Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Veilig verbonden. Klaar voor morgen.

100 jaar RDI

Meerjarenplan 2027-2031

Meerjarenplan RDI 2027-2031

Toekomstgericht voor een veilig verbonden Nederland

In 2027 vieren we dat we al 100 jaar veilig verbonden zijn. Een eeuw waarin technologie en samenleving voortdurend veranderden en de mensen van de RDI steeds opnieuw meebewogen met de ontwikkelingen van hun tijd. Ook de komende jaren zullen technologische, maatschappelijke en geopolitieke ontwikkelingen van invloed zijn op de digitale infrastructuur en onze opgave.

De digitale infrastructuur is van groot belang voor onze samenleving en economie. Technologische ontwikkelingen volgen elkaar in hoog tempo op en geopolitieke verhoudingen verschuiven. Wat eerder vanzelfsprekend leek, is dat nu steeds minder. Ook de maatschappelijke verwachtingen en wettelijke eisen nemen toe. Europese en nationale wetgeving brengt nieuwe verantwoordelijkheden voor de RDI met zich mee. Dit vraagt om passende kennis en capaciteit maar ook om een intensievere samenwerking met stakeholders.

De digitale infrastructuur wordt bovendien steeds complexer. Er ontstaan meer vervlochten ecosystemen en ketenafhankelijkheden, waardoor ontwikkelingen in de ene sector gevolgen kunnen hebben voor andere sectoren. Ook maatschappelijke, geopolitieke en technologische ontwikkelingen grijpen steeds meer op elkaar in. Daarmee wordt het belangrijker om ontwikkelingen in samenhang te bezien en risico's, voor de verschillende ketens en het systeem als geheel, vroegtijdig te signaleren.
In deze veranderende context werkt de RDI aan beschikbaarheid, continuïteit, en betrouwbaarheid van de digitale infrastructuur. Zodat iedereen kan vertrouwen op een veilige werking ervan, zowel in Europa als Caribisch Nederland. We kijken vooruit naar de ontwikkelingen die de komende jaren van invloed zijn op onze opgave en onze inzet. Daarbij is de samenwerking met collega-toezichthouders, ministeries en andere partners in binnen- en buitenland essentieel.

In dit compacte plan vindt u de kern van onze inzet terug. We bouwen daarmee in 2027 voort op de koers die we de afgelopen jaren in onze meerjarenplannen hebben uitgezet.

Hoofdstuk 1

Wat zien we op ons afkomen?

Een belangrijk onderdeel van ons werk als rijksinspectie is het signaleren van ontwikkelingen in de digitale infrastructuur. Deze informatie helpt ons om vooruit te kijken, risico's vroegtijdig te signaleren, de context te zien waarin we werken en de betekenis van ontwikkelingen voor onze toezichtopgave te duiden. Eén van de manieren waarop we dat doen, is de driejaarlijkse Trendradar. Deze hebben we dit jaar weer samen met stakeholders gemaakt. Vijf ontwikkelingen springen in het oog.

1 - Geopolitieke spanningen en een fragmenterende wereldorde

De digitale infrastructuur wordt steeds vaker ingezet als strategisch machtsinstrument. Hybride dreigingen, zoals het verstoren van communicatiesignalen door jamming van het frequentiespectrum of sabotage van fysieke infrastructuur, vormen een toenemend risico. De toenemende afhankelijkheid van internationale ketens vraagt om een proactieve benadering samen met ketenpartners. De RDI richt zich hierbij op de weerbaarheid van vitale onderdelen van de digitale infrastructuur, zoals hacking van vitale infrastructuur, beperkte frequentieruimte en satellietcommunicatie. Daarnaast versterken we de samenwerking met (inter)nationale partners en ontwikkelen we zogenaamde grijze fase scenario's om als rijksinspectie beter te kunnen anticiperen op de onvoorspelbaarheid van de hybride dreigingen.

2 - Verschuiving van wetgeving naar Europees niveau

Veel van de nieuwe wetgeving wordt ontwikkeld op Europees niveau. Denk hierbij aan de Cyberbeveiligingswet (Cbw), de AI-Act en de Wet weerbaarheid kritieke entiteiten (Wwke). Deze Europese wetgeving beoogt een eenduidig en hoog beveiligingsniveau binnen de Europese Unie. Dit vraagt om intensievere samenwerking – niet alleen met Europese partners, maar ook met nationale stakeholders – om de implementatie en handhaving van deze regelgeving effectief te organiseren.

3 - Disruptieve technologische ontwikkelingen

Technologische doorbraken, zoals quantum computing, ruimtenetwerken en Agentic AI, volgen elkaar in hoog tempo op. Deze ontwikkelingen brengen nieuwe kansen, maar ook risico's met zich mee. De RDI bereidt zich hier bijvoorbeeld op voor door expertise verder uit te bouwen op gebieden als satellietcommunicatie en toekomstbestendig frequentiebeheer. De RDI zet in op flexibele en toekomstgerichte kaders, waarbij het anticiperen op wet- en regelgeving een centrale rol speelt.

4 - Complexiteit van het digitale domein

Het digitale domein kenmerkt zich door toenemende complexiteit, met sterk vervlochten ecosystemen en onderlinge afhankelijkheden binnen ketens. Om het toezicht hierop doeltreffend en uitvoerbaar te houden, is intensieve netwerksamenwerking onmisbaar. Dit vraagt om afstemming tussen toezichthouders onderling en met vertegenwoordigers uit de sectoren.

5 - Publieke belangen onder druk

De afhankelijkheid van digitale infrastructuur neemt toe door het groeiende aantal toeleveranciers van cruciale elementen én de toenemende integratie van systemen, processen en apparaten in het dagelijks leven. Een bijkomende complicatie is de hoge omloopsnelheid en ongecontroleerde import (e-commerce) van digitale producten, waarbij commercieel verkrijgbare producten eenvoudig in kritische omgevingen gebruikt kunnen worden. Ook de gevolgen van (het ontbreken van) software-updates op de veilige werking van producten voegen extra complexiteit toe aan het stelsel.

Wat betekent dit voor onze toezichtsopgave?

Zowel de bovenstaande ontwikkelingen als de komende hoofdstukken laten zien dat de toezichtsopgave van de RDI steeds complexer en dynamischer wordt. Risico's kunnen zich snel ontwikkelen, grenzen tussen sectoren vervagen en afhankelijkheden in ketens kunnen gevolgen hebben voor de digitale infrastructuur en de samenleving. Met de toezichtcapaciteit die er is, wordt van ons verwacht dat we een complexer en dynamischer digitaal domein overzien. Een meer adaptieve en risicogerichte benadering van toezicht is daarom noodzakelijk.

De RDI werkt risico gestuurd en kijkt daarbij naar de maatschappelijke impact van risico's. Dat vraagt om kennis van ontwikkelingen in de digitale infrastructuur, om nieuwe en veranderende risico's te kunnen duiden en om een toezichtaanpak die kan meebewegen met de ontwikkelingen. Daarom werken we aan risicoanalyses, signaleren we ontwikkelingen met de Trendradar en organiseren we expertsessies. In de komende jaren gaan we het informatiegericht en risico gestuurd werken verder uitbouwen en uniformeren. Naast het verbeteren van landelijke samenwerkingen, wordt vanuit de rijksbrede taakstellingen ook gestreefd naar efficiënter werken tussen toezichthouders. Scherper risico-gestuurd werken gaat ons helpen om afwegingen en keuzes te maken binnen onze toezichtsopgave. Dit vraagt ook om het accepteren van maatschappelijke risico's.

De opgave voor onze organisatie reikt nog verder. Het zijn van een betrouwbare rijksinspectie vraagt om een organisatie die inrichtingsbepalende wet- en regelgeving blijvend waarborgt en aansluit bij de behoeften en verwachtingen van de samenleving door voorspelbaar en transparant te zijn, over het uitvoeren van haar toezichtsopgave. Bijvoorbeeld een veilige, betrouwbare en toekomstbestendige IV-huishouding, maar ook signaalmanagement om maatschappelijke vraagstukken te adresseren en effectief te blijven richting burgers en bedrijven. Dat vraagt niet alleen om investeringen in systemen en processen, maar ook de nodige capaciteit, prioritering en het maken van keuzes qua interne sturing.

Bovenal vraagt het ook om samenwerking. Met collega-toezichthouders, ministeries, brancheorganisaties en andere partners in binnen- en buitenland. Nieuwe technologie en veranderende wet- en regelgeving vragen daarnaast om kennis en expertise die met de ontwikkelingen meegroeien.

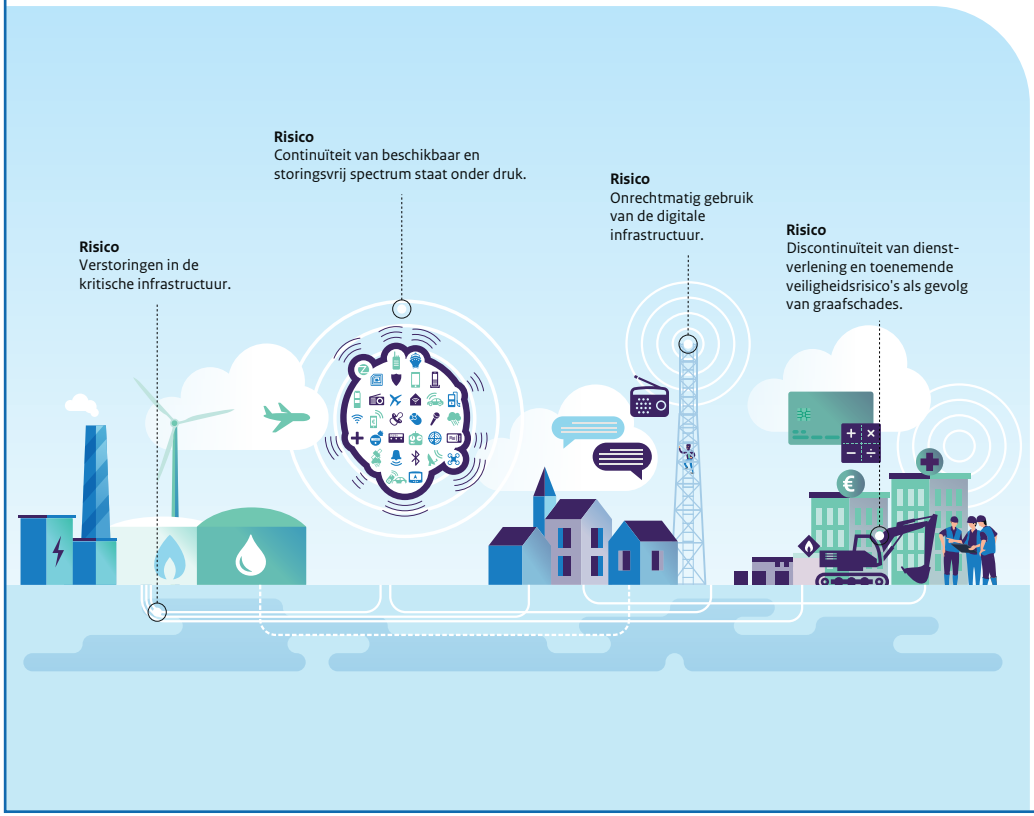
Hoofdstuk 2

Zo houden we de infrastructuur beschikbaar

Wat is onze maatschappelijke opgave?

De Nederlandse samenleving rekent op een hoogwaardige analoge en digitale infrastructuur. De RDI waarborgt beschikbaarheid door schaarse middelen zoals frequentieruimte zorgvuldig te verdelen, graafschade te voorkomen en internationale afstemming te organiseren. Op deze wijze bevordert en beschermt de RDI de beschikbaarheid van draadloze en draad gebonden netwerken en de goede werking ervan.

Wat zien we?



Wat zijn onze doelen voor 2027-2031?

- Een veilige en storingsvrije digitale infrastructuur, door expertise en afspraken te versterken, met name voor counterdrone-maatregelen.
- Toekomstbestendig frequentiebeheer, door middel van innovatie en kennisopbouw, zoals in ons 6G-lab.
- Het opvangen van risico's van verstorende technologieën, door het houden van toezicht op satellieten en drones.
- Een zo zorgvuldig mogelijke uitvoering van de aanleg van kabels en leidingen in de Nederlandse ondergrond, in het kader van de energietransitie en aanleg van glasvezel, met zo min mogelijk impact op de beschikbaarheid van netwerken.

Aan welke resultaten werken we in 2027?

- Nederland beschikt over voldoende frequentieruimte, die verdeeld is naar gebruikers en gebruikstoepassingen.
- De verdeelde frequentierechten zijn beschermd en de voorwaarden die aan de rechten zijn verbonden worden nageleefd.
- Toegenomen veiligheid van mensen, omgeving en leveringszekerheid van essentiële diensten, door toezicht op het veilig en zorgvuldig uitvoeren van graafwerkzaamheden.

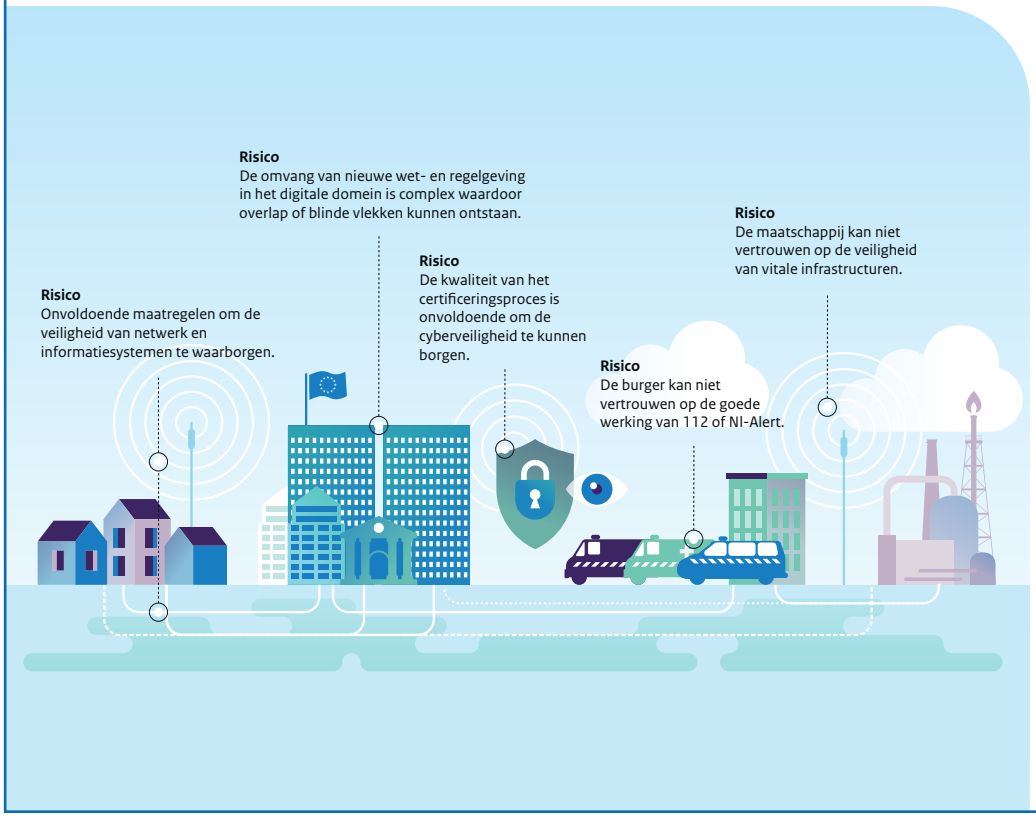
Hoofdstuk 3

Zo houden we netwerken en diensten betrouwbaar

Wat is onze maatschappelijke opgave?

Burgers en bedrijven moeten erop kunnen vertrouwen dat de Nederlandse digitale infrastructuur werkt, betrouwbaar is en beschermd wordt. De RDI ziet erop toe dat vitale sectoren zoals telecom en energie maatregelen nemen om hun digitale weerbaarheid op orde te krijgen en te houden. Cyberaanvallen zijn niet te voorkomen en iedere aanval heeft impact. We stimuleren bedrijven en overheden om hun digitale weerbaarheid op orde te brengen en te houden. Twee vragen die daarbij helpen: hoe voorkom je dat het misgaat en wat heb je geregeld als het toch misgaat?

Wat zien we?



Wat zijn onze doelen voor 2027-2031?

- Een gecertificeerd stelsel van digitale producten, diensten en processen, door dit stelsel te borgen.
- Een betrouwbare keten voor digitale identificatie en authenticatie, door deze te bewaken.
- Bewaken van de weerbaarheid van vitale en essentiële dienstverleners van infrastructuur in de domeinen overheid, telecom, internet en energie, en van belangrijke (digitale) dienstverleners, zoals cloudcomputerdiensten en online marktplaatsen.
- Inzicht in nieuwe trends en risico's in de digitale infrastructuur en bewustwording bij maatschappij en stakeholders. Dit doen we door trends en risico's te onderzoeken en signaleren en de maatschappij en stakeholders, zoals beleidsmakers, bedrijven en gebruikers, hierover te informeren.
- Een digitaal weerbare maatschappij, door de maatschappij te informeren over het belang van de eigen digitale weerbaarheid, ten aanzien van de restrisico's die er altijd zijn.

Aan welke resultaten werken we in 2027?

- Een gedegen beeld van de mate van digitale weerbaarheid van de relevante sectoren om gericht te kunnen inzetten op stimulering van intrinsieke naleving door guidance te bieden of handhavend op te treden.
- Partijen en diensten zijn na een toelatingstoets toegelaten tot de relevante stelsels.
- Bijdragen aan ontwikkeling en beheer van (Europese) certificeringsschema's en de processen rond standaardisatie in cybersecurity en digitalisering.

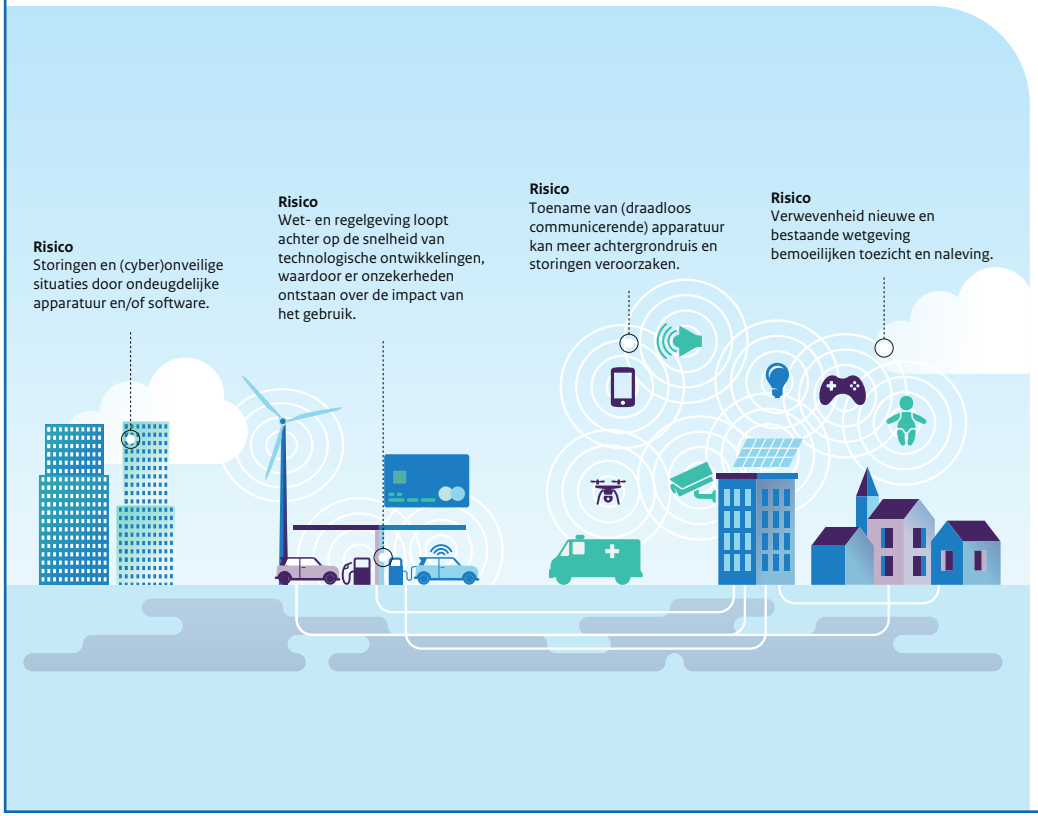
Hoofdstuk 4

Zo kan iedereen vertrouwen op apparaten en digitale producten

Wat is onze maatschappelijke opgave?

Nederland moet kunnen vertrouwen op veilige en betrouwbare producten die volgens geldende regelgeving in de handel zijn gebracht. De veiligheid en betrouwbaarheid van deze digitale producten omvatten fysieke componenten zoals de software, data, cloud- en andere digitale diensten én de omgeving waarin deze producten worden gebruikt.

Wat zien we?



Wat zijn onze doelen voor 2027-2031?

- Implementatie van ons toezicht op de Cyber Resilience Act, AI Act en de Energie Meter Wissel.
- Intensivering van markttoezicht door samen te werken met Douane en andere toezichthouders bij het toezicht aan de grens en het toezicht op e-commerce platformen.
- Innovatie in toezichtsmethoden, zoals webcrawling en data gedreven werken.
- Tijdige signalering en agendering van trends voor toekomstig toezicht.

Aan welke resultaten werken we in 2027?

- Actieve deelname aan productstandaardisatie gremia, om vanuit het publieke belang betekenis te geven aan algemene wet- en regelgeving, voor veilige producten.
- Non-conforme producten worden effectief opgespoord. Storingen worden onderzocht en weggenomen.
- Wij dragen bij aan het ontwerp en de toekomstige invoering van het digitaal productpaspoort.

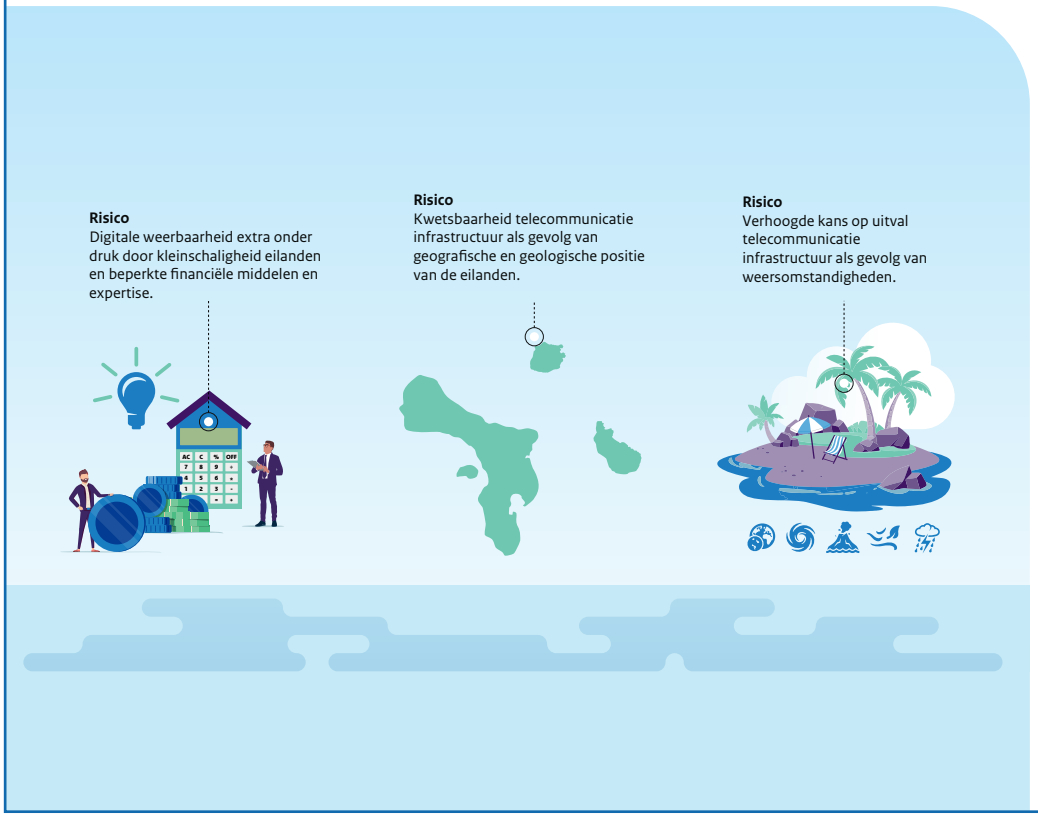
Hoofdstuk 5

Zo zorgen we voor een veilig verbonden Caribisch Nederland

Wat is onze maatschappelijke opgave?

De digitale transitie voor Caribisch Nederland vraagt van ons dat we vanuit onze maatschappelijke verantwoordelijkheid de beschikbaarheid van netwerken bevorderen en beschermen, het storingvrij gebruik van radioapparaten bevorderen en bijdragen aan de continuïteit en integriteit van netwerken. Daarmee geven wij uitvoering aan de maatschappelijke opgave die voortvloeit uit de Wet telecommunicatievoorzieningen BES (Bonaire, Sint-Eustatius en Saba) en onderliggende regelgeving. Zo zorgen wij voor een veilig verbonden Caribisch Nederland.

Wat zien we?



Wat zijn onze doelen voor 2027-2031?

- Storingsvrij frequentiegebruik, door storingen veroorzaakt door producten te onderzoeken en daar waar mogelijk weg te nemen.
- Actieve samenwerking met andere toezichthouders, uitvoeringsorganisaties en andere stakeholders van en voor Caribisch Nederland, door zowel nationaal als internationaal samen te werken.
- Continuïteit en integriteit van de digitale infrastructuur, door concessiehouders passende maatregelen te laten nemen om deze te waarborgen.

Aan welke resultaten werken we in 2027?

- Caribisch Nederland beschikt over voldoende, beschermde frequentieruimte, die verdeeld is naar gebruikers en gebruikstoepassingen.
- Telecomoperators hebben passende maatregelen getroffen in het kader van beschikbaarheid, authenticiteit, vertrouwelijkheid en integriteit en we hebben een goed beeld van de mate van naleving.
- Caribisch Nederland kan storingsvrij gebruik maken van netwerken en apparaten.
- De RDI onderzoekt samen met het ministerie van Economische Zaken en Klimaat en de Autoriteit Consument & Markt (ACM) waar de bestaande telecomwetgeving moet worden vernieuwd om zo beter aan te sluiten bij de huidige ontwikkelingen.

Dit is een uitgave van
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Emmasingel 1 Groningen
088 - 041 60 00
info@rdi.nl
www.rdi.nl

Oktober 2026

#wijzijnRDI