N  Network

I  Information

S  Security

NIS2-richtlijn

informatiebrochure

mei 2024

Inleiding

Onze afhankelijkheid van digitalisering gaat gepaard met toenemende dreigingen in het huidige geopolitieke landschap. De NIS-richtlijn (NIS1) heeft al voor grotere cyberveiligheid van de EU lidstaten gezorgd, maar de huidige context vraagt om een versterkte aanpak. Om de digitale weerbaarheid van organisaties in de Europese Unie te versterken heeft de Europese Unie eind 2022 de Network and Information Security Directive (NIS2-richtlijn) aangenomen als opvolger van de NIS1. Deze richtlijn focust zich op risico's die een bedreiging kunnen zijn voor netwerk- en informatiesystemen die worden gebruikt voor het leveren van diensten.

In Nederland zal de NIS2-richtlijn geïmplementeerd worden in de vorm van de Cyberbeveiligingswet[1]. Hier wordt sinds januari 2023 door de Rijksoverheid aan gewerkt. Op het moment dat de Cyberbeveiligingswet wordt aangenomen, zal deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangen.

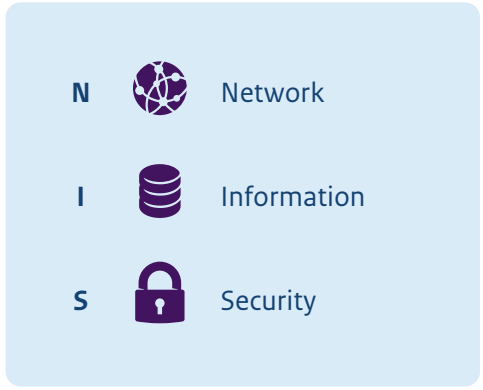
Het omzetten van de richtlijn tot nationale wetgeving is een omvangrijk en complex traject dat zorgvuldigheid vergt, ook omdat de impact voor Nederlandse organisaties die onder de NIS2-richtlijn vallen, groot is. Zo moeten er ten opzichte van bestaande wetgeving meer sectoren en meer organisaties voldoen aan de nieuwe wetgeving, zijn er een zorg- en meldplicht van toepassing op deze organisaties, en worden mechanieken om toezicht te houden ingericht.

Wat zijn de belangrijkste onderdelen van de Cyberbeveiligingswet?

- **Onderscheid tussen essentiële entiteiten en belangrijke entiteiten**
- **Zorgplicht, registratieplicht en meldplicht**
- **Bestuurlijke aansprakelijkheid en opleidingsplicht voor bestuurders**
- **Meer sectoren en organisaties**
- **Toezicht & handhaving**
- **Inrichting van stelsel van Computer Security Incident Response Teams (CSIRTs) voor bijstand aan NIS2 entiteiten**

1 Zolang deze nog niet in werking is getreden gaat het om een wetsvoorstel. Met het oog op de leesbaarheid van deze brochure wordt hier gesproken van "Cyberbeveiligingswet".

Inhoud



1

Valt uw organisatie onder de Cyber-beveiligingswet?

Valt uw organisatie onder de Cyberbeveiligingswet?

De NIS2-richtlijn richt zich op kritieke organisaties en sectoren waarbij uitval van hun diensten kunnen zorgen voor maatschappelijke en economische ontwrichting. Zie Bijlage 1 en 2 van de richtlijn voor een gedetailleerd overzicht van deze sectoren. Organisaties die in de volgende sectoren opereren vallen onder de NIS2-richtlijn, en daarmee de Nederlandse Cyberbeveiligingswet:

Bijlage 1 Zeer kritieke sectoren

- Energie
- Transport
- Bankwezen
- Infrastructuur financiële markt
- Gezond-heidszorg
- Drinkwater
- Digitale infrastructuur
- Beheerders van ICT-diensten
- Afvalwater
- Overheids-diensten
- Lokale overheden
- Ruimtevaart

Bijlage 2 Andere kritieke sectoren

- Digitale aanbieders
- Post- en koeriersdiensten
- Afvalstoffen-beheer
- Levens-middelen
- Chemische stoffen
- Onderzoek
- Vervaardiging

Entiteiten die **domeinregistratiediensten** aanbieden vallen ook onder NIS2, ongeacht hun omvang, maar behoren niet tot bijlage 1 of 2, aangezien op deze categorie andersoortige verplichtingen van toepassing zijn.

Valt uw organisatie onder de Cyberbeveiligingswet?

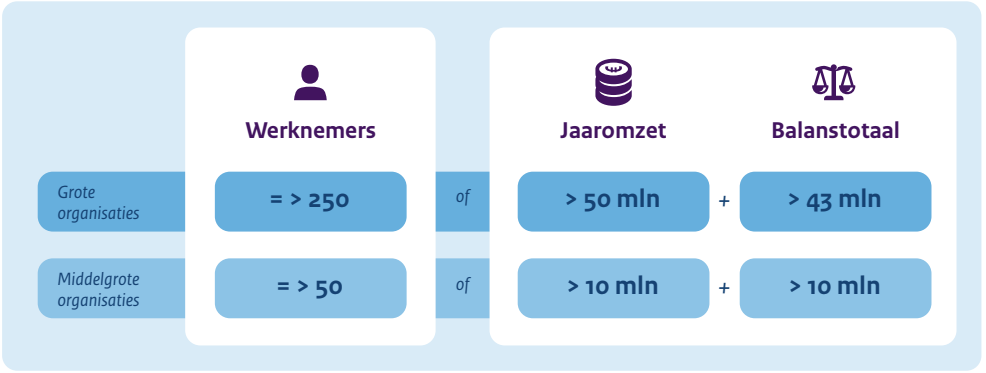
Aan de hand van in welke sector een organisatie actief is en wat de grootte van een organisatie is wordt bepaald of deze organisatie onder de NIS2-richtlijn valt, en daarmee ook onder de Cyberbeveiligingswet. De grootte van een organisatie wordt bepaald aan de hand van twee categorieën. Hiervoor zijn de volgende criteria vastgesteld:

Een organisatie is 'groot' als er:

1. Minimaal 250 personen werkzaam zijn OF;
2. Er sprake is van een jaaromzet van meer dan 50 miljoen euro, en een balanstotaal van meer dan 43 miljoen euro

Een organisatie is 'middelgroot' als er:

1. Minimaal 50 personen werkzaam zijn OF;
2. Er sprake is van een jaaromzet van meer dan 10 miljoen euro, en een balanstotaal van meer dan 10 miljoen euro



Vervolgens wordt aan de hand van de genoemde sectoren in bijlage I en II van de Cyberbeveiligingswet bepaald of een organisatie als een 'kritieke entiteit' of een 'belangrijke entiteit' wordt beschouwd.

Micro- en kleinbedrijven vallen in principe niet onder de NIS2-richtlijn. De vakminister die verantwoordelijk is voor een bepaalde sector kan er echter wel voor kiezen om een micro- of kleinbedrijf alsnog aan te wijzen op basis van een risicobeoordeling. Bijvoorbeeld als blijkt dat hun dienstverlening van cruciaal belang is voor de Nederlandse economie of maatschappij. In dat geval worden deze bedrijven hierover geïnformeerd door het desbetreffende ministerie. Daarmee kunnen ze alsnog onder de Cyberbeveiligingswet komen te vallen.

Een uitzondering geldt voor de sector Overheid, aanbieders van openbare elektronische communicatienetwerken en -diensten, aanbieders van vertrouwensdienstverleners, registers voor topleveldomeinnamen, DNS-dienstverleners en verleners van domeinregistratiediensten. Al deze organisaties (zowel groot, middelgroot als micro/klein), dus ongeacht hun omvang vallen direct onder de Cyberbeveiligingswet.

Valt uw organisatie onder de Cyberbeveiligingswet?

Essentiële entiteiten

Grote organisaties die actief zijn in een van de genoemde sectoren uit bijlage I van de Cyberbeveiligingswet kwalificeren als essentiële entiteit. Ook zijn organisaties die als 'Kritieke entiteit' onder de Critical Entities Resilience Richtlijn (CER) vallen automatisch een 'essentiële entiteit' in de Cyberbeveiligingswet.

Een uitzondering geldt voor de sector Overheid, gekwalificeerde vertrouwensdienstverleners (QTSP), registers voor topleveldomeinnamen en verleners van DNS-diensten. Al deze organisaties (zowel groot, middelgroot als micro/klein) vallen direct onder de Cyberbeveiligingswet als essentiële entiteit. Ook middelgrote aanbieders van openbare elektronische communicatienetwerken en -diensten zijn essentiële entiteiten.

Belangrijke entiteiten

Middelgrote organisaties die actief zijn in een van de genoemde sectoren uit bijlage I en middelgrote en grote organisaties die actief zijn in een van de genoemde sectoren uit bijlage II van de Cyberbeveiligingswet kwalificeren als belangrijke entiteit.

Domeinnaamregistratiediensten

Entiteiten die domeinnaamregistratiediensten aanbieden vallen onder de wet, maar zijn geen essentiële of belangrijke entiteit. Zij zijn een afzonderlijke categorie, omdat voor hen bijzondere verplichtingen gelden; zij hebben geen meldplicht van incidenten en zorgplicht maar moeten een database met domeinnaamregistratiegegevens bijhouden. Hierop vindt ook toezicht plaats.

Overheidsinstanties

Een overheidsinstantie is een essentiële entiteit wanneer de entiteit voldoet aan de definitie en criteria voor een overheidsinstantie, zoals beschreven in artikel 6, onderdeel 35 van de richtlijn. Ministeries, provincies, gemeenten en waterschappen voldoen in elk geval aan deze criteria. Voor zelfstandige bestuursorganen en gemeenschappelijke regelingen is dit afhankelijk van het geval. Overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, zijn uitgesloten van het toepassingsgebied van de Cyberbeveiligingswet.

Onderwijs

Het wetsvoorstel maakt het mogelijk om hoger onderwijsinstellingen onder de Cyberbeveiligingswet te brengen. De Minister van Onderwijs, Cultuur en Wetenschap kan dit bepalen via een ministeriële regeling.

Zelfevaluatie

In nauwe afstemming met betrokken ministeries voor de verschillende sectoren en bijbehorende toezichthouders, heeft de Rijksinspectie Digitale Infrastructuur (RDI) een vragenlijst ontwikkeld, waarmee organisaties zelf een eerste beoordeling kunnen doen of ze onder de NIS2-richtlijn vallen en of ze gekenmerkt worden als essentieel of belangrijk. **U vindt de zelfevaluatie hier.**

2

Wat betekent de Cyberbeveiligings-wet voor uw organisatie?

Welke verplichtingen schrijft de Cyberbeveiligingswet voor?

Organisaties die vallen onder de NIS2-richtlijn hebben een aantal plichten.

1. Registratieplicht

Organisaties die vallen onder de Cyberbeveiligingswet zijn wettelijk verplicht zich te registreren in het entiteitenregister. Er wordt door het Nationaal Cyber-Security Centrum (NCSC) gewerkt aan een online registratievoorziening waarin organisaties zichzelf registreren en aanmelden als NIS2 entiteit. Doordat alle lidstaten over een register moeten beschikken, levert dit ook een Europees beeld van het aantal entiteiten onder de NIS2 op.

2. Zorgplicht

Het wetsvoorstel bevat een zorgplicht die organisaties verplicht zelf een risicoanalyse uit te voeren, op basis waarvan zij passende en evenredige maatregelen nemen voor de beveiliging van hun netwerk- en informatiesystemen die worden gebruikt voor de verlening van hun diensten. De leden van het bestuur van entiteiten moeten de maatregelen goedkeuren en toezicht houden op de uitvoering ervan. Om dit goed te kunnen doen, dienen zij ook een opleiding te volgen.

3. Meldplicht

Het wetsvoorstel schrijft voor dat entiteiten significante incidenten binnen 24 uur moeten melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Het gaat om incidenten die de verlening van de diensten van de organisatie aanzienlijk (kunnen) verstoren. Computer Security Incident Response Teams (CSIRT) kunnen vervolgens hulp en bijstand verlenen. De drempelwaarden voor significante incidenten worden nog nader uitgewerkt. Voorbeelden van factoren die incidenten tot een significant incident kunnen maken zijn de omvang van de financiële verliezen voor betrokkenen, veroorzaken van (operationele) schade aan andere entiteiten dan de getroffen entiteit. Voor het doen van meldingen wordt een centraal meldpunt ingericht door het NCSC. Het Meldportaal dat voor het doel van significante meldingen wordt ingericht is tevens geschikt voor het doen van vrijwillige meldingen van niet-significante incidenten of van bijna-incidenten.

4. Toezicht

Organisaties die onder de Cyberbeveiligingswet vallen zijn onderworpen aan toezicht. Hierbij wordt gekeken naar de naleving van de verplichtingen uit de Cyberbeveiligingswet, zoals de zorg- en meldplicht. Toezichtsmaatregelen richten zich tot de entiteit maar kunnen in een uiterst geval ook de individuele bestuurders raken.

Welke maatregelen kunt u nemen om aan de zorgplicht te voldoen?

Onder de zorgplicht vallen ten minste:

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

U kunt bovendien kijken naar informatie over aanvullende normen en kaders die gelden in specifieke sectoren. Denk aan de zorg of de overheid.

Wat valt onder meldplicht?

De Cyberbeveiligingswet heeft een meldplicht voor significante incidenten. Voor deze meldingen wordt door het Nationaal Cyber Security Centrum een centraal meldpunt ingericht. Dit om ervoor te zorgen dat het voor organisaties makkelijk is om een melding bij zowel het CSIRT als de toezichthouder te doen.

Factoren die een incident meldingswaardig maken zijn de omvang van de financiële verliezen voor betrokkenen, veroorzaken van (operationele) schade aan andere entiteiten dan de getroffen entiteit.

Er geldt een gefaseerde meldplicht:

Definitie van significant incident

Een incident is een significant incident als het:

a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of

b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken

3

Wat kunnen organisaties van de overheid verwachten?

Wat kunnen organisaties van de overheid verwachten?

Lidstaten zijn verplicht om essentiële en belangrijke entiteiten te ondersteunen in het verbeteren van hun weerbaarheid tegen digitale dreigingen.

De entiteiten waarop de Cyberbeveiligingswet van toepassing is moeten met advies en bijstand worden ondersteund door een CSIRT (Computer Security Incident Response Team). De ondersteuning vanuit de overheid kan verder bestaan uit informatie-uitwisseling, richtlijnen en kennisuitwisseling over maatregelen met als doeleinde het verhogen van cyberweerbaarheid.

In Nederland wordt het CSIRT-takenpakket dat in de NIS-2 richtlijn benoemd wordt met name belegd bij verschillende sectorale CSIRTs. Zij leveren directe ondersteuning voor de sectoren. Daarnaast heeft het Nationaal Cyber Security Centrum (NCSC) een rol als het nationale CSIRT voor sector overkoepelende taken.

- De ondersteuning van de sectorale CSIRTs is erop gericht om organisaties te helpen met de beveiliging van de netwerk- en informatiesystemen, informeren over bekende kwetsbaarheden en bedreigingen en bijstand te verlenen in het geval van een incident.

Hoe kunt u uw organisatie voorbereiden?

U kunt direct beginnen met het digitaal weerbaar maken van uw organisatie.
Het is raadzaam hier tijdig mee te beginnen zodat u op tijd voldoet aan de Cyberbeveiligingswet die voortvloeit uit NIS2-richtlijn. Met de volgende maatregelen kunt u zich voorbereiden:

- Maak een risicoanalyse van de digitale dreigingen die de dienstverlening van uw organisatie kunnen verstoren.
- Neem waar mogelijk maatregelen die uw organisatie (beter) beschermen tegen deze risico's. De 10 genoemde maatregelen om aan de zorgplicht te doen die eerder in deze brochure genoemd werden kunnen hiervoor als basis gebruikt worden.
- Zorg voor procedures die uw organisatie in staat stellen om incidenten die bedrijfsprocessen (kunnen) verstoren te detecteren, monitoren, op te lossen en te melden.

Kijk hier voor meer informatie over deze voorbereidende stappen.

Hoe wordt toezicht gehouden?

Bij ‘essentiële entiteiten’ heeft de uitval van hun diensten naar alle waarschijnlijkheid meer ontwrichtende impact op de economie en samenleving, dan uitval bij ‘belangrijke entiteiten’.

Essentiële entiteiten vallen in de Cyberbeveiligingswet daarom onder proactief toezicht. Dit wil zeggen dat er toezicht gehouden wordt op het naleven van de verplichtingen, ook wanneer er geen sprake is van eventuele incidenten. Voor belangrijke entiteiten geldt dat toezicht achteraf plaatsvindt, bijvoorbeeld als er aanwijzingen zijn voor het niet naleven van de wet, of als er een incident heeft plaatsgevonden. In alle gevallen kan de toezichthouder beveiligingsaudits en –scans uitvoeren en informatie verzoeken die nodig is om de risicobeheers-maatregelen van de betrokken entiteit te beoordelen. Het inrichten van toezicht op het naleven van deze wetgeving en het invoeren van sanctiemogelijkheden in de vorm van bestuurlijke boetes geven aan dat de vrijblijvendheid van het adequaat inrichten van een cyber security aanpak voorbij is.

- Het inzetten van het instrumentarium is enerzijds gericht op het mitigeren/ bestrijden van risico’s die een entiteit loopt door het niet naleven van bijvoor-beeld de zorgplicht of het niet melden van incidenten, en anderzijds op het beschermen van het netwerk en de keten waarin een entiteit opereert in het geval dat risico’s bij een entiteit niet gemitigeerd worden.
- Toezichthouders opereren onafhankelijk, ook onafhankelijk van de sectorale CSIRTs.

Handhavingsinstrumentarium

Essentiële entiteiten

- Controlefunctionaris
- Beveiligingsscan
- Beveiligingsaudit
- Openbaarmaking overtreding
- Bindende aanwijzing
- Last onder bestuursdwang
- Verzoek tot schorsing certificering of vergunning[2]
- Verzoek tot schorsing leden van het bestuur[2]
- Bestuurlijke boete

Belangrijke entiteiten

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

2 Dit handhavingsinstrument is niet van toepassing op overheidsinstanties

Bijlagen

Bijlage 1 Zeer kritieke sectoren

Bevoegde autoriteit	Sector	Subsector	*Grote organisaties*	*Middelgrote organisaties*	*Kleine- en micro-organisaties*
Minister van Klimaat en Energie	**Energie**	Elektriciteit; stadsverwarming & -koeling; gas; waterstof; olie. Inclusief aanbieders van oplaaddiensten aan eindgebruikers	Essentieel	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	**Transport**	Lucht (commerciële luchtvaartmaatschappijen; luchthavens; luchtverkeersleiding); spoor (infra en ondernemingen); water (vervoersmaatschappijen; havens; verkeersbegeleidingsdiensten voor schepen; wegtransport	Essentieel	Belangrijk	Niet van toepassing
		Openbaar vervoer: alleen indien geïdentificeerd als kritieke aanbieder in de Critical Entities Resilience Directive (CER-richtlijn)	Essentieel	Belangrijk	Niet van toepassing
Minister van Financiën	**Bankwezen**	Kredietinstellingen	Essentieel	Belangrijk	Niet van toepassing
Minister van Financiën	**Infrastructuur financiële markt**	Handelsplatforms	Essentieel	Belangrijk	Niet van toepassing

Bevoegde autoriteit	Sector	Subsector	*Grote organisaties*	*Middelgrote organisaties*	*Kleine- en micro-organisaties*
Minister van Volksgezondheid, Welzijn en Sport	**Gezondheidszorg**	Zorgverleners; laboratoria; onderzoek & ontwikkeling van geneesmiddelen; vervaardiging van farmaceutische basisproducten en -preparaten; vervaardiging van medische hulpmiddelen die van cruciaal belang zijn bij noodsituaties op het gebied van de volksgezondheid	Essentieel	Belangrijk	Niet van toepassing
		Entiteiten met een distributievergunning voor geneesmiddelen: alleen indien geïdentificeerd als kritieke aanbieder in de Critical Entities Resilience Directive (CER-richtlijn)	Essentieel	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	**Drinkwater**		Essentieel	Belangrijk	Niet van toepassing
Minister van Economische Zaken en Klimaat	**Digitale infrastructuur**	Gekwalificeerde vertrouwensdienstverleners (QTSP)	Essentieel	Essentieel	Essentieel
		Registers voor topleveldomeinnamen	Essentieel	Essentieel	Essentieel
		Verleners van domeinnaamregistratiediensten	Essentieel	Essentieel	Essentieel
		Aanbieders van openbare elektronische communicatienetwerken	Essentieel	Belangrijk	Niet van toepassing

Bevoegde autoriteit	Sector	Subsector	*Grote organisaties*	*Middelgrote organisaties*	*Kleine- en micro-organisaties*
Minister van Economische Zaken en Klimaat	**Digitale infrastructuur**	Niet-gekwalificeerde vertrouwensdienstverleners	Essentieel	Belangrijk	Belangrijk
		Aanbieders van internet exchange points	Essentieel	Belangrijk	Niet van toepassing
		Cloudserviceprovider	Essentieel	Belangrijk	Niet van toepassing
		Datacenter serviceprovider	Essentieel	Belangrijk	Niet van toepassing
		Content delivery network providers	Essentieel	Belangrijk	Niet van toepassing
Minister van Economische Zaken en Klimaat	**Beheerders van ICT-diensten**	Managed service providers, managed security service providers	Essentieel	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	**Afvalwater**	Alleen als het een essentieel onderdeel is van de algemene activiteit	Essentieel	Belangrijk	Niet van toepassing

Bevoegde autoriteit	Sector	Subsector	*Grote organisaties*	*Middelgrote organisaties*	*Kleine- en micro-organisaties*
Minister van Binnenlandse Zaken en Koninkrijks-relaties	**Overheids-diensten**	Van centrale overheden (uitgezonderd rechterlijke macht, parlementen, centrale banken; defensie, nationale of openbare veiligheid)	Essentieel	Essentieel	Essentieel
Minister van Binnenlandse Zaken en Koninkrijks-relaties	**Lokale overheden**	Provincies, gemeenten, waterschappen	Essentieel	Essentieel	Essentieel
Minister van Economische Zaken en Klimaat	**Ruimtevaart**	Infrastructuur op de grond	Essentieel	Belangrijk	Niet van toepassing

Bijlage 2 Andere kritieke sectoren

Bevoegde autoriteit	Sector	Subsector	*Grote organisaties*	*Middelgrote organisaties*	*Kleine- en micro-organisaties*
Minister van Economische Zaken en Klimaat	**Digitale aanbieders**	Online marktplaatsen, zoekmachines, social media platforms	Belangrijk	Belangrijk	Niet van toepassing
Minister van Economische Zaken en Klimaat	**Post- en koeriersdiensten**	Online marktplaatsen, zoekmachines, social media platforms	Belangrijk	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	**Afvalstoffen-beheer**	Alleen als afvalstoffenbeheer de voornaamste economische activiteit is	Belangrijk	Belangrijk	Niet van toepassing
Minister van Landbouw, Natuur en Voedselkwaliteit	**Levensmiddelen**	Groothandelsproductie, industriële productie, verwerking	Belangrijk	Belangrijk	Niet van toepassing
Minister van Infrastructuur en Waterstaat	**Chemische stoffen**	Vervaardiging, productie, distributie	Belangrijk	Belangrijk	Niet van toepassing

Bevoegde autoriteit	Sector	Subsector	*Grote organisaties*	*Middelgrote organisaties*	*Kleine- en micro-organisaties*
Nader te bepalen	**Onderzoek**	Onderzoeksinstellingen (met uitzondering van onderwijsinstellingen)	**Belangrijk**	**Belangrijk**	**Niet van toepassing**
Minister van Economische Zaken en Klimaat	**Vervaardiging**	(in-vitro diagnostische) medische apparaten; computer-, elektronische optische producten; elektrische apparatuur; machines; motorvoertuigen, aanhangwagens, opleggers	**Belangrijk**	**Belangrijk**	**Niet van toepassing**

Bijlage 3 Overzicht

Zeer kritieke sectoren	Grote organisaties	Middelgrote organisaties	Kleine- en micro-organisaties
Energie	✓	✓	✗
Transport	✓	✓	✗
Bankwezen	✓	✓	✗
Infrastructuur financiële markt	✓	✓	✗
Gezondheidszorg	✓	✓	✗
Drinkwater	✓	✓	✗
Digitale infrastructuur	✓	✓	✗
Beheerders van ICT-diensten	✓	✓	✓ ✗ *Afhankelijk van subcategorie*
Afvalwater	✓	✓	✗
Overheidsdiensten	✓	✓	✓
Lokale overheden	✓	✓	✓
Ruimtevaart	✓	✓	✗

	Werknemers		Jaaromzet		Balanstotaal
Grote organisaties	= > 250	*of*	> 50 mln	+	> 43 mln
Middelgrote organisaties	= > 50	*of*	> 10 mln	+	> 10 mln

Andere kritieke sectoren	Grote organisaties	Middelgrote organisaties	Kleine- en micro-organisaties
Digitale aanbieders	✓	✓	✗
Post- en koeriersdiensten	✓	✓	✗
Afvalstoffenbeheer	✓	✓	✗
Levensmiddelen	✓	✓	✗
Chemische stoffen	✓	✓	✗
Onderzoek	✓	✓	✗
Vervaardiging	✓	✓	✗

Legenda

- ✓ Essentiële entiteit
- ✓ Belangrijke entiteit
- ✗ Niet van toepassing