeld of wordt voldaan aan de omvangscriteria. Daarbij wordt onder meer gekeken naar het aantal medewerkers, de jaaromzet en het balanstotaal.

Voor sommige organisaties gelden deze omvangscriteria niet. Zij vallen onder de Cyberbeveiligingswet, ongeacht hun omvang. Dit geldt voor: aanbieders van openbare elektronische communicatienetwerken, aanbieders van openbare elektronische communicatiediensten, (gekwalificeerde) verleners van vertrouwensdiensten, aanbieders van registers voor topleveldomeinnamen, DNS-dienstverleners en overheidsorganisaties, en voor verleners van domeinnaamregistratiediensten.

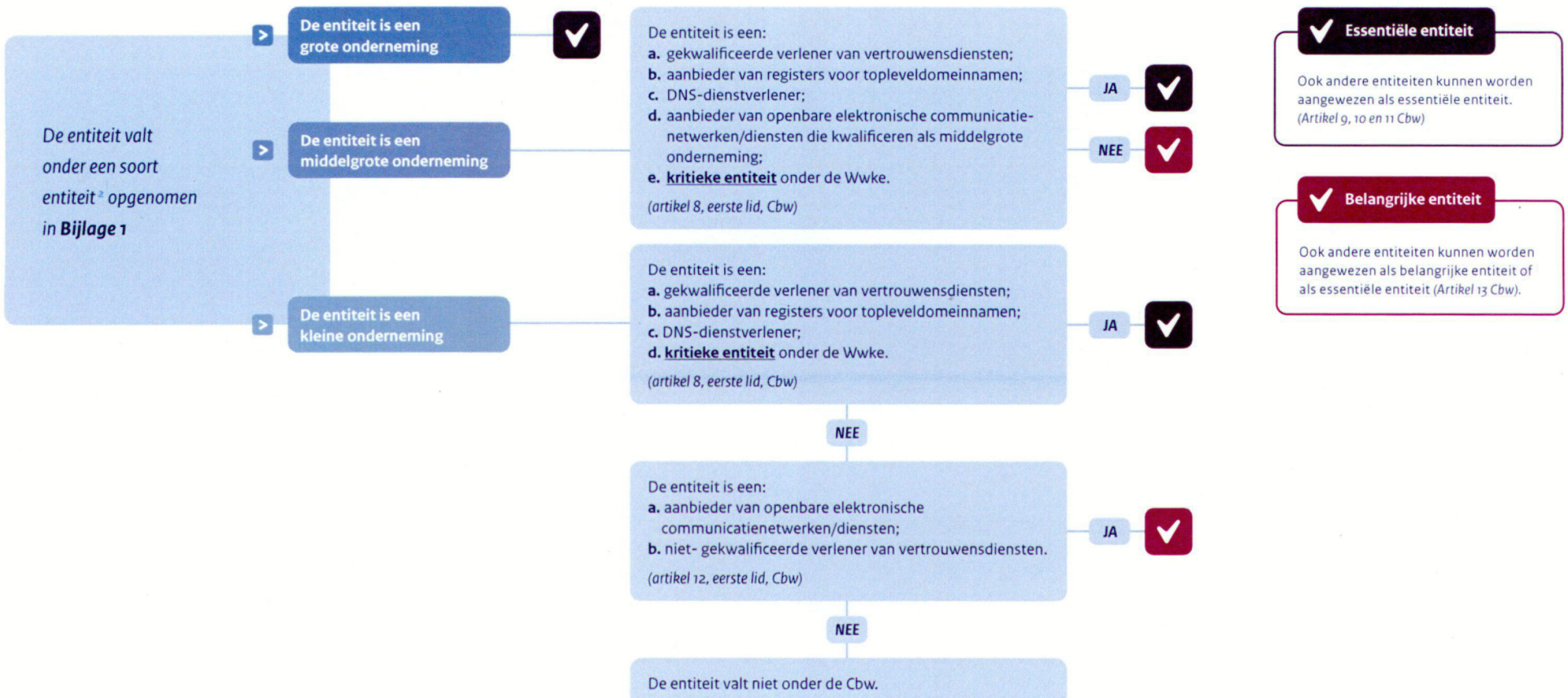
Stap 3: Bepaal aan de hand van het stroomschema of jouw organisatie een essentiële entiteit óf een belangrijke entiteit is

Wanneer duidelijk is dat jouw organisatie onder bijlage 1 of bijlage 2 van de Cyberbeveiligingswet valt én wat de omvang van jouw organisatie is, kan met behulp van de stroomschema's worden bepaald of er sprake is van een essentiële entiteit óf een belangrijke entiteit. Dit onderscheid is belangrijk, omdat het invloed heeft op de manier waarop toezicht wordt gehouden:



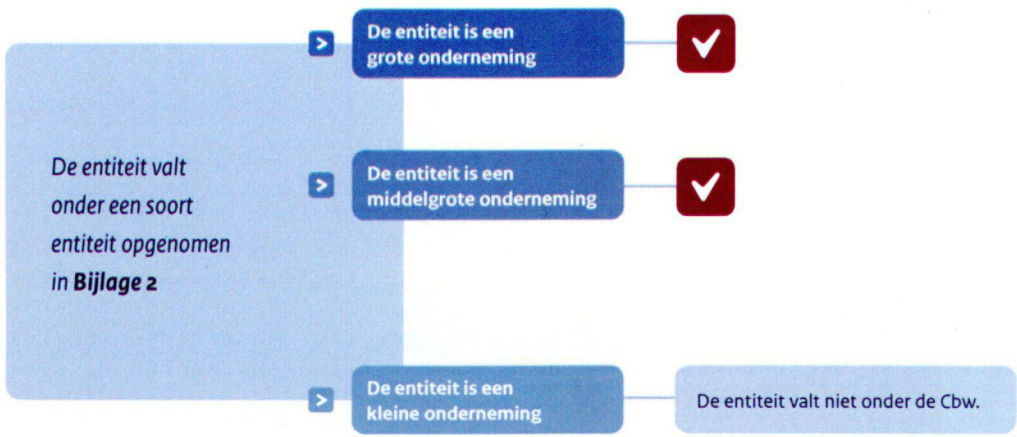
- **Essentiële entiteiten staan onder proactief toezicht:** de naleving van verplichtigen wordt actief gecontroleerd, ook als er geen aanwijzingen voor een mogelijke overtreding zijn.
- **Belangrijke entiteiten vallen onder reactief toezicht:** controles vinden achteraf plaats, naar aanleiding van bijvoorbeeld aanwijzingen of informatie over een mogelijke overtreding. Zoals in het stroomschema op de volgende pagina te zien is, zijn ook hier enkele uitzonderingen van toepassing.

Stroomschema: entiteit valt onder Bijlage 1 van de Cyberbeveiligingswet



2 Soort entiteit: een organisatie valt onder Bijlage 1 en/of Bijlage 2 als deze behoort tot een soort entiteit binnen een (sub)sector genoemd in de bijlagen. Bijvoorbeeld: als de organisatie actief is binnen de sector energie, in de subsector elektriciteit én als soort entiteit een elektriciteitsbedrijf is, valt de organisatie onder Bijlage 1.

Stroomschema: entiteit valt onder Bijlage 2 van de Cyberbeveiligingswet



Belangrijke entiteit

Ook andere entiteiten kunnen worden aangewezen als belangrijke entiteit of als essentiële entiteit *(Artikel 13 Cbw)*.

Let op

Voor sommige soorten organisaties gelden uitzonderingen op de hoofdregels. Dit geldt bijvoorbeeld voor overheidsinstanties, bekostigde hogescholen en universiteiten, aanbieders van elektronische communicatienetwerken en bepaalde digitale dienstverleners. In onderstaande paragrafen worden deze uitzonderingen toegelicht.

Essentiële entiteiten

Grote organisaties die behoren tot een van de sectoren, genoemd in bijlage 1 van de Cyberbeveiligingswet, kwalificeren als essentiële entiteit. De volgende organisaties kwalificeren, ongeacht hun omvang, als essentiële entiteit onder de Cyberbeveiligingswet: centrale en decentrale overheden (zie hieronder voor een nadere toelichting), gekwalificeerde vertrouwensdienstverleners, aanbieders van registers voor topleveldomeinnamen en verleners van DNS-diensten. Ook aanbieders van openbare elektronische communicatienetwerken of -diensten, die middelgroot zijn, zijn essentiële entiteiten.

Belangrijke entiteiten

Middelgrote organisaties die behoren tot een van de sectoren, genoemd in bijlage 1 van de Cyberbeveiligingswet (en niet op grond van het bovenstaande kwalificeren als essentiële entiteit) kwalificeren als belangrijke entiteit. Ook middelgrote en grote organisaties, die behoren tot een van de genoemde sectoren, genoemd in bijlage 2 van de Cyberbeveiligingswet, kwalificeren als belangrijke entiteit. Ook aanbieders van openbare elektronische communicatienetwerken of -diensten en verleners van vertrouwensdiensten die een kleine of micro-organisatie zijn, kwalificeren als belangrijke entiteit.

Relatie met de Wet weerbaarheid kritieke entiteiten

Organisaties die door de vakminister worden aangewezen als kritieke entiteit op grond van de Wet weerbaarheid kritieke entiteiten, kwalificeren van rechtswege als essentiële entiteit onder de Cyberbeveiligingswet. Voor deze organisaties gelden daarom ook de verplichtingen uit de Cyberbeveiligingswet, zoals de registratie-, zorg- en meldplicht.

Overheidsinstanties

Binnen de overheid vallen verschillende organisaties onder de Cyberbeveiligingswet als essentiële entiteit. Het gaat onder meer om ministeries (inclusief daaronder behorende dienstonderdelen), zelfstandige bestuursorganen die als overheidsinstantie kwalificeren, provincies, gemeenten, waterschappen en organisaties die zijn opgericht op grond van de Wet gemeenschappelijke regelingen.

Voor deze organisaties gelden geen omvangscriteria: ook kleinere organisaties kunnen onder de Cyberbeveiligingswet vallen. Wel moeten zij voldoen aan de definitie van overheidsinstantie zoals opgenomen in artikel 1 van de Cyberbeveiligingswet.

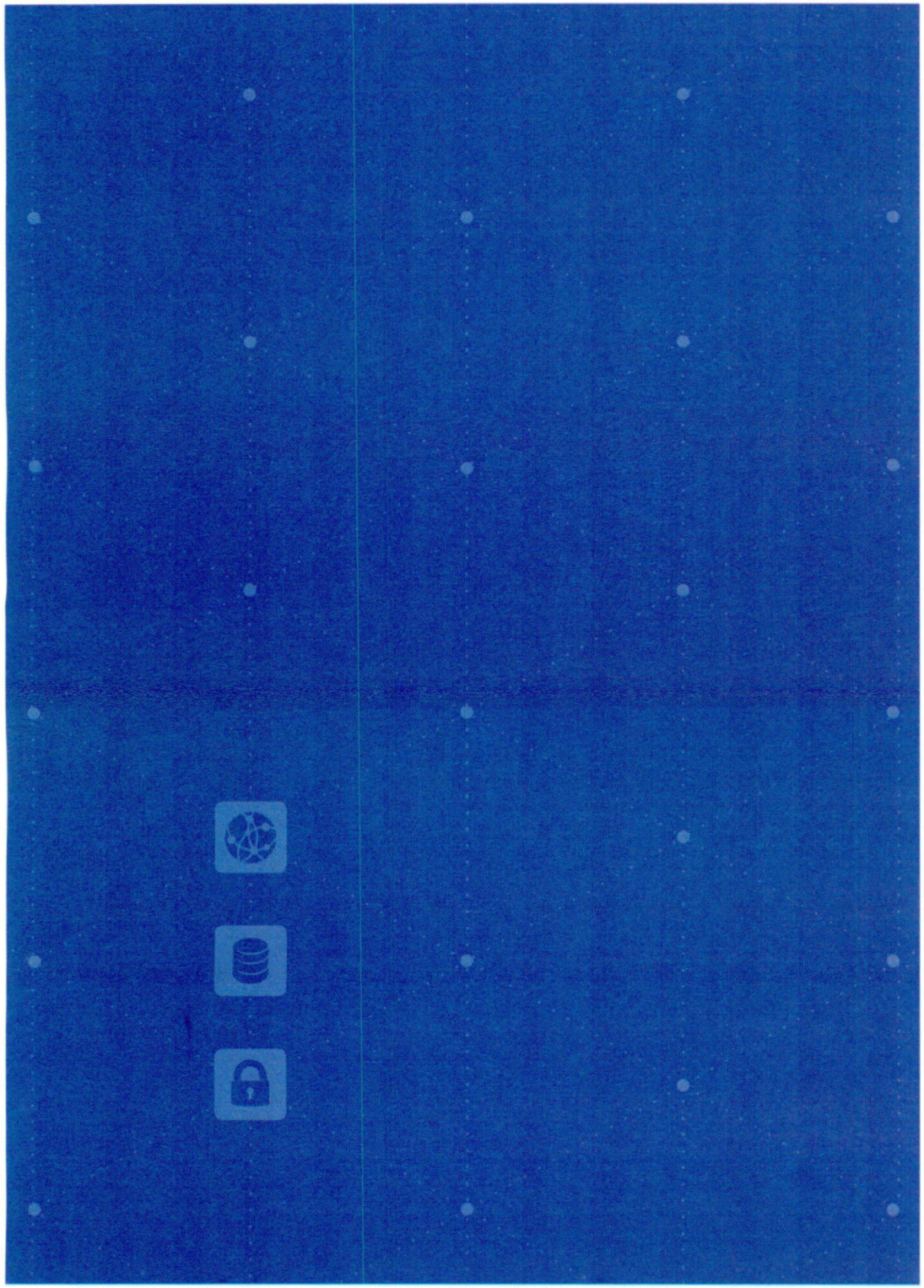
Van de Cyberbeveiligingswet zijn overheidsinstanties uitgezonderd die hun werkzaamheden hoofdzakelijk uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving. Hieronder vallen onder meer het Ministerie van Defensie, de inlichtingen- en veiligheidsdiensten, het Openbaar Ministerie, de politie en de veiligheidsregio's.

Onderwijs

De Minister van Onderwijs, Cultuur en Wetenschap heeft voor bekostigde hogescholen en universiteiten gebruikgemaakt van de mogelijkheid in de Cyberbeveiligingswet om hoger-onderwijsinstellingen aan te wijzen als belangrijke entiteit. Met de ministeriële regeling waarin deze aanwijzing is vastgelegd, vallen deze instellingen onder de Cyberbeveiligingswet.

Complexe bedrijfsmodellen

Voor organisaties met een complexe bedrijfsstructuur, zoals organisaties met vestigingen in meerdere EU-landen, kan het vaststellen of de Cyberbeveiligingswet van toepassing is, ingewikkeld zijn. In sommige gevallen is niet de Nederlandse Cyberbeveiligingswet van toepassing, maar de nationale wetgeving van een andere EU-lidstaat. De Handreiking complexe bedrijfsmodellen biedt ondersteuning bij het bepalen welke wetgeving op de organisatie van toepassing is.



2.

Wat betekent de Cyberbeveiligingswet voor jouw organisatie?

Wat betekent de Cyberbeveiligingswet voor jouw organisatie?

Organisaties die vallen onder de Cyberbeveiligingswet, krijgen onder andere te maken met:



Registratieplicht

Voor organisaties die onder de Cyberbeveiligingswet vallen, geldt sinds de inwerkingtreding van de wet een registratieplicht. Organisaties registreren zich via MijnNCSC bij het Nationaal Cyber Security Centrum (NCSC). Organisaties krijgen onder meer toegang tot de dienstverlening van het voor hun sector aangewezen CSIRT. Bekijk de website van het NCSC voor meer informatie over het doorlopen van een succesvolle registratie.



Zorgplicht

De zorgplicht houdt in dat essentiële entiteiten en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Het gaat hierbij om de netwerk- en informatiesystemen die zij gebruiken voor hun werkzaamheden of voor het verlenen van hun diensten, waarvoor zij onder de Cyberbeveiligingswet vallen. Zie op pagina 14 een overzicht van de maatregelen die organisaties in het kader van de zorgplicht moeten nemen.



Meldplicht

Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten melden aan hun Computer Security Incident Response Team (CSIRT) en de toezichthouder. Voor het doen van deze meldingen is een centraal meldportaal ingericht op MijnNCSC. In dit meldportaal kunnen organisaties in één keer melden bij hun CSIRT en toezichthouder. Na de melding van een significant incident kan bijstand worden verkregen van het CSIRT. Een incident is significant als het een ernstige verstoring van de diensten of financiële verliezen voor de organisatie veroorzaakt of kan veroorzaken óf andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. In de ministeriële regelingen van voor sectoren verantwoordelijke ministers zijn per sector drempelwaarden opgenomen om te bepalen wanneer er sprake is van een significant incident. Organisaties doen er daarom goed aan de ministeriële regeling voor hun sector te raadplegen. Bekijk het overzicht van de ministeriële regelingen.



Bestuurlijke verantwoordelijkheid en trainingsplicht voor bestuurders

De Cyberbeveiligingswet bevat ook enkele verplichtingen voor het bestuur van een essentiële entiteit of belangrijke entiteit. Dat bestuur moet namelijk de maatregelen in het kader van de zorgplicht van de entiteit goedkeuren en toezien op de uitvoering van die maatregelen. Daarnaast moeten de leden van het bestuur een training volgen om zo kennis en vaardigheden te verwerven om bijvoorbeeld de gevolgen van risico's en risicobeheersmaatregelen te kunnen beoordelen.



Toezicht

Op de naleving van de verplichtingen uit de Cyberbeveiligingswet door een organisatie, zoals de zorg- en de meldplicht, wordt toezicht gehouden. In geval van overtredingen zullen handhavingsmaatregelen hoofdzakelijk de organisatie betreffen, maar in bepaalde gevallen (bijvoorbeeld bovengenoemde trainingsplicht) ook de individuele bestuurders raken.

Welke maatregelen moet een organisatie nemen om aan de zorgplicht te voldoen?

De Cyberbeveiligingswet schrijft voor dat organisaties in ieder geval maatregelen moeten treffen op de volgende gebieden:



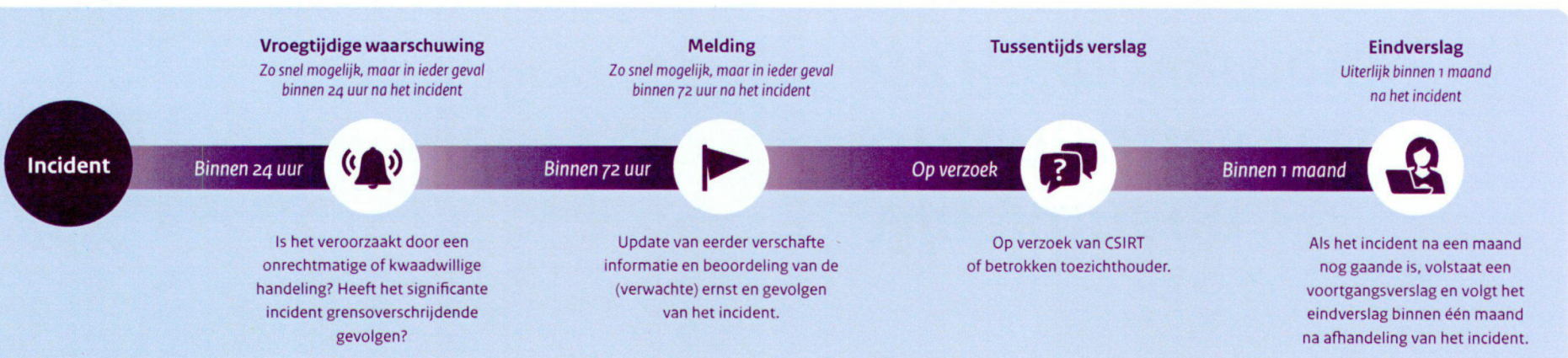
- Maatregel 1 Beleid over risicoanalyse en beveiliging van netwerk- en informatiesystemen;
- Maatregel 2 Incidentenbehandeling;
- Maatregel 3 Bedrijfscontinuïteit, zoals back-upbeheer en herstelplannen, en crisisbeheer;
- Maatregel 4 Beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten ten aanzien van de relaties met rechtstreekse leveranciers en dienstverleners;
- Maatregel 5 Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, waaronder de respons op en bekendmaking van kwetsbaarheden;
- Maatregel 6 Beleid en procedures om de effectiviteit van maatregelen voor het beheersen van cyberbeveiligingsrisico's te beoordelen;
- Maatregel 7 Basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
- Maatregel 8 Beleid en procedures voor het gebruik van cryptografie en, waar aangewezen, encryptie;
- Maatregel 9 Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets;
- Maatregel 10 Waar passend, het gebruik van multifactorauthenticatie- of continue authenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de organisatie.

Deze zorgplichtmaatregelen zijn verder uitgewerkt in het Cyberbeveiligingsbesluit. Daarnaast zijn voor verschillende sectoren in ministeriële regelingen sectorspecifieke voorschriften vastgesteld.

Wat valt onder meldplicht?

Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten melden aan hun CSIRT en toezichthouder. Voor het doen van deze meldingen is een centraal meldportaal ingericht op MijnNCSC. In dit meldportaal kunnen organisaties in één keer melden bij hun CSIRT en toezichthouder.

Er geldt een gefaseerde meldplicht:

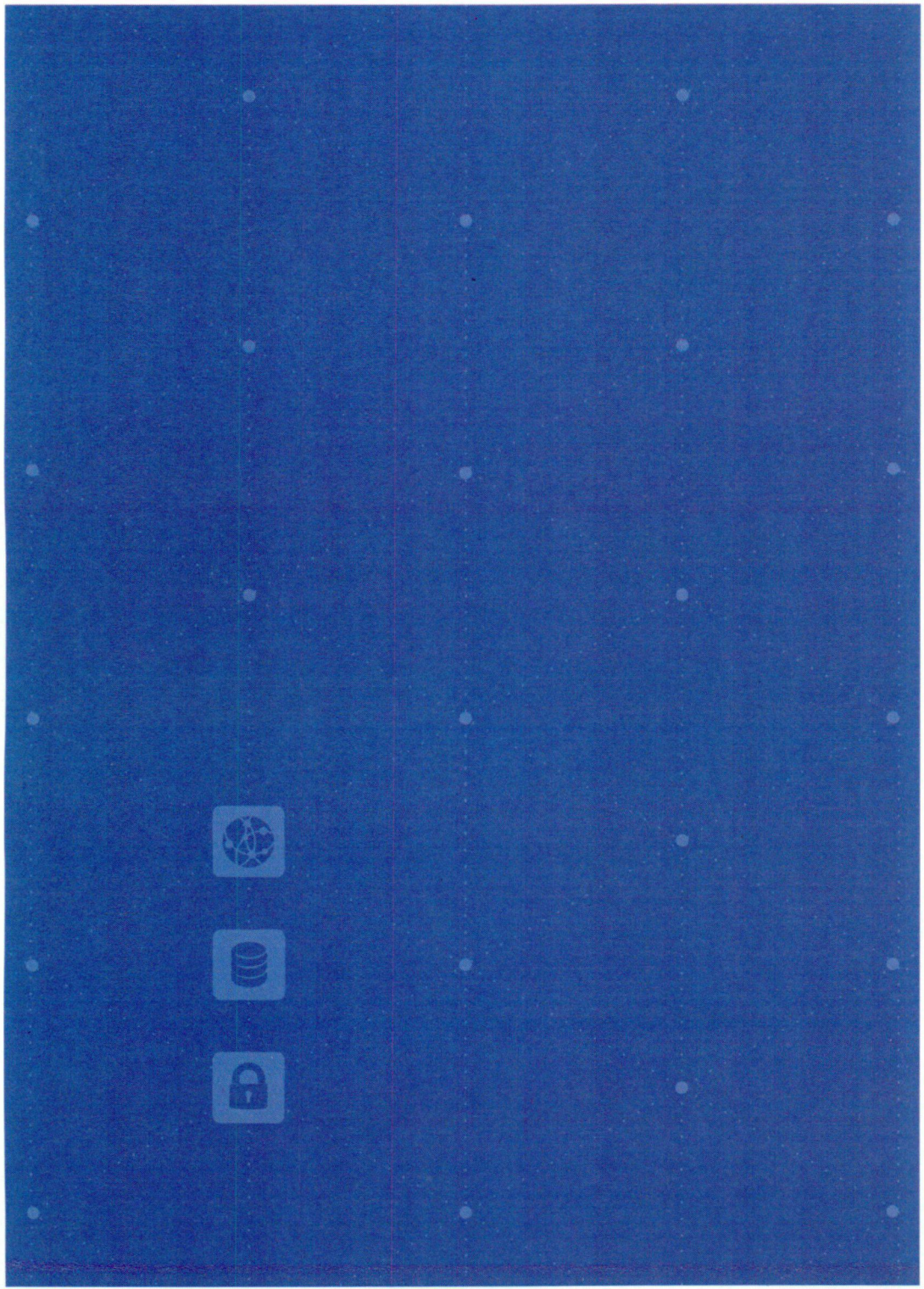


Significant incident

Een incident is significant als het een ernstige verstoring van de diensten of financiële verliezen voor de organisatie veroorzaakt of kan veroorzaken óf andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

In de ministeriële regelingen van voor sectoren verantwoordelijke vakministers zijn per sector drempelwaarden opgenomen om te bepalen wanneer een incident significant is. Deze drempelwaarden kunnen dus verschillen per sector.

Raadpleeg daarom de ministeriële regeling die voor de eigen sector van toepassing is.



3.

Wat kunnen organisaties van de Rijksoverheid verwachten?

Wat kunnen organisaties van de Rijksoverheid verwachten?

De organisaties die onder de Cyberbeveiligingswet vallen, kunnen worden ondersteund door een Computer Security Incident Response Team (CSIRT). Het hoofddoel van een CSIRT is om snel en efficiënt te reageren op cyberincidenten, het adequaat afhandelen van een incident en het minimaliseren van schade. Het CSIRT doet dit onder meer door bijstand te verlenen bij cyberdreigingen en -incidenten, en door organisaties te waarschuwen voor en informatie te verstrekken over dreigingen, kwetsbaarheden en incidenten. Daarnaast kan het CSIRT bijvoorbeeld ook op verzoek van een organisatie netwerk- en informatiesystemen van die organisatie scannen. Vanwege hun registratie bij het NCSC kunnen organisaties gebruik maken van de dienstverlening van het voor hun sector aangewezen CSIRT.

De taken van het CSIRT zullen voor een groot deel van de organisaties in de praktijk worden uitgevoerd door het Nationaal Cyber Security Centrum (NCSC). Voor enkele sectoren of soorten organisaties (bijvoorbeeld waterschappen, sector gezondheidszorg) zal een andere instantie als CSIRT worden aangewezen. Het NCSC voert daarnaast de in de Cyberbeveiligingswet opgenomen taken van het centrale contactpunt uit. Ook beheert het NCSC het nationale register van entiteiten.

Bekijk de Cyberbeveiligingswet doorverwijsboom voor een overzicht van de verantwoordelijke ministeries, CSIRTS en toezichthouders per sector.

Hoe kan jouw organisatie voldoen aan de Cyberbeveiligingswet?

Ga aan de slag met het voldoen aan de Cyberbeveiligingswet en het digitaal weerbaar maken van jouw organisatie:

- Breng in kaart of jouw organisatie onder de Cyberbeveiligingswet valt, bijvoorbeeld aan de hand van de NIS2 Zelfevaluatie NL van de RDI.
- Registreer jouw organisatie via MijnNCSC. Hierdoor krijgen organisaties onder meer toegang tot de dienstverlening van het voor hun sector aangewezen CSIRT.
- Beoordeel jouw cybersecuritymaatregelen en identificeer jouw verbeterpunten. Het Cbw Control Framework, ontwikkeld door de Auditdienst Rijk en NOREA, helpt IT-verantwoordelijken om verbeterpunten, uitgaand van de verplichtingen in de Cyberbeveiligingswet, te identificeren en gerichte stappen te zetten richting compliance. Gebruik de NIS2-Quickscan van de RDI om te toetsen of jouw bestaande maatregelen van jouw organisatie voldoen aan de eisen in de Cyberbeveiligingswet en de daaronder vallende lagere regelgeving.
- Ga aan de slag met de in de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en de sectorale ministeriële regeling vereiste zorgplichtmaatregelen. Voer een grondige risicoanalyse uit om de vereiste maatregelen en vervolgstappen in kaart te brengen. Het NCSC biedt diverse adviesproducten die je hierbij ondersteunen.

Lees meer over deze stappen en de beschikbare hulpmiddelen op de website van het NCSC.

Hoe wordt toezicht gehouden?

De toezichthouder controleert of organisaties voldoen aan de verplichtingen uit de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en de sectorale ministeriële regelingen.

Voor essentiële entiteiten geldt proactief toezicht. Dit betekent dat de toezichthouder actief kan controleren of aan de wettelijke verplichtingen wordt voldaan, ook als er geen aanwijzingen zijn voor een mogelijke overtreding.

Voor belangrijke entiteiten geldt reactief toezicht. De toezichthouder treedt in beginsel pas op als daar aanleiding voor is, bijvoorbeeld na een incident, een melding of andere aanwijzingen voor een mogelijke overtreding.

Voor bepaalde verplichtingen, zoals de verplichte training van bestuurders, ziet de toezichthouder toe op de naleving door de individuele leden van het bestuur. Daarnaast wordt toezicht gehouden op de naleving van de verplichtingen die gelden voor aanbieders van domeinnaamregistratiediensten.

Hieronder is per categorie weergegeven welke handhavingsinstrumenten een toezichthouder kan inzetten.

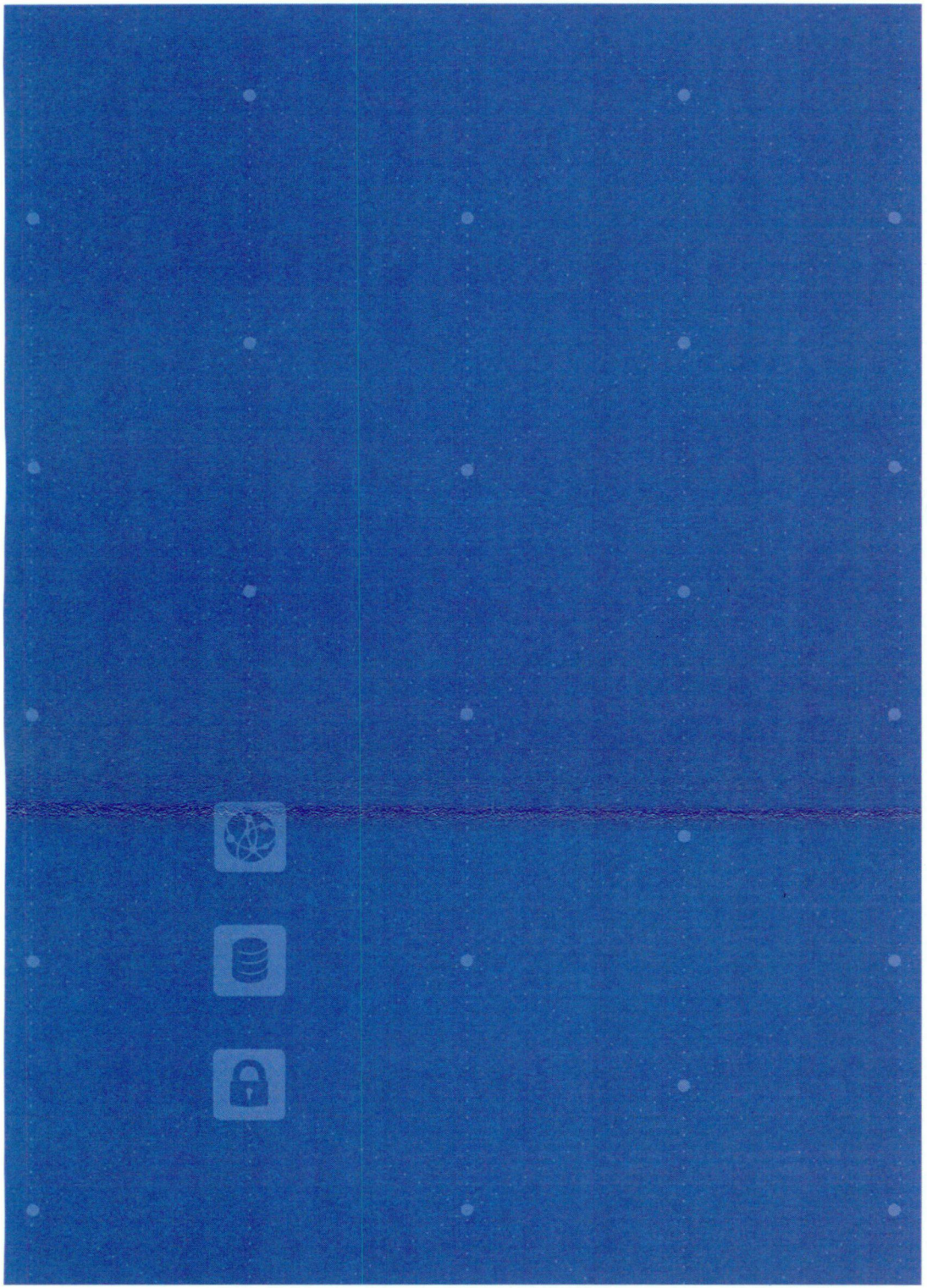
Handhavingsinstrumentarium

Essentiële entiteiten
- Controlefunctionaris
- Beveiligingsscan
- Beveiligingsaudit
- Openbaarmaking overtreding
- Bindende aanwijzing
- Last onder bestuursdwang
- Last onder dwangsom
- Verzoek tot schorsing certificering of vergunning
- Verzoek tot schorsing bestuurslid
- Bestuurlijke boete

Belangrijke entiteiten
- Beveiligingsscan
- Beveiligingsaudit
- Bindende aanwijzing
- Openbaarmaking overtreding
- Last onder bestuursdwang
- Last onder dwangsom
- Bestuurlijke boete

Entiteiten die domeinnaamregistratiediensten verlenen
- Bindende aanwijzing
- Last onder dwangsom
- Bestuurlijke boete

Bestuursleden van essentiële entiteiten en belangrijke entiteiten
- Last onder dwangsom
- Bestuurlijke boete



4.

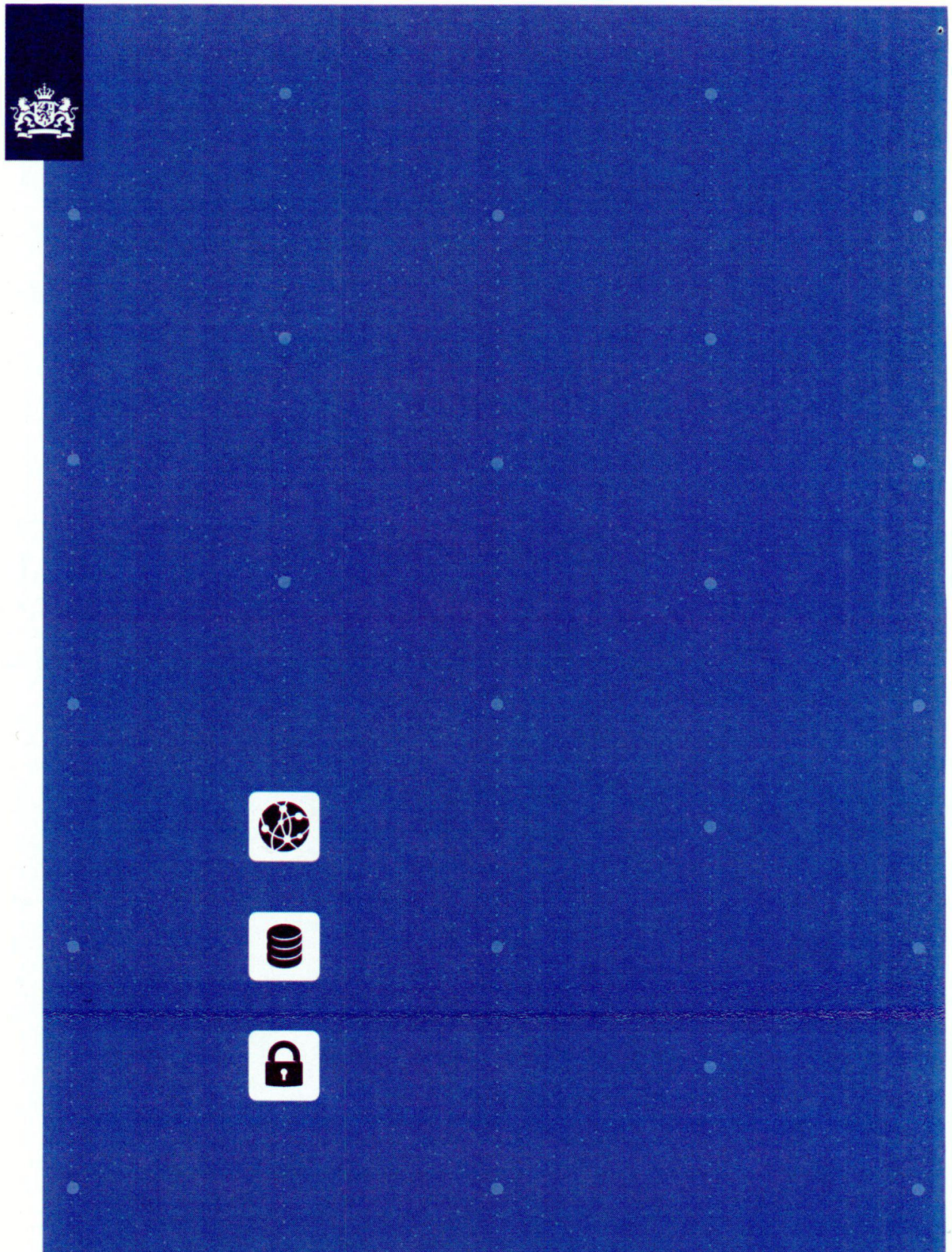
Meer weten?

Meer weten?

De Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten zijn sinds 15 augustus 2026 van kracht. Organisaties die onder de Cyberbeveiligingswet vallen, zijn zelf verantwoordelijk voor het naleven van de hierin opgenomen wettelijke verplichtingen. Meer informatie is te vinden op de website van de NCTV, het NCSC en de ministeries.

augustus 2026

Medegefinancierd door
de Europese Unie



w wet

w weerbaarheid

k kritieke

e entiteiten

Wet weerbaarheid kritieke entiteiten

Handreiking voor kritieke entiteiten

augustus 2026

Inleiding

Om de weerbaarheid van Europese lidstaten te versterken heeft de Europese Unie eind 2022 de Critical Entities Resilience Directive (CER-richtlijn) vastgesteld. Het doel van deze richtlijn is om kritieke infrastructuur en essentiële diensten in Europa beter te beschermen tegen risico's die de continuïteit daarvan kunnen verstoren. Denk hierbij aan sabotage, natuurrampen, noodsituaties op het gebied van de volksgezondheid of andere incidenten met een grote maatschappelijke impact.

In Nederland is de CER-richtlijn uitgewerkt in de Wet weerbaarheid kritieke entiteiten (Wwke).

De Wwke heeft als doel de weerbaarheid te vergroten van organisaties die essentiële diensten verlenen in Nederland. Deze organisaties zijn aangemerkt als kritieke entiteit.
Het gaat om de weerbaarheid tegen uiteenlopende dreigingen en risico's, zoals natuurrampen en ongevallen, maar ook (terroristische) misdrijven en sabotage, die de levering van essentiële diensten aanzienlijk kunnen verstoren.

Cyberbeveiligingswet

Naast de Wwke is ook de herziening van de Europese Network and Information Security Directive (NIS2-richtlijn) in Nederlandse wetgeving omgezet via de Cyberbeveiligingswet (Cbw). De Cyberbeveiligingswet richt zich op de digitale weerbaarheid van organisaties. De Wwke heeft een all-hazard benadering. Dit betekent dat organisaties zich richten op de fysieke, organisatorische en andere risico's die essentiële diensten kunnen verstoren. Beide wetten vullen elkaar aan en dragen bij aan een weerbare samenleving.

Voor welke organisaties geldt de Wwke?

De Wwke is van toepassing op organisaties die essentiële diensten verlenen binnen verschillende sectoren.

Verantwoordelijke ministeries beoordelen welke organisaties als kritieke entiteit worden aangewezen. Daarbij kijken zij onder meer naar de mogelijke gevolgen die een verstoring van de dienstverlening kan hebben voor maatschappelijke functies, economische activiteiten, de volksgezondheid, de openbare veiligheid of het milieu.

Meer informatie over de sectoren waarop de Wwke op dit moment van toepassing is en de criteria voor aanwijzing is te vinden op de **website** van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Voor **sectorspecifieke vragen** over de toepassing van de Wwke kunnen organisaties terecht bij het ministerie dat verantwoordelijk is voor hun sector.

Voor wie is deze handreiking bedoeld?

Deze handreiking helpt organisaties die zijn aangewezen als kritieke entiteit om te begrijpen welke verplichtingen gelden, welke termijnen belangrijk zijn en welke ondersteuning beschikbaar is.

Voor welke sectoren geldt de Wwke?



w wet

w weerbaarheid

k kritieke

e entiteiten

Inhoud

Inleiding 4

1. U bent aangewezen als kritieke entiteit: wat nu? 5

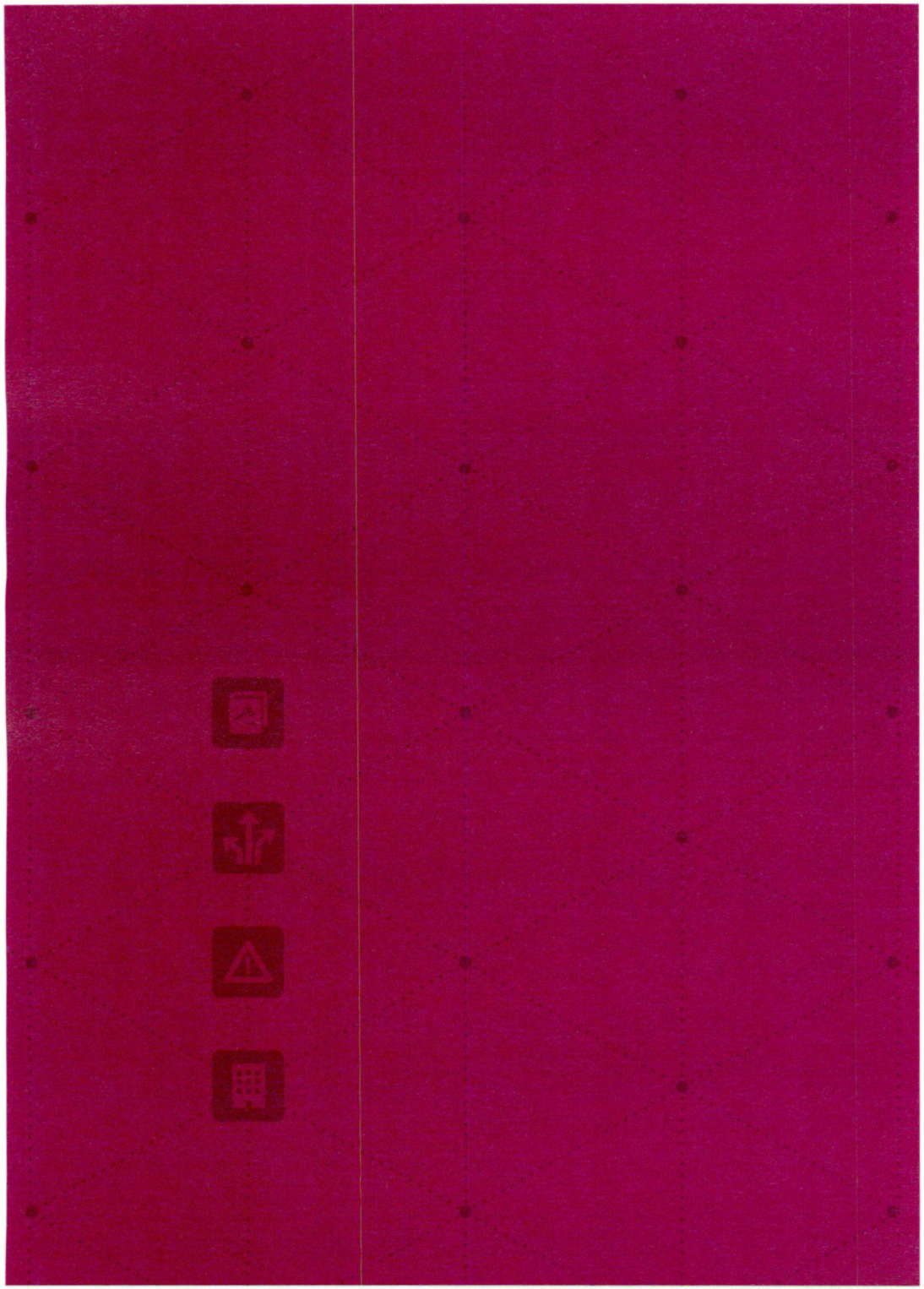
2. Voer een risicobeoordeling uit 9

3. Voldoe aan de zorgplicht 12

4. Voldoe aan de meldplicht 16

5. Maak gebruik van ondersteuning 19

6. Toezicht en handhaving 21



1.

U bent aangewezen als kritieke entiteit: wat nu?

Wat houdt de Wet weerbaarheid kritieke entiteiten in?

Uw organisatie is aangewezen als kritieke entiteit onder de Wet weerbaarheid kritieke entiteiten (Wwke) door de voor uw sector verantwoordelijke vakminister. Met deze aanwijzing gelden voor uw organisatie verschillende wettelijke verplichtingen. Ook kan uw organisatie gebruikmaken van ondersteuning om de weerbaarheid van essentiële diensten te versterken.

In dit hoofdstuk leest u welke stappen uw organisatie moet zetten na de aanwijzing en welke verplichtingen en ondersteuningsmogelijkheden daarbij horen.

Wat zijn de belangrijkste onderdelen van de Wet weerbaarheid kritieke entiteiten?



Wat betekent de Wwke voor uw organisatie?

Hieronder vindt u een overzicht van de belangrijkste stappen en de bijbehorende verplichtingen. Daarnaast zijn er nog overige verplichtingen, waaronder het aanwijzen van een verbindingsfunctionaris.

Stap 1: Voer een risicobeoordeling uit

Binnen negen maanden na de aanwijzing moet uw organisatie een eigen risicobeoordeling uitvoeren. Hiermee brengt uw organisatie in kaart welke risico's de continuïteit van uw essentiële diensten kunnen verstoren en welke gevolgen deze risico's kunnen hebben.

Meer informatie hierover staat in hoofdstuk 2.

Stap 2: Voldoe aan de zorgplicht

Binnen tien maanden na de aanwijzing moet uw organisatie passende technische, organisatorische en fysieke maatregelen hebben getroffen om de weerbaarheid van uw essentiële diensten te vergroten.

Meer informatie hierover staat in hoofdstuk 3.

Stap 3: Voldoe aan de meldplicht

Als kritieke entiteit bent u verplicht binnen 24 uur incidenten te melden die een aanzienlijke verstoring veroorzaken of kunnen veroorzaken van uw essentiële diensten. Het doel van de melding is om de bevoegde autoriteit, bestaande uit het verantwoordelijke ministerie en de toezichthouder, in staat te stellen om te reageren op incidenten en waar nodig en mogelijk kan het ministerie ondersteuning bieden aan uw organisatie.

Meer informatie hierover staat in hoofdstuk 4.

Stap 4: Maak gebruik van ondersteuning

Als kritieke entiteit kunt u gebruikmaken van verschillende vormen van ondersteuning die de overheid mogelijk maakt. Denk hierbij aan informatie over dreigingen en risico's, waarschuwingen en andere hulpmiddelen die bijdragen aan het versterken van de weerbaarheid van uw organisatie. De beschikbare ondersteuning kan verschillen per sector.

Meer informatie hierover staat in hoofdstuk 5.

Stap 5: Toezicht en handhaving

De bevoegde autoriteit houdt toezicht op de naleving van de Wwke. Deze kan informatie opvragen of onderzoeken uitvoeren om te beoordelen of aan de wettelijke verplichtingen wordt voldaan.

Meer informatie hierover staat in hoofdstuk 6.

Van aanwijzing naar naleving



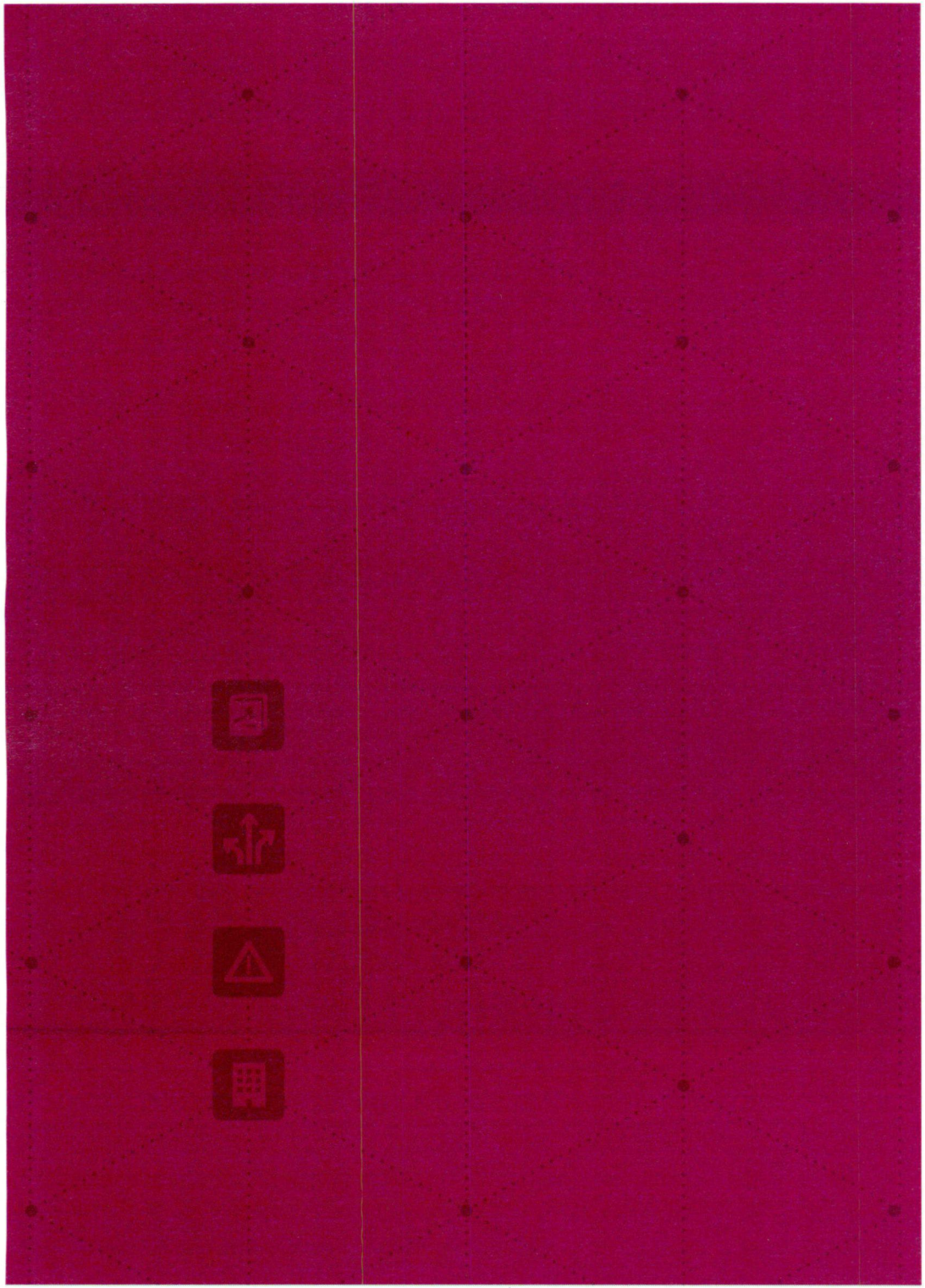
Termijn	*Verplichting*
Dag 1	Ontvangst aanwijzingsbrief
Binnen 9 maanden	Risicobeoordeling uitvoeren
Binnen 10 maanden	Voldoen aan de zorgplicht en meldplicht
Doorlopend	Incidenten melden en maatregelen actueel houden
Iedere vier jaar	Evalueren van uw risicobeoordeling - ten minste iedere vier jaar of eerder wanneer ontwikkelingen daartoe aanleiding geven.

Let op:
uw organisatie valt ook onder de Cyberbeveiligingswet

Alle organisaties die als kritieke entiteit zijn aangewezen onder de Wwke, worden automatisch aangemerkt als essentiële entiteit onder de **Cyberbeveiligingswet** (Cbw).

Andersom geldt dit niet: een essentiële entiteit onder de Cyberbeveiligingswet is niet automatisch een kritieke entiteit. Daarvoor is een formele aanwijzing door het verantwoordelijke ministerie nodig.

Door de aanwijzing als kritieke entiteit en de automatische kwalificatie als essentiële entiteit zijn ook de rechten en verplichtingen van de Cbw die gelden voor essentiële entiteiten van toepassing op uw organisatie. Dit betekent onder meer dat uw organisatie zich moet registreren in het **MijnNCSC-portaal**. Meer informatie over de stappen en verplichtingen onder de Cbw is te vinden op de **website** van de NCTV.



2.

Voer een risicobeoordeling uit

Voer een risicobeoordeling uit

Binnen negen maanden nadat uw organisatie is aangewezen als kritieke entiteit, moet u een risicobeoordeling uitvoeren. Hiermee brengt u in kaart welke risico's de continuïteit van uw essentiële diensten kunnen bedreigen en welke maatregelen nodig zijn om deze risico's te beheersen. Het is belangrijk om deze beoordeling schriftelijk vast te leggen.

Wat is een risicobeoordeling?

Met een risicobeoordeling brengt u de dreigingen, kwetsbaarheden en gevaren in kaart die kunnen leiden tot een incident. Daarnaast beoordeelt u welke impact een incident kan hebben op de verlening van uw essentiële diensten. Deze beoordeling geeft inzicht in het huidige weerbaarheidsniveau van uw organisatie en de maatregelen die nog nodig zijn om risico's te beperken en de weerbaarheid te versterken.

Wat brengt u in kaart?

In de risicobeoordeling brengt u in ieder geval in kaart:

- welke dreigingen en risico's de continuïteit van uw essentiële diensten kunnen verstoren;
- hoe groot de impact van een incident op uw dienstverlening kan zijn;
- welke maatregelen nodig zijn om risico's te voorkomen, beperken of beheersen;
- wat het huidige weerbaarheidsniveau van uw organisatie is.

Let op: sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur zijn uitgezonderd van de verplichting tot het uitvoeren van een risicobeoordeling.

De risicobeoordeling helpt u inzicht te krijgen in de kwetsbaarheden van uw organisatie en vormt de basis voor de maatregelen die u neemt om de weerbaarheid verder te versterken.

Welke informatie gebruikt u?

De manier waarop u de risicobeoordeling uitvoert is vormvrij. Het is belangrijk dat u bij de risicobeoordeling in ieder geval de informatie betrekt die u van uw ministerie hebt ontvangen. Deze informatie heeft ertoe geleid dat u bent aangewezen als kritieke entiteit. U kunt hiervoor aansluiten bij bestaande processen en documenten binnen uw organisatie, zoals:

- bestaande risicomanagementsystemen en risicoanalyses met daarbinnen bijvoorbeeld een business impact analyse (BIA);
- risicoanalyses die zijn uitgevoerd in het kader van de Cyberbeveiligingswet;
- andere bestaande risicomanagementprocessen.

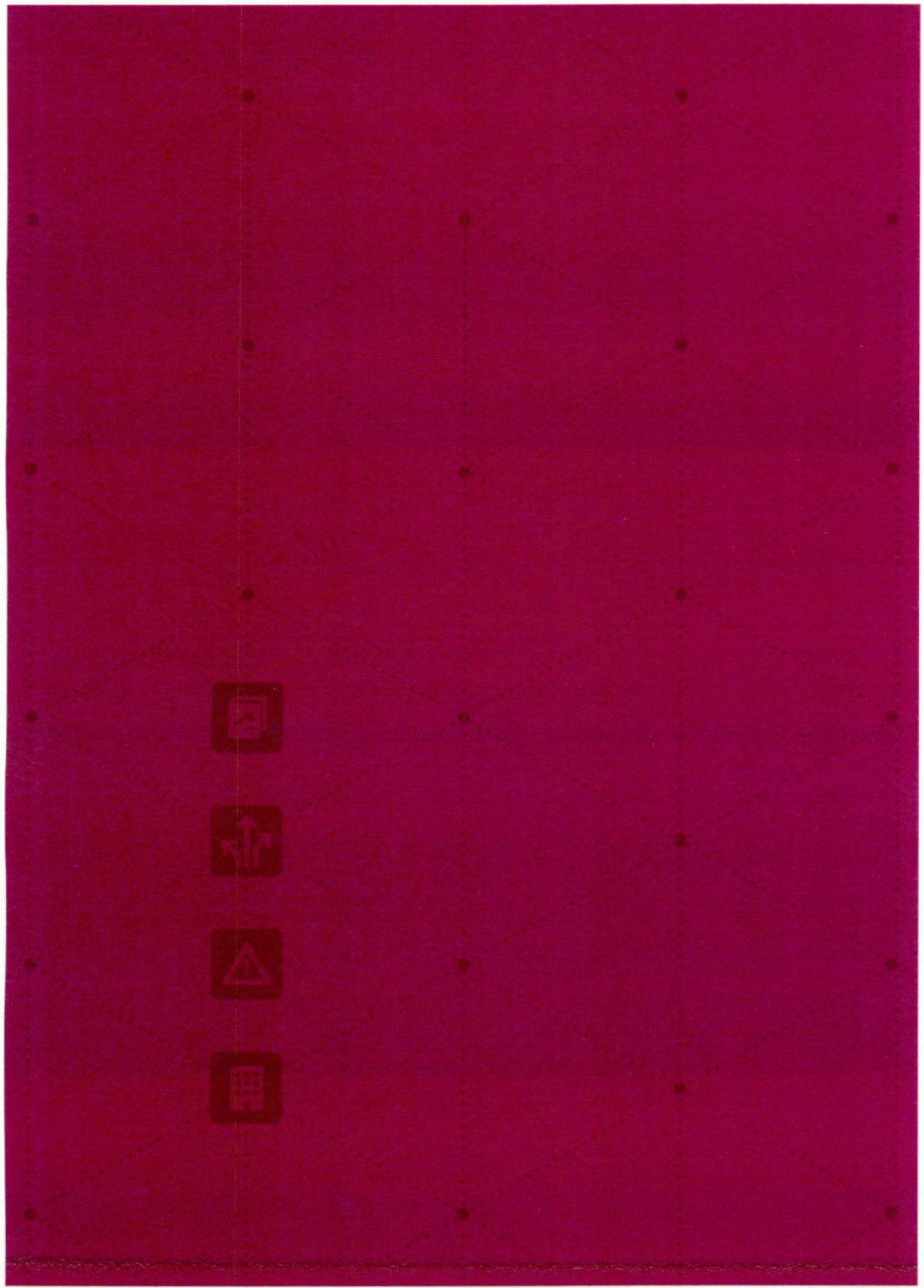
Met welke risico's houdt u rekening?

Bij de risicobeoordeling houdt u in ieder geval rekening met:

- risico's van sectoroverstijgende of grensoverschrijdende aard;
- ongevallen;
- natuurrampen;
- noodsituaties op het gebied van de volksgezondheid;
- hybride dreigingen of andere opzettelijke dreigingen, zoals terroristische misdrijven.

Evalueren en actualiseren

De risicobeoordeling evalueert u ten minste iedere vier jaar, of eerder wanneer ontwikkelingen of incidenten daartoe aanleiding geven. Wanneer nodig past uw organisatie de risicobeoordeling en het daarop gebaseerde beleid aan.



3.

Voldoe aan de zorgplicht

Voldoe aan de zorgplicht

Als kritieke entiteit ben u verplicht passende en evenredige maatregelen te nemen om risico's voor uw organisatie te beperken en de weerbaarheid van uw essentiële diensten te vergroten. De zorgplicht geldt vanaf tien maanden nadat uw organisatie is aangewezen als kritieke entiteit.

Wat is het doel van de zorgplicht?

Het doel van de zorgplicht is om de weerbaarheid van uw organisatie en de continuïteit van de essentiële diensten te versterken. Door passende en evenredige maatregelen te nemen, kunnen incidenten zoveel mogelijk worden voorkomen. Als zich toch een incident voordoet, helpen deze maatregelen om de gevolgen te beperken, de dienstverlening zo veel mogelijk in stand te houden en na een incident zo snel mogelijk te herstellen.

De maatregelen die u neemt, zijn gebaseerd op:

- de resultaten van uw eigen risicobeoordeling;
- de relevante informatie uit de sectorale risicobeoordeling die u van uw ministerie hebt ontvangen;
- relevante waarschuwingen, adviezen en informatie van andere organisaties.

De zorgplicht is opgenomen in de Wet weerbaarheid kritieke entiteiten (Wwke) en is verder uitgewerkt in **onderliggende regelgeving**, zoals het Besluit weerbaarheid kritieke entiteiten. Hierin worden maatregelen beschreven waaraan kritieke entiteiten in ieder geval aandacht moeten besteden. Deze maatregelen vormen een algemeen kader.

Op basis van de uitkomsten van uw risicobeoordeling en de sectorale risicobeoordeling die u van uw ministerie heeft ontvangen, bepaalt u welke maatregelen passend en evenredig zijn voor uw organisatie en de essentiële diensten die u verleent. De getroffen maatregelen legt u schriftelijk vast.

Let op: de sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur zijn uitgezonderd van de zorgplicht voor de Wwke, omdat zij al soortgelijke verplichtingen kennen uit andere regelgeving. Organisaties in de sector digitale infrastructuur moeten wel voldoen aan de zorgplicht voor de Cyberbeveiligingswet.

Passende en evenredige maatregelen

Niet iedere maatregel is voor iedere organisatie op dezelfde manier van toepassing. De Wwke, inclusief de onderliggende regelgeving, bevat een algemeen kader met maatregelen waaraan kritieke entiteiten aandacht moeten besteden. Voor de concrete invulling is ruimte voor een eigen afweging.

Uw organisatie bepaalt zelf welke maatregelen redelijkerwijs nodig zijn om risico's te beheersen. Daarbij houdt u onder meer rekening met:

- de uitkomsten van uw risicobeoordeling;
- de mate waarin uw organisatie is blootgesteld aan risico's;
- de omvang van uw organisatie;
- de kans dat zich incidenten voordoen;
- de mogelijke impact op de maatschappij en economie;
- de verhouding tussen de kosten van een maatregel en het beoogde effect daarvan.

Een passende maatregel kan daardoor per organisatie verschillen.

Onderwerpen waarop uw organisatie maatregelen moet nemen

De maatregelen die kritieke entiteiten in het kader van de zorgplicht moeten nemen, zijn nader uitgewerkt in het **Besluit weerbaarheid kritieke entiteiten (Bwke)**. Hierbij moet uw organisatie in ieder geval maatregelen treffen op de volgende onderwerpen:

Kritieke infrastructuur

- Identificeer uw kritieke infrastructuur (een voorziening, een faciliteit, apparatuur, een netwerk of een systeem of onderdelen daarvan die noodzakelijk zijn voor de verlening van een essentiële dienst) en houd hiervan een actueel overzicht bij;
- Leg het beheer van deze infrastructuur vast in beleid;
- Stel beleid op voor het verwerven, ontwikkelen, onderhouden, herstellen en beëindigen van kritieke infrastructuur.

Leveranciers en dienstverleners

- Identificeer de rechtstreekse leveranciers en dienstverleners die van belang zijn voor uw essentiële dienstverlening;
- Stel beleid vast over hun rol ten aanzien van de essentiële diensten en de weerbaarheid daarvan.

Fysieke beveiliging

Neem passende maatregelen voor de bescherming van gebouwen en kritieke infrastructuur, zoals:

- het instellen van beveiligingszones;
- het inrichten van toegangsbeveiliging;
- het beveiligen van kantoren, ruimten, faciliteiten, bedrijfsmiddelen buiten het terrein en nutsvoorzieningen;
- het monitoren van de beveiliging;
- het veilig plaatsen en beschermen van kritieke apparatuur. Denk bijvoorbeeld aan servers, procesbesturingssystemen, netwerkapparatuur of andere systemen die essentieel zijn voor de verlening van de essentiële dienst.

Personeelsbeveiliging

Breng de rollen, bevoegdheden en verantwoordelijkheden van medewerkers die verantwoordelijk zijn voor de weerbaarheid van uw organisatie in kaart en leg dit vast in beleid.

Denk hierbij onder meer aan:

- het identificeren van personeelsleden met kritieke functies;
- het vaststellen van toegangsrechten;
- regelmatige bewustwordings- en opleidingsactiviteiten;
- oefeningen voor personeel.

Crisisbeheersing en bedrijfscontinuïteit

Zorg voor vastgestelde plannen voor:

- het beheersen van crises en incidenten;
- het waarborgen van de continuïteit van de essentiële diensten.

Bescherming van gevoelige informatie

Neem maatregelen om de beveiliging, integriteit en vertrouwelijkheid van gevoelige informatie die van belang is voor de weerbaarheid van uw organisatie te waarborgen.

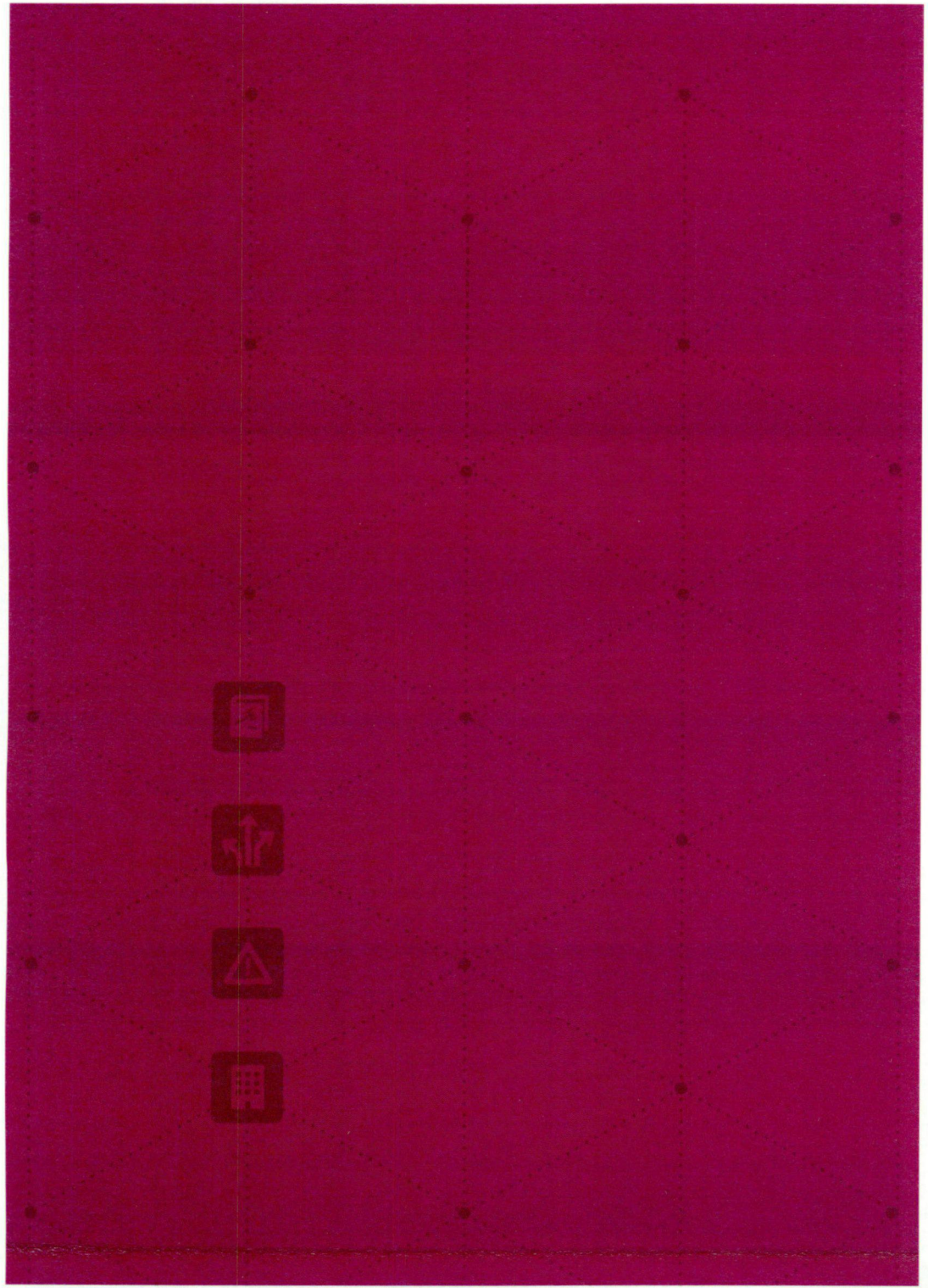
Bestaande maatregelen als uitgangspunt

Beschikt uw organisatie al over vergelijkbare maatregelen, beleid, procedures of plannen? Dan kan dit een goede basis vormen om te voldoen aan de verplichtingen uit de Wwke.

Het blijft daarbij belangrijk om rekening te houden met de risico's uit zowel de sectorale risicobeoordeling van het ministerie als de risicobeoordeling van uw eigen organisatie. Daarbij wordt uitgegaan van een zogenoemde all-hazard benadering, waarbij rekening wordt gehouden met alle typen dreigingen.

Evalueren en actualiseren

De risicobeoordeling en de getroffen maatregelen evalueert u ten minste iedere vier jaar, of eerder wanneer ontwikkelingen of incidenten daartoe aanleiding geven. Daarbij toetst u ook of de maatregelen nog doeltreffend zijn en aansluiten bij de actuele risico's voor uw organisatie.



4.

Voldoe aan de meldplicht

Voldoe aan de meldplicht

De Wet weerbaarheid kritieke entiteiten (Wwke) verplicht kritieke entiteiten om incidenten te melden die de verlening van hun essentiële diensten aanzienlijk verstoren of kunnen verstoren. De meldplicht geldt vanaf tien maanden nadat uw organisatie is aangewezen als kritieke entiteit.

Hoe werkt de meldplicht?

De meldplicht bestaat uit twee fasen:

- een eerste melding binnen 24 uur nadat uw organisatie kennis heeft genomen van het incident;
- een gedetailleerd eindverslag binnen één maand na de eerste melding.

Meldingen doet u via het **MijnNCSC-portaal.**

Welke incidenten moet u melden?

De meldplicht geldt voor incidenten die de verlening van uw essentiële diensten aanzienlijk verstoren of kunnen verstoren. Dit kunnen zowel fysieke als digitale incidenten zijn.

Om te bepalen of een verstoring significant is, wordt onder andere gekeken naar:

- het aantal getroffen gebruikers;
- de duur van de verstoring;
- het getroffen geografische gebied;

De exacte drempelwaarden verschillen per sector en zijn uitgewerkt in **ministeriële regelingen**.

Kritieke entiteiten worden daarnaast aangemoedigd om vrijwillige meldingen te doen, bijvoorbeeld van incidenten die relevant kunnen zijn voor de weerbaarheid van de sector. Deze meldingen kunnen bijdragen aan een beter inzicht in dreigingen en risico's en daarmee aan het versterken van de weerbaarheid van de sector.

Waar doet u een melding?

U doet een melding via het centrale meldpunt op **MijnNCSC.nl**.
Dit is hetzelfde portaal dat wordt gebruikt voor meldingen onder de **Cyberbeveiligingswet**. Via dit centrale meldpunt kunnen kritieke entiteiten meldingen doen voor zowel de Cyberbeveiligingswet als de Wet weerbaarheid kritieke entiteiten.

Let op: de sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur zijn uitgezonderd van de meldplicht voor de Wwke, omdat zij al soortgelijke verplichtingen kennen uit andere regelgeving. Organisaties in de sector digitale infrastructuur moeten wel voldoen aan de meldplicht voor de Cyberbeveiligingswet.

Uw organisatie dient zich voor dit portaal te registreren. Meer informatie over registratie kunt u vinden op de **website** van het NCSC.

Let op: zolang uw organisatie deze registratie niet heeft voltooid, kunnen geen meldingen worden gedaan onder de Wwke.

Welke informatie bevat een melding?

Voor het doen van een melding vult u in het **MijnNCSC-portaal** een korte vragenlijst in. Hiermee kan de bevoegde autoriteit beoordelen:

- wat de aard van het incident is;
- wat de vermoedelijke oorzaak is;
- wat de mogelijke gevolgen van het incident zijn;
- of sprake is van vermoedelijke grensoverschrijdende gevolgen.

Daarnaast verstrekt u de contactgegevens van een contactpersoon binnen uw organisatie, zodat - indien nodig - contact kan worden opgenomen over het incident.

Wat gebeurt er met uw melding?

De melding wordt via het **MijnNCSC-portaal** doorgestuurd naar de bevoegde autoriteit.

De melding stelt de bevoegde autoriteit in staat om adequaat te reageren op incidenten en inzicht te krijgen in de aard, oorzaak, impact en mogelijke gevolgen daarvan.
Uw organisatie ontvangt in ieder geval een ontvangstbevestiging. Waar mogelijk verstrekt de bevoegde autoriteit aanvullende informatie of advies om adequaat op het incident te kunnen reageren.

Een melding van een incident leidt niet tot verhoogde aansprakelijkheid voor uw organisatie. Meldingen worden vertrouwelijk behandeld.

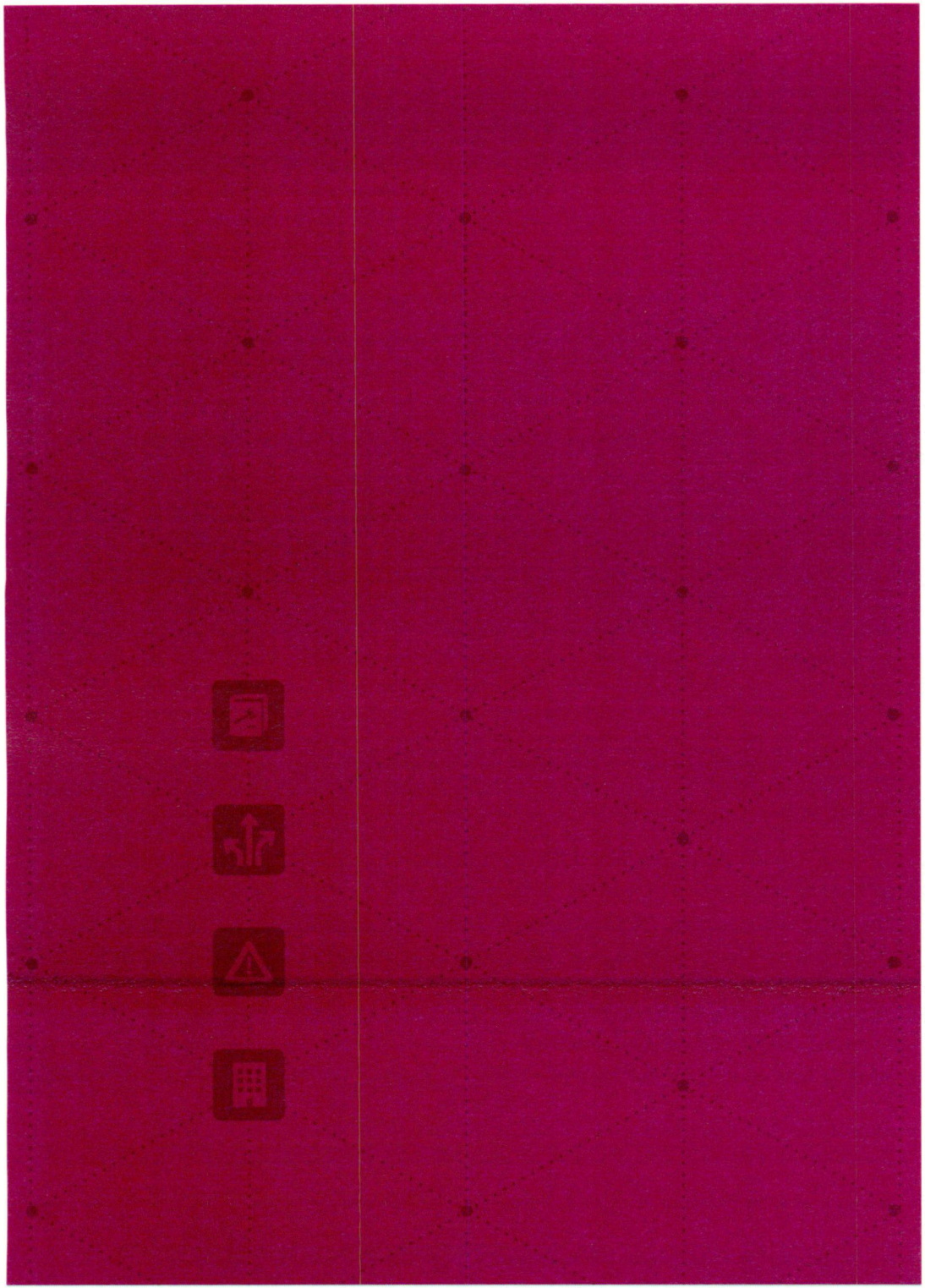
Tijdlijn meldplicht

1. Incident ontdekt
Zo snel mogelijk melding maken, binnen 24 uur na kennisname.

2. Eerste melding
- aard van het incident;
- vermoedelijke oorzaak;
- mogelijke gevolgen;
- beschikbare informatie op dat moment.

De melding wordt via het MijnNCSC-portaal doorgestuurd naar de bevoegde autoriteit (ministerie en toezichthouder).
Uiterlijk één maand na de eerste melding.

3. Gedetailleerd eindverslag
- aanvulling op de eerste melding;
- nadere analyse van het incident;
- aanvullende informatie over oorzaak, impact en gevolgen.



5.

Maak gebruik van ondersteuning

Maak gebruik van ondersteuning

De Rijksoverheid ondersteunt organisaties bij het vergroten van hun weerbaarheid. Die ondersteuning helpt organisaties om zich voor te bereiden op verstoringen van essentiële diensten en om te voldoen aan de verplichtingen uit de Wet weerbaarheid kritieke entiteiten (Wwke).

Waar bestaat de ondersteuning uit?

De ondersteuning bestaat bijvoorbeeld uit:

- sectorspecifieke handreikingen en informatie;
- uitleg over de wettelijke verplichtingen;
- informatiebijeenkomsten of webinars;
- ondersteuning bij sectorale risico-informatie;
- verwijzingen naar relevante hulpmiddelen, normen en samenwerkingsverbanden;
- het verlenen van bijstand in het geval van crisis- of noodsituaties.

De wijze waarop deze ondersteuning wordt aangeboden, kan per sector verschillen en wordt waar nodig nader uitgewerkt in lagere regelgeving, in afstemming met de toezichthouder, het betrokken ministerie en de NCTV.

6.

Toezicht en handhaving

Toezicht en handhaving

De verantwoordelijke ministeries wijzen toezichthouders aan die toezicht houden op de naleving van de verplichtingen uit de Wet weerbaarheid kritieke entiteiten (Wwke). De toezichthouder controleert of uw organisatie voldoet aan de verplichtingen die gelden voor kritieke entiteiten. Daarbij wordt onder meer gekeken naar de uitvoering van de risicobeoordeling, de meldplicht en de zorgplicht. Het is daarom van belang om deze stappen goed vast te leggen en zorgvuldig te bewaren.

Wat kunt u verwachten?

De toezichthouder kan informatie opvragen of onderzoek doen om te beoordelen of uw organisatie voldoet aan de verplichtingen uit de Wwke. Daarbij kan bijvoorbeeld worden gekeken naar:

- de uitgevoerde risicobeoordeling;
- de maatregelen die uw organisatie heeft getroffen in het kader van de zorgplicht;
- de wijze waarop incidenten worden gemeld en afgehandeld;
- de vastlegging van beleid, procedures en maatregelen.

Handhaving

Wanneer blijkt dat een organisatie niet voldoet aan de verplichtingen uit de Wwke, kan de toezichthouder besluiten om een inspectie uit te voeren bij uw organisatie. U bent verplicht om daaraan mee te werken.

De toezichthouder kan daarbij verschillende acties inzetten, zoals:

- communicatie en voorlichting;
- bestuurlijk gesprek, bedrijfsbezoek, etc.;
- het geven van een aanwijzing of opdracht om bepaalde maatregelen te treffen;
- het laten uitvoeren van een audit;
- het opleggen van een last onder bestuursdwang of een last onder dwangsom;
- het opleggen van een bestuurlijke boete.

Voor meer informatie over de Wet weerbaarheid kritieke entiteiten kunt u terecht op de **website** van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Medegefinancierd door
de Europese Unie