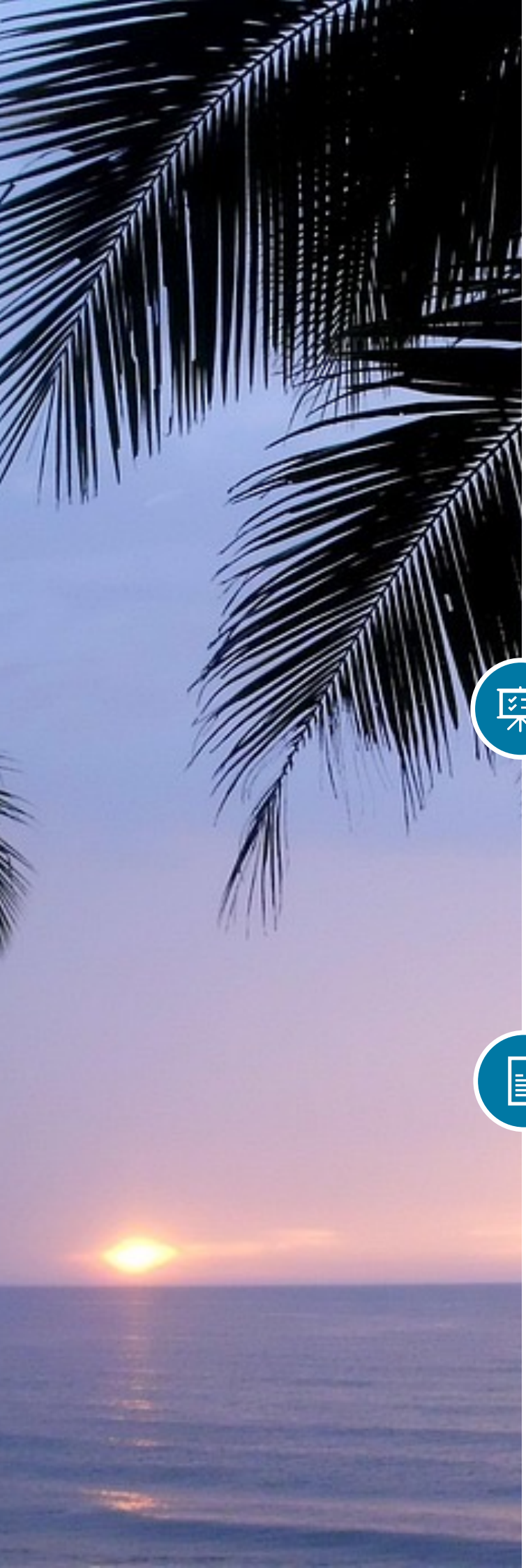
Advies datacenterstrategie Caribisch Nederland

November 2025

Opgesteld door:
Highberg, in samenwerking met vertegenwoordiging vanuit CIO-Office RCN, CIO Rijk, BZK, SSO-CN, RCN, OL Bonaire, OL Sint Eustatius, OL Saba, Belastingdienst CN, en op basis van interviews met ODC's, Logius, EZ, SBIR, SZW, RVB, VWS, KPCN, IND, SSC-ICT, RvIG, Kmar, Belastingdienst CN, huidige leveranciers (Netvision, Flamingo TV).



Inhoudsopgave

In dit rapport zijn twee afzonderlijke secties opgenomen om zowel de bestuurlijke als de inhoudelijke behoefte te ondersteunen. Deze opzet maakt het mogelijk om in één document zowel een overzicht op hoofdlijnen te bieden als de noodzakelijke verdieping en onderbouwing te waarborgen. Daarmee sluit de structuur aan bij verschillende doelgroepen.

Sectie 1 – SAMENVATTING

Deze sectie biedt een uitgebreide samenvatting van het advies voor de datacenterstrategie voor de overheid in Caribisch Nederland, met koppeling aan de Nederlandse Digitaliseringsstrategie (NDS). De sectie belicht de uitgangssituatie, de strategische richting, de kernargumenten en de keuzes.

Sectie 2 – RAPPORT (pagina 16 e.v.)

Voor nadere onderbouwing, context en technische details is in deze sectie het volledige rapport Analyse en uitwerking advies datacenterstrategie overheid Caribisch Nederland, inclusief bijlagen, opgenomen.

Samenvatting

Sectie 1

HIGHBERG

Datacenterstrategie Caribisch Nederland

In opdracht van Ministerie van Binnenlandse Zaken en Koninkrijkrelaties

De digitale infrastructuur van de overheid in Caribisch Nederland is versnipperd, kwetsbaar en onvoldoende voorbereid op toekomstige eisen ten aanzien van digitale dienstverlening aan burgers en bedrijven. Zonder ingrijpen dreigt uitval, verlies van regie en blijvende afhankelijkheid van buitenlandse partijen. De bestaande faciliteiten van RCN zijn weliswaar professioneel en up-to-date, maar door schaal en locatie alleen niet toereikend voor de lange termijn. De voorgestelde datacenterstrategie in dit document kiest daarom bewust voor een parallelle aanpak: realisatie van een twin-datacenterstructuur op Bonaire, Sint Eustatius en Saba én een rechtstreekse koppeling met een Overheidsdatacenter (ODC) in Europees Nederland.

Door deze combinatie ontstaat lokaal redundantie, beschikbaarheid en schaalbaarheid, waarmee burgers, bedrijven en lokale overheden kunnen rekenen op veilige en stabiele dienstverlening. Tegelijkertijd waarborgt de koppeling met Europees Nederland structurele uitwijk, centrale ondersteuning, naleving van wet- en regelgeving, en versterking van publieke waarden zoals digitale soevereiniteit, compliance en continuïteit.

De voordelen zijn: hogere weerbaarheid tegen storingen en geopolitieke risico's, versterkte samenwerking tussen eilanden en Rijk, en aansluiting op de Nederlandse Digitaliseringsstrategie. Voor duurzame borging zijn nu duidelijke besluiten nodig over governance, financiering en uitvoering.

Digitale weerbaarheid van de overheid in Caribisch Nederland

De datacenterstrategie voor Caribisch Nederland vormt een onderbouwing en richtinggevend kader voor de versterking van de digitale infrastructuur in Caribisch Nederland. De noodzaak voor een structurele oplossing is urgent en breed gedragen onder stakeholders, waaronder de Rijksoverheid, de openbare lichamen van Bonaire, Sint Eustatius en Saba (de OL'en), de uitvoerende diensten en ZBO's en departementale beleidsdirecties. De Openbare Lichamen benoemen hierbij tevens het belang van de (semi-) overheidsorganisaties met een publiek belang. Dit rapport maakt inzichtelijk waarom een gezamenlijke aanpak noodzakelijk is, welke varianten onderzocht zijn, wat de implicaties zijn voor wet- en regelgeving, en welke keuzes op korte termijn vereist zijn.

Noodzaak tot actie

De digitale infrastructuur in Caribisch Nederland is de afgelopen jaren verder geprofessionaliseerd, maar blijft in schaal en capaciteit beperkt. Met de recente besluitvorming over de nieuwe zeekabel tussen Aruba en Bonaire wordt nu wel een belangrijke stap gezet richting structurele versterking van de connectiviteit en routediversiteit. Tegelijkertijd is sprake van een stapeling van strategische belangen. Overheidsdatacenters (ODC's) in Europees Nederland zoeken geografisch gespreide uitwijklocaties. Voor Defensie is het strategisch van belang om operationele capaciteit in de regio op te bouwen en het gebruik van datacenters op de BES-eilanden te verkennen (bijv. voor back-up). De openbare lichamen op Bonaire, Sint Eustatius en Saba worstelen met structurele knelpunten in hun digitale ondersteuning. Deze strategie biedt een samenhangend beleidsmatig en technisch kader om deze belangen te verbinden en gezamenlijk tot een toekomstbestendige digitale infrastructuur van de overheid te komen, in lijn met de zes prioriteiten van de Nederlandse Digitaliseringsstrategie (NDS).

Eén digitale overheid

Burgers en bedrijven moeten kunnen rekenen op veilige, betrouwbare en continue digitale overheidsdiensten. Zonder robuuste infrastructuur dreigt uitval, zijn gegevens kwetsbaar en komt het vertrouwen in de overheid onder druk te staan. De datacenterstrategie beoogt dat risico weg te nemen en richt zich nadrukkelijk niet alleen op de rijksoverheid, maar ook op de openbare lichamen van Bonaire, Sint Eustatius en Saba, evenals semi-overheden, ZBO's en uitvoeringsdiensten. Deze organisaties hebben een stabiele digitale basis nodig om hun wettelijke taken uit te voeren, maar blijken daar in de praktijk vaak niet zelfstandig toe in staat. Uit de DigiD Pre-Check blijkt bijvoorbeeld dat de criteria voor basisvoorzieningen zoals DigiD regelmatig niet worden gehaald. Bovendien leidt de sterke afhankelijkheid van externe leveranciers tot kwetsbaarheden in continuïteit, beveiliging en regie. De strategie voorziet daarom in gedeeld gebruik, schaalbaarheid, beheerbaarheid en duidelijke segmentatie op vertrouwelijkheidsniveau, zodat één toekomstbestendige digitale overheid ontstaat.

Digitale realiteit van de overheid in Caribisch Nederland

De digitale realiteit in Caribisch Nederland is versnipperd: meerdere overheden en organisaties werken zonder centrale regie, met kleinschalige en deels verouderde datacenterfaciliteiten. De aanleg van de nieuwe zeekabel tussen Aruba en Bonaire verbetert de connectiviteit, maar digitale autonomie en schaalbaarheid blijven beperkt, terwijl ad-hoc cloudgebruik publieke waarden onvoldoende borgt..

Fragmentatie en gebrek aan regie

De digitale inrichting in Caribisch Nederland is versnipperd en maakt nog nauwelijks gebruik van beschikbare voorzieningen en bouwstenen uit Europees Nederland. Het Rijk is vertegenwoordigd via RCN, terwijl de Openbare Lichamen beschikken over eigen IT-structuren en geen toegang hebben tot de voorzieningen van RCN. Semi-overheden, zoals zorginstellingen en nutsbedrijven, gebruiken commerciële IT-diensten zonder centrale coördinatie. Er is geen gezamenlijk beleid, geen gedeelde infrastructuurplanning en geen structurele afstemming. Dit ondermijnt het NDS-principe van een "samenhangende digitale overheid" en belemmert de ontwikkeling van collectieve voorzieningen.

Kwetsbare datacenterstructuur

Er is een Rijksdatacenterfaciliteit op Bonaire, deze is onlangs gemoderniseerd. Echter uitbreiding binnen de huidige faciliteiten en realisatie van fysiek gescheiden omgevingen is niet mogelijk, het DC voldoet niet aan Tier III-normen. Het tweede datacenter, bij Flamingo TV, is niet in publiek eigendom, kleinschalig en ligt ook op Bonaire. Saba en Sint Eustatius beschikken slechts over beperkte serverruimtes met minimale voorzieningen; samenwerking met commerciële telecomaanbieders wordt actief verkend. Er is geen structurele uitwijkcapaciteit voor Saba en Sint Eustatius. RCN heeft uitwijk op Bonaire. Deze situatie maakt de continuïteit van publieke dienstverlening kwetsbaar door het ontbreken van een robuuste en redundante infrastructuur.

Gebrek aan digitale autonomie

In Caribisch Nederland verlopen verbindingen voor overheidsdienstverlening via infrastructuur in andere landen, grotendeels via de VS. Meer routediversiteit en redundantie zijn nodig om de betrouwbaarheid te vergroten, in lijn met de NDS die inzet op digitale autonomie en weerbaarheid.

Groeiende belasting

De digitale vraag vanuit (semi-)overheidsdiensten en inwoners groeit. De huidige netwerkinfrastructuur van de overheid biedt onvoldoende snelheid. De sterke afhankelijkheid van een enkele IP-transitprovider beperkt de gewenste routediversiteit en redundantie. Dit belemmert een toekomstbestendige, overheidsbrede informatievoorziening tussen Caribisch en Europees Nederland.

Ad-hoc cloudgebruik zonder borging van publieke waarden

Commerciële clouddiensten worden ingezet, maar er ontbreken centrale richtlijnen voor dataveiligheid, eigenaarschap en toezicht. SSO-CN biedt geen ondersteuning buiten de Rijksoverheid en lokale expertise is beperkt. Er is geen formele regie op cloudgebruik. Hierdoor zijn publieke waarden als transparantie, soevereiniteit, autonomie en rechtmatigheid onvoldoende geborgd.

Stakeholderbehoeften als fundament voor de datacenterstrategie van de overheid

De datacenterstrategie voor de overheid in Caribisch Nederland speelt in op uiteenlopende belangen van betrokken stakeholders. Overheden willen zeggenschap, flexibiliteit en continuïteit van dienstverlening. Aansluiting op centrale netwerken is essentieel, evenals het voldoen aan strikte beveiligingsnormen. Sturing is van belang op compliance, standaardisatie en kostenbeheersing. Terwijl burgers en bedrijven snelheid, betrouwbaarheid en gegevensbescherming verwachten. Wat hen bindt, is de behoefte aan een robuuste en toekomstbestendige digitale infrastructuur van de overheid.

De oplossing ligt in een modulaire opzet van dienstverlening. Alleen met een modulaire architectuur kan voldaan worden aan de behoefte aan zowel standaardisatie als maatwerk. Zo kunnen centrale, generieke diensten (zoals opslag, hosting, netwerkconnectiviteit en security van de overheid) gedeeld worden, terwijl specifieke componenten (zoals lokale e-loketten of latencygevoelige toepassingen) decentraal en op maat ingericht kunnen worden. Dit voorkomt dat iedereen in hetzelfde keurslijf moet opereren, terwijl er toch schaalvoordeel, veiligheid en regie behouden blijft.

Deze benadering is volledig in lijn met de uitgangspunten van de Nederlandse Digitaliseringsstrategie (NDS). De NDS stelt dat digitale overheidsvoorzieningen moeten worden ingericht op basis van collectieve bouwstenen, hergebruik van ontwikkelde oplossingen en een gezamenlijke architectuur. Door modulariteit, herbruikbaarheid en interoperabiliteit te waarborgen, kan de overheid als één geheel opereren en adaptief, wendbaar en toekomstbestendig blijven. Daarbij hoort ook het zorgvuldig organiseren van governance en gegevensbescherming, met oog voor zowel lokale autonomie als centrale regie. De NDS schrijft voor dat digitale voorzieningen onder nationale standaarden en een gezamenlijke architectuur vallen, met ruimte voor verschillen in adoptietempo tussen organisaties.

De datacenterstrategie doet recht aan het feit dat Caribisch Nederland formeel onderdeel is van Nederland. Dat vraagt om digitale gelijkwaardigheid, zonder overbelasting van de lokale capaciteit. De inzet op modulaire dienstverlening, gekoppeld aan duidelijke sturing en aansluiting op generieke infrastructuur, is de enige reële manier om dat duurzaam en bestuurbaar te realiseren.

> ***“Er is veel meer nodig dan alleen een werkende DigiD-koppeling; zonder structurele ontwikkeling van de infrastructuur met BBN-segmentatie en modulaire dienstverlening voor álle betrokken overheden in Caribisch Nederland blijft digitale dienstverlening ontoereikend”***
>
> *Werkgroep Datacenterstrategie Caribisch Nederland*

Formulering strategische uitgangspunten

De datacenterstrategie voor de overheid in Caribisch Nederland biedt een juridisch verantwoorde, veilige en toekomstbestendige digitale infrastructuur, gebaseerd op de Nederlandse Digitaliseringsstrategie en de BIO-normen (BBN). De strategie adresseert in een veranderende geopolitieke context mogelijke risico's door digitale soevereiniteit te versterken, afhankelijkheid van buitenlandse partijen te beperken (waar mogelijk en relevant) en robuuste, redundante verbindingen te realiseren. Daarmee wordt weerbaarheid vergroot, lokaal vakmanschap gestimuleerd en aansluiting op overheidsvoorzieningen geborgd. Acht strategische uitgangspunten en technische randvoorwaarden, geformuleerd in overleg met de direct betrokken stakeholders vanuit de overheid, vormen het toetsingskader; afwijkingen brengen risico's voor compliance, continuïteit en regie. De netwerkarchitectuur van de overheid waarborgt voorspelbare latency en gescheiden routes voor stabiele, betrouwbare dienstverlening.

EU-regelgeving als leidraad

Ondanks afwijkende wetgeving is aansluiting op AVG-niveau noodzakelijk om ketenkoppelingen met Europees NL mogelijk, rechtmatig en veilig te houden binnen EU-compliant systemen.

Beveiliging volgens cybersecuritystelsel

De infrastructuur voldoet aantoonbaar aan BIO 2 en DigiD normen, is voorbereid op NIS2-wetgeving en borgt BBN2/BBN3 via SOC/CERT, monitoring en toetsbare normen.

Digitale soevereiniteit

Data blijft volledig onder Nederlandse of EU-regie; afhankelijkheid van infrastructuur onder niet-EU wetgeving wordt uitgesloten.

Context Caribisch Nederland

Datacentervoorzieningen zijn schaalbaar en lokaal uitvoerbaar, afgestemd op de specifieke context van Caribisch Nederland, met geborgde belangen en respect voor bestuurlijke autonomie.

Aansluiten op beleid

De strategie sluit aan op de NDS, de Generieke Digitale Infrastructuur en sluit aan op overheidsstandaarden.

Weerbaarheid en continuïteit

De infrastructuur weerstaat calamiteiten en cyberincidenten via redundantie, offline-back-ups en herstel, afgestemd op BBN-classificaties.

Ontwikkelkracht en capaciteit CN

De strategie kiest voor schaalbare, lokaal uitvoerbare infrastructuur met mogelijke ondersteuning op afstand, zonder blijvende afhankelijkheid van schaars gespecialiseerd personeel.

Centrale regie en duidelijke afspraken

Sturing en aanspreekbaarheid over bestuurslagen en partijen heen worden geborgd door centrale regie en heldere afspraken, ter voorkoming van versnippering. De noodzaak van één centrale digitale overheid (NDS).

Strategische koersbepaling datacenter tbv de overheid in Caribisch Nederland

10 varianten voor een robuuste digitale infrastructuur in Caribisch Nederland

De digitale infrastructuur van de overheid in Caribisch Nederland moet grondig worden herzien. Het CIO-Office RCN en SSO-CN hebben hierin al belangrijke stappen gezet, maar richten zich vooralsnog primair op de Rijksoverheid. Jarenlange fragmentatie in beheer, decentrale besluitvorming en het ontbreken van een gezamenlijke architectuur maken de huidige situatie onhoudbaar. Zonder integrale strategie blijven schaalvoordelen uit, ontbreekt grip op beveiliging en continuïteit, en stokt de aansluiting op overheidsbrede digitale ontwikkelingen. Deze constatering vormt het vertrekpunt voor de strategische afweging. Voortzetting van de huidige situatie (variant 0) is onwenselijk. Daarom moeten er duidelijke keuzes worden gemaakt. Er zijn tien varianten gedefinieerd.

1 **Volledig Lokaal op elk eiland**
Drie eigen datacenters, één per eiland. Lokale regie, maar zeer kostbaar, inefficiënt en kwetsbaar door beperkte schaalgrootte en gebrek aan centrale regie.

2 **Twin-datacenter binnen CN**
Datacenter zowel bovenwinds als benedenwinds. Goede continuïteit en spreiding, lokaal eigendom, maar hoge kosten en afhankelijk van stabiele verbindingen tussen de eilanden.

3 **Lokaal + edge + back-up in E-NL**
Bonaire als hoofddatacenter, edge op Saba/Sint Eustatius, back-up in Nederland. Robuust, maar technisch complex en relatief duur in beheer.

4 **Alles in E-NL, lokaal noodplatform**
Datacenter volledig in E-NL met minimale noodvoorziening op BES. Lage investering, maar onacceptabel risico bij verbindingsuitval en nauwelijks lokale regie.

5 **Private Rijkscloud**
Volledige hosting in Nederlandse overheidsdatacenters. Governance en compliance uitstekend, maar geen lokale fallback en afhankelijkheid van externe verbindingen blijft een groot risico.

6 **Volledig in Publieke Cloud (EU-regio)**
Alles draait in Europese public cloud. Schaalbaar en modern, maar afhankelijk van big tech, minder zeggenschap en kwetsbaar bij netwerkproblemen.

7 **Private Cloud bij EU dienstverlener**
Hosting bij niet-overheidsdienstverlener in EU. Juridisch iets veiliger dan public cloud, maar verbinding en afhankelijkheid blijven zwakke punten. Beperkte lokale impact.

8 **Lokale outsourcing aan marktpartij**
Datacenter in CN gerealiseerd en geëxploiteerd door commerciële partij. Stimuleert markt, maar risico op afhankelijkheid en monopoliepositie is groot.

9 **Hybride per applicatie**
Geen centrale keuze, mix van lokaal, cloud en outsourcing per toepassing. Flexibel maar zeer complex en moeilijk bestuurbaar zonder stevige regie.

10 **Twin-Datacenter CN en E-NL**
Eén datacenter op Bonaire, één in E-NL. Sterke continuïteit, compliance en regie. Wel uitbreiding nodig voor Saba/Sint Eustatius voor volledige dekking.

Toekomstbestendige datacentervoorziening Voor Caribisch Nederland

Analyse van 3 kansrijke varianten uit 10 strategische opties

Beleidskader en noodzakelijke afweging
De inrichting van een toekomstbestendige datacenterstrategie voor Caribisch Nederland vereist een strategische keuze die recht doet aan de eisen van continuïteit, bestuurbaarheid, compliance en aansluiting op het Nederlandse overheidsbeleid. Uit de analyse van tien varianten blijkt dat zeven opties structureel tekortschieten als basis. Ze voldoen niet aan de gestelde uitgangspunten of zijn technisch, organisatorisch of juridisch onhaalbaar. Slechts drie varianten blijven overeind: variant 1 (lokale datacenters per eiland), variant 2 (twin-datacenter binnen CN) en variant 10 (twin-datacenter tussen CN en E-NL (Europees Nederland)).

Afwijzing van variant 1
Variant 1 biedt ruimte voor eigen keuzes naast centrale besluitvorming., maar kent structurele tekortkomingen. De investerings- en beheerkosten zijn disproportioneel, de personele haalbaarheid is onvoldoende en de governance versnipperd. Deze variant is niet schaalbaar en sluit onvoldoende aan op het streven naar één overheidsbrede datacenterstrategie. Vanuit bestuurlijk perspectief is dit geen houdbare optie.

Variant 2 als logische start
Variant 2 biedt een werkbare opzet op korte termijn. Door gebruik te maken van bestaande datacentercapaciteit op Bonaire en deze uit te breiden met een tweede (orkaanbestendige) locatie op Sint Eustatius of Saba (tbv zowel St. Eustatius als Saba) ontstaat een lokale beschikbaarheid. Dit model versterkt de samenwerking tussen de eilanden en maakt snelle realisatie mogelijk, mits wordt voorzien in heldere governance en afspraken over rolverdeling. Variant 2 is daarmee beleidsmatig verdedigbaar als initiële stap. Om doorgroei-mogelijkheden en hogere BBN-niveaus te kunnen ondersteunen, moet nieuwbouw van het datacenter op Bonaire worden overwogen.

Variant 10 als doelarchitectuur
Voor de middellange termijn is aanvulling met variant 10 noodzakelijk om aansluiting te vinden bij het overheidsbrede digitale ecosysteem. Deze opzet koppelt het datacenter op Bonaire en Sint Eustatius of Saba aan een overheidsdatacenter (ODC) in Europees Nederland en combineert lokale beschikbaarheid met centrale regie, schaalvoordeel en compliance. Dit scenario bevordert standaardisatie, versterkt publieke waarden en sluit het best aan bij de langetermijnambities van de Nederlandse Digitaliseringsstrategie.

Strategische richting en besluit
De combinatie van variant 2 als startmodel, uitgebreid met variant 10 tot een triple-datacenter structuur biedt een realistische en bestuurbare koers. Variant 2 maakt een snelle start mogelijk binnen de lokale context, variant 10 realiseert het groeipotentieel richting landelijke integratie. Het advies is om nu te besluiten tot de realisatie van een gecombineerde aanpak op basis van variant 2 en variant 10. Dit vraagt direct afspraken over regie, financiering en samenwerking, zodat de digitale infrastructuur voor Caribisch Nederland stapsgewijs kan worden opgebouwd tot een duurzaam, veilig en schaalbaar fundament.

Rechtstreekse verbindingen randvoorwaardelijk

De twin-datacenteropzet op Bonaire en Sint Eustatius vormt een solide basis voor de digitale infrastructuur van Caribisch Nederland. Om deze structuur toekomstbestendig te maken, wordt geadviseerd te voorzien in directe, juridisch beheersbare verbindingen tussen de eilanden en met de overheidsbrede digitale infrastructuur in Europees Nederland. Deze verbindingen dienen te voldoen aan de BIO-normen (BBN) en aanverwante standaarden voor continuïteit, veiligheid en beheersbaarheid..

Geopolitieke afhankelijkheid en compliancerisico's
Het langdurig gebruik van verbindingen via buitenlandse infrastructuur of derde landen wordt afgeraden. Dergelijke routes vallen buiten Nederlandse of Europese jurisdictie en brengen risico's mee op afluistering, manipulatie en verstoring. Encryptie biedt slechts gedeeltelijke bescherming, terwijl toekomstige ontwikkelingen zoals quantumcomputing bestaande encryptiestandaarden verder kunnen verzwakken. Vanuit het oogpunt van digitale soevereiniteit, BIO en NIS2 is het daarom wenselijk te streven naar rechtstreekse verbindingen onder Nederlands beheer.

Interinsulaire en trans-Atlantische infrastructuur
Voor de betrouwbaarheid van de digitale infrastructuur is het van belang dat zowel de interinsulaire verbindingen tussen Bonaire, Saba en Sint Eustatius als de trans-Atlantische verbinding met Europees Nederland worden versterkt. De uitbreiding van het CELIA-netwerk binnen het Koninkrijk biedt kansen om de stabiliteit tussen de eilanden te verbeteren, maar de trans-Atlantische verbinding blijft een kwetsbaar punt.

Het wordt aanbevolen om bij de verdere optimalisatie van de WAN-infrastructuur expliciet een afweging te maken tussen:
- de aanleg van nieuwe, rechtstreekse verbindingen onder Nederlands beheer, die maximale autonomie en veiligheid bieden maar aanzienlijke investeringen en een langere doorlooptijd vragen; en
- het tijdelijk benutten van bestaande kabelsystemen met gegarandeerde capaciteit en contractuele borging, die sneller uitvoerbaar en financieel haalbaarder zijn, maar afhankelijk blijven van commerciële partijen en buitenlandse jurisdictie.

Een gefaseerde, hybride benadering ligt daarbij voor de hand: benut bestaande infrastructuur op korte termijn met harde kwaliteits- en beveiligingsafspraken, terwijl op middellange termijn wordt toegewerkt naar nieuwe, rechtstreekse verbindingen onder Nederlands beheer.

Strategische kans: veilige digitale uitwijklocatie buiten Europa
Caribisch Nederland kan, als Nederlands grondgebied buiten Europa, een strategische rol vervullen als veilige digitale uitwijklocatie. Met directe, vertrouwde verbindingen wordt het mogelijk om gevoelige data, back-ups en strategische informatie vanuit Europees Nederland veilig op te slaan onder Nederlands gezag. In een tijd van geopolitieke spanningen en dreigingen op het Europese continent versterkt dit de digitale weerbaarheid van de overheid.

Oproep: structureel investeren in soevereine verbindingen
Tot slot is het raadzaam om structureel te investeren in betrouwbare, juridisch beheersbare zeekabelverbindingen. Tijdelijke benutting van bestaande infrastructuur kan de continuïteit op korte termijn ondersteunen, maar vormt geen duurzame oplossing. Alleen directe verbindingen onder Nederlands beheer kunnen de benodigde controle, beveiliging en continuïteit op de lange termijn waarborgen en zo de digitale autonomie van Caribisch Nederland daadwerkelijk veiligstellen.

Bestuurlijke regie voor digitale continuïteit in Caribisch Nederland

De uitvoering van de datacenterstrategie voor Caribisch Nederland vraagt om meer dan techniek: zonder stevige governance en heldere afspraken over rollen, zeggenschap en prioritering is deze strategie niet uitvoerbaar. Alleen als centrale en decentrale overheden samenwerken vanuit een gedeeld bestuurlijk kader dat aansluit op het Nederlandse bestuursmodel, kan de digitale infrastructuur duurzaam en bestuurbaar worden gerealiseerd. De gekozen aanpak sluit aan bij de principes van "de tafel van Thorbecke", met een duidelijke regierol voor het Ministerie van BZK en formele betrokkenheid van de stakeholders zoals ZBO's en openbare lichamen.

In deze structuur neemt SSO-CN de operationele beheerrol op zich, ondersteund door overheidsbrede partijen zoals SSC-ICT, Logius, DICTU en ODC-Noord. Hiermee ontstaat een hybride model waarin lokaal eigenaarschap en centraal vakmanschap elkaar aanvullen. Tegelijk blijft de zeggenschap over uitvoering en prioritering binnen de gestelde kaders ten aanzien van techniek en beleid bij stakeholders, zodat lokale behoeften leidend blijven. Dit is essentieel voor het draagvlak én voor het benutten van de digitale infrastructuur als aanjager van publieke dienstverlening en economische ontwikkeling.

De governance- en samenwerkings-structuur is afgestemd op de eisen rond betrouwbaarheid, beveiliging en continuïteit. Concrete afspraken via SLA's, DVO's auditing zorgen voor voorspelbare en compliance dienstverlening. Ook marktpartijen kunnen op onderdelen bijdragen, mits juridisch geborgd en zonder afbreuk te doen aan de publieke regie. Aanbestedingskaders, staatssteunregels en transparantie-eisen zijn randvoorwaardelijk.

Belangrijk is dat deze structuur wendbaar blijft. Nieuwe partijen moeten kunnen aansluiten, exit-opties moeten vooraf geregeld zijn, en taken moeten overdraagbaar zijn zonder afhankelijkheid van individuen of specifieke leveranciers. De samenwerking moet juridisch houdbaar, bestuurlijk afrekenbaar en technisch overdraagbaar zijn.

Tot slot is risicomanagement geen bijzaak, maar fundament. Capaciteitstekorten, onduidelijke taakverdeling of gebrekkige voorbereiding vormen directe bedreigingen voor de uitvoerbaarheid. Door risico's structureel te beheersen en tijdig te investeren in kennis en organisatiecapaciteit in zowel CN als E-NL, wordt de strategie toekomstbestendig.

> ***"De datacenterstrategie is alleen effectief als die aansluit bij de realiteit van Caribisch Nederland, met respect voor de lokale context, bestuurlijke verhoudingen en onderlinge verschillen."***
>
> *Werkgroep Datacenterstrategie Caribisch Nederland*

Slotbeschouwing

Noodzaak tot versnelling

De digitale infrastructuur van de overheid in Caribisch Nederland schiet tekort: gefragmenteerde, tijdelijke oplossingen ondermijnen betrouwbaarheid en kwaliteit. Zonder versnelling komt een veilige, toekomstgerichte digitale overheid (en daarmee beleid, lokale context en vertrouwen) structureel in het gedrang.

Een strategie in twee fasen

Scenario 2 en 10 vormen samen de logische keuze: een twin-datacenter in Caribisch Nederland met koppeling naar Europees Nederland. Dit levert robuustheid, schaalvoordeel en bestuurlijke grip, en maakt snelle, modulaire integratie met bestaande overheidsvoorzieningen technisch en organisatorisch haalbaar.

Digitale weerbaarheid en autonomie

Een robuuste overheidsinfrastructuur vereist veilige, directe verbindingen tussen eilanden en met Europees Nederland, zonder die ontbreekt uitwijk, wordt koppeling met overheidsnetwerken bemoeilijkt en neemt afhankelijkheid van externe routes toe. Verbetering van de zeekabels is essentieel voor digitale soevereiniteit, risicobeheersing en betrouwbare datacenterdiensten.

Governance structureel beleggen

Zonder centrale regie, juridische borging en structurele financiering stokt elke strategie. BZK moet regie voeren, met SSO-CN, CIO Rijk en Openbare Lichamen als partners. Digitale infrastructuur vereist wettelijk vastgelegd eigenaarschap en structurele middelen als publieke nutsvoorziening. Tijdelijke middelen remmen structurele voortgang.

Beheer en vakmanschap organiseren

Professioneel beheer vereist overheidsbrede ondersteuning en conforme standaarden. Beheerprocessen moeten hybride en adaptief zijn, met vanaf dag één ingebed risicomanagement. Capaciteit, verbindingen en compliance vereisen een actueel risicoregister en helder eigenaarschap van mitigerende maatregelen.

Lokale inbedding

De strategie slaagt alleen als overheden in Caribisch Nederland actief meedoen. Dat vraagt betrokkenheid bij inrichting en beheer. Maar ook zeggenschap. Rijksoverheid, lokale overheden en semi-overheden moeten structureel meedoen. Alleen dan ontstaat het draagvlak en de veerkracht voor blijvende digitale vooruitgang.

Verbinden met bredere digitalisering

De datacenterstrategie sluit aan op bredere opgaven zoals NDS, gegevensuitwisseling en netwerkveiligheid. Voor Caribisch Nederland betekent dat: aansluiten op landelijke infrastructuur, digitale inclusie versterken en investeren in lokaal vakmanschap binnen een toekomstbestendige, digitale werkomgeving.

Bestuurlijke keuze vereist doorzetting

De verkenningsfase is afgerond. Er is nu bestuurlijke conceptbesluitvorming nodig over de combinatie van scenario 2 en 10, gevolgd door programmatische uitwerking met mandatering, marktverkenning en het ontwerp van het triple-datacenter en de zeekabel. Dit vormt de basis voor het vaststellen van de planning en de benodigde financiële middelen. Na het definitieve besluit is gerichte uitvoering cruciaal om structurele voortgang te realiseren.

Besluitpunten ten behoeve van het bepalen van de benodigde financiële middelen en doorlooptijd

1 Vaststellen van de triple-datacenterstructuur als voorkeursvariant

Conceptbesluit om de digitale infrastructuur op te bouwen via logisch gekoppelde datacenters in CN, met uitwijk naar ODC-Noord in Europees Nederland. Daarmee ontstaat ook voor ODC-Noord een strategische uitwijk buiten Europees Nederland.

2 Positionering Bovenwindse Eilanden als aanvullende locatie

Conceptbesluit om Bovenwinds een strategisch tweede locatie in te richten voor spreiding, veerkracht en continuïteitsborging bij calamiteiten in CN.

3 Formele verankering van samenwerking met ODC's

Conceptbesluit om de Caribische datacenters integraal onderdeel te maken van het overheidsdatacenterlandschap via afspraken over interoperabiliteit, eigenaarschap en samenwerking.

4 Governance en gezamenlijke digitale voorzieningen

Gezamenlijke sturing en uitvoering versterkt weerbaarheid, kwaliteit en slagkracht. Richt een Bestuurlijk Overleg Digitalisering op met de verschillende overheidsorganisaties.

5 Besluit tot koppeling aan nieuwe onderzeese kabelinfrastructuur

Conceptbesluit om Europees Nederland en Caribisch Nederland te verbinden via een toekomstvaste onderzeese infrastructuur, met een afweging tussen nieuwe rechtstreekse verbindingen onder Nederlands beheer en (tijdelijke) benutting van bestaande kabelsystemen met gegarandeerde capaciteit.

Colofon

November 2025

[redacted]

[redacted]

HIGHBERG

Rapport

Sectie 2

Voorgaande sectie bevat de kern van het advies voor de datacenterstrategie van de overheid in Caribisch Nederland, met expliciete aandacht voor de relatie met de Nederlandse Digitaliseringsstrategie (NDS). Het schetst de huidige situatie, de strategische koers, de hoofdargumenten en de belangrijkste keuzes. Voor nadere onderbouwing, context en technische details wordt verwezen naar het volledige rapport 'Analyse en uitwerking advies datacenterstrategie overheid Caribisch Nederland', dat in de volgende sectie is opgenomen.

HIGHBERG

SECTIE 2: ANALYSE EN UITWERKING ADVIES DATACENTERSTRATEGIE OVERHEID CARIBISCH NEDERLAND

In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties

DATUM	**29-10-2025**
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20252670
INTERNE TOETS	Kerngroep BZK

TOELICHTING OP SECTIE 2

Het voorliggende deel van dit document bevat de inhoudelijke uitwerking van de keuzes, uitgangspunten en aanbevelingen uit de strategie. Het schetst een realistisch, uitvoerbaar en toekomstbestendig pad richting een robuuste digitale infrastructuur van de overheid in Caribisch Nederland. Daarbij wordt de gecombineerde koers van scenario 2 en 10 geadviseerd als richtinggevend kader voor de komende jaren. Een voorwaarde voor succesvolle uitvoering is dat regie, financiering en samenwerking vanaf de start stevig zijn geborgd. Deze koers legt de basis voor gelijke digitale toegang voor alle inwoners van Caribisch Nederland en zorgt voor een structurele aansluiting op de bredere overheidsinfrastructuur. Daarmee vormt de strategie tevens een fundament voor de verdere invulling van de Nederlandse Digitaliseringsstrategie (NDS) en de ambities van het programma Digitalisering Caribisch Nederland.

Onderstaand volgt een beknopt overzicht van de afwegingen:

Keuze	Te maken afweging	Mogelijke impact	Verantw. partij
Scenario 2: Twin-Datacenter binnen CN	Investeren in lokale datacenters ondanks beperkte schaalgrootte	Verbeterde lokale continuïteit en digitale dienstverlening op BES-eilanden	BZK, RCN, SSO-CN, Openbare Lichamen
Scenario 10: Koppeling met ODC in Europees Nederland	Investeren in koppeling, integratie en samenwerking met Overheidsdatacenters	Betere uitwijk, vereenvoudigde integratie met overheidsnetwerken.	BZK, Logius, RCN, RDI
Investeren in WAN-infrastructuur (Bv. onderzeese glasvezelkabels of dedicated verbindingen)	Kosten en technische realisatie versus soevereiniteit en connectiviteit	Versterkt digitale autonomie, continuïteit en betrouwbaarheid.	BZK, RCN, overige stakeholders met een belang
Centrale governance inrichten onder regie BZK	Ruimte voor eigen keuzes naast centrale besluitvorming	Duidelijke verantwoordelijkheid, samenhangend beheer en financiering	BZK, RCN, Openbare Lichamen
Lokale capaciteit opbouwen voor beheer	Lokale expertise ontwikkelen versus afhankelijkheid van Europees Nederland	Sneller lokaal herstel, versterking weerbaarheid	SSO-CN, Openbare Lichamen
Structurele financiering voor beheer en exploitatie	Publiek geld inzetten versus efficiency en accountability	Duurzame exploitatie en capaciteitsgroei	BZK, MinFin, RCN
Architectuur gebaseerd op GDI en basisregistraties	Afstemming op standaarden en federatief datastelsel	Toegang tot landelijke voorzieningen, interoperabiliteit	BZK, Logius, RCN
Noodzaak één overheid in de digitale wereld (NDS)	De Openbare Lichamen mogen gebruik maken van Overheidsfaciliteiten, -expertise en -dienstverlening.	Digitalisering van Caribisch Nederland kan op gelijkwaardig niveau gebracht worden als in Europees Nederland.	BZK, Openbare Lichamen, RCN

INHOUDSOPGAVE

1 INLEIDING

1.1 Achtergrond

Het programma "Digitalisering Caribisch Nederland" is een breed overheidsinitiatief gericht op het verbeteren van de digitale overheid en dienstverlening op Bonaire, Sint Eustatius en Saba. Het doel is om de voordelen van digitalisering beter te benutten voor inwoners, bedrijven en overheden. Hiervoor moeten randvoorwaarden als connectiviteit, dataopslag en digitale veiligheid op orde zijn. Een robuuste en toekomstbestendige digitale infrastructuur is daarbij cruciaal. De ontwikkeling van een datacenterstrategie speelt hierin een sleutelrol: het biedt een fundament voor verdere digitalisering en garandeert veilige, toegankelijke en efficiënte dataopslag en -verwerking.

Caribisch Nederland staat voor de opgave om de digitale infrastructuur structureel te versterken. De huidige situatie is versnipperd en kwetsbaar, met twee gemoderniseerde maar kleine datacenters, afhankelijkheid van verouderde zeekabels die verlopen via omslachtige, inefficiënte en geopolitiek kwetsbare routes, en een beperkt aantal lokale IT- en cybersecurityspecialisten. Tegelijkertijd neemt de vraag naar digitale overheidsdiensten toe, waarbij continuïteit en beveiliging onmisbaar zijn. Dit rapport presenteert een datacenterstrategie die hierop inspeelt, rekening houdend met de relevante wet- en regelgeving, het overheidsbeleid en de specifieke context van Caribisch Nederland.

1.2 Vraagstelling

CENTRALE VRAAG

Hoe kan een toekomstbestendige, veilige en efficiënte datacenterstrategie voor Caribisch Nederland worden vormgegeven, die aansluit bij de groeiende behoefte aan digitale overheidsdienstverlening en voldoet aan relevante wet- en regelgeving?

DIEPGANG VAN HET RAPPORT

De opdracht richt zich op het opstellen van een strategisch advies voor een datacenterstrategie in Caribisch Nederland. Een basisanalyse is in deze context geschikt, omdat het voldoende inzicht biedt in de belangrijkste elementen en risico's om een weloverwogen advies te formuleren, zonder dat alle details of complexiteiten volledig worden uitgediept. Nadere uitdieping en concretisering dient in een vervolg plaats te vinden.

1.3 Doel van dit document

Het doel van dit document is om richting te geven aan de datacenterfaciliteiten in Caribisch Nederland die de digitalisering en (online) dienstverlening van de overheid vanuit verschillende invalshoeken (veiligheid, efficiency, juridisch, Cloud beleid, hoogwaardige infrastructuur) ondersteunt.

1.4 Doelgroep

- Rijksoverheid / IV Bedrijfsvoering
- Beleidsmakers en beslissers binnen het Ministerie van BZK en andere departementen
- Lokale overheden in Caribisch Nederland (Bonaire, Sint Eustatius, Saba)
- ICT-uitvoeringsorganisaties
- Partners betrokken bij digitale dienstverlening en infrastructuur

1.5 Totstandkoming van het rapport

Dit rapport is tot stand gekomen via een praktijkgerichte aanpak, waarbij vanaf de start is ingezet op nauwe samenwerking tussen betrokken regionale, lokale en landelijke stakeholders uit zowel het Caribisch deel van Nederland en het Koninkrijk, - als het Europees deel van Nederland. Een centrale rol was weggelegd voor een werkgroep bestaande uit circa acht tot tien materiedeskundigen, afkomstig van diverse overheidsorganisaties. Deze werkgroep fungeerde als inhoudelijk klankbord en was verantwoordelijk voor het leveren van input, het toetsen van tussenresultaten en het valideren van keuzes gedurende het traject. Door de verscheidenheid aan

achtergronden en expertise in de werkgroep is het gelukt om het vraagstuk integraal te benaderen en breed draagvlak te creëren voor de uiteindelijke richting.
Parallel daaraan gaf een kerngroep (samengesteld uit vertegenwoordigers van de opdrachtgever en de externe adviseurs van Highberg) sturing. Deze kerngroep bewaakte de voortgang en zorgde voor inhoudelijke verdieping waar nodig. Door deze sturende rol heeft de kerngroep ervoor gezorgd dat het proces doelgericht bleef en dat de resultaten daadwerkelijk aansluiten bij de beleidsmatige en operationele realiteit.

Voor het onderzoek zijn verschillende instrumenten ingezet. Er is gebruikgemaakt van gerichte interviews met sleutelfiguren om behoeften, knelpunten en contextfactoren scherp in beeld te brengen. Daarnaast is relevante documentatie geanalyseerd, waaronder wet- en regelgeving en beleidsdocumenten. Scenario's zijn vervolgens ontwikkeld die zijn getoetst op strategische uitgangspunten en criteria met betrekking tot technische haalbaarheid, juridische kaders, organisatorische inpasbaarheid en financiële consequenties.
De kwaliteit en toepasbaarheid van het rapport zijn geborgd door een iteratieve werkwijze, met meerdere terugkoppelmomenten tussen de werkgroep en kerngroep. Bevindingen zijn steeds opnieuw getoetst, aangescherpt en verrijkt op basis van de verkregen feedback. Bovendien zijn de adviseurs afgereisd naar Bonaire voor een verkenning van de lokale situatie, inclusief gesprekken met betrokkenen ter plaatse. Op Saba en St. Eustatius heeft geen lokale verkenning plaatsgevonden, maar is door middel van interviews, een documentstudie en openbaar beschikbare informatie een beeld gevormd. Deze aanpak heeft ervoor gezorgd dat het rapport geen puur theoretische exercitie is geworden, maar een concreet, realistisch en uitvoerbaar advies dat daadwerkelijk aansluit bij de behoeften en mogelijkheden van Caribisch Nederland.

1.6 Indeling van het rapport

De volgende hoofdstukken werken de deelvragen verder uit. Hoofdstukken 2 en 3 geven een beschrijving van de huidige situatie en relevante ontwikkelingen. In Hoofdstuk 4 worden de behoeften van stakeholders geanalyseerd. Hoofdstuk 5 bevat de strategische uitgangspunten en randvoorwaarden. De huisvesting van het datacenter op de BES-eilanden wordt in hoofdstuk 6 besproken. En hoofdstuk 7 beschrijft de randvoorwaarden voor netwerkinfrastructuur. Hoofdstuk 8 verkent de mogelijke varianten, waarna in Hoofdstuk 9 en bijlage D de beoordelingscriteria worden toegelicht. Hoofdstukken 10 en 11 gaan in op de samenwerkingsmogelijkheden en het risicomanagement. Hoofdstuk 12 bevat de conclusies en aanbevelingen. Tot slot worden in de bijlagen het stappenplan, de duurzaamheidsaspecten en de globale doelarchitectuur voor de voorkeursvariant uitgewerkt.

1.7 Document historie

Tabel 1. Document historie

Datum	Versie / Status	Toelichting
29 april 2025	Conceptrapport fase 1 (afgerond)	Feedback verwerkt in eindrapport
6 mei 2025	Datacenter strategische opties CN	Feedback verwerkt in eindrapport
7 t/m 19 mei 2025	Concepteindrapport versie 0.1 t/m 0.6	Conceptversies Highberg, interne QA
19 mei 2025	Concepteindrapport versie 0.6	Conceptversie tbv de werkgroep
10 juni 2025	Concepteindrapport versie 0.7	Conceptversie tbv de kerngroep
6 augustus 2025	Concepteindrapport versie 0.8	Conceptversie tbv kerngroep
28 augustus 2025	Eindrapport, versie 0.9	Definitief concept
November 2025	Eindrapport, versie 1.0	Definitief

1.8 Lijst met afkortingen en definities

De lijst met afkortingen en definities is opgenomen in bijlage F.

2 SITUATIE EN ARCHITECTUUR OVERHEIDSINFRASTRUCTUUR

In dit hoofdstuk wordt kort een overzicht gegeven van de bestaande digitale infrastructuur in Caribisch Nederland, inclusief datacenterlocaties, verbindingen en gebruikte diensten. Dit geeft een eerste beeld voor verdere strategievorming.

ORGANISATIE OVERHEDEN IN CARIBISCH NEDERLAND

Binnen Caribisch Nederland zijn meerdere overheidslagen actief met eigen verantwoordelijkheden en uiteenlopende organisatorische inrichtingen van hun ICT. Het Rijk voert de een groot deel van Rijksbrede taken uit via RCN en SSO-CN, die hun datacenterfaciliteiten hebben geconsolideerd op Bonaire. Tegelijkertijd beschikken de Openbare Lichamen (gemeenteniveau) op Saba, Sint Eustatius en Bonaire over eigen, kleinschalige IT-oplossingen, vaak zonder structurele koppeling met de centrale overheidsinfrastructuur. Daarnaast zijn er semi-overheden zoals onderwijsinstellingen, water- en energiebedrijven, lucht- en zeehavens en zorgorganisaties, die hun digitale voorzieningen ad hoc inrichten, veelal via commerciële partijen. Deze versnippering leidt tot verschillen in beveiliging, continuïteit en schaalbaarheid, en beperkt het vermogen om gezamenlijk op te trekken richting een robuuste, gedeelde infrastructuur. Dit vraagt om regie en afstemming over de lagen heen.

DATACENTERS IN CARIBISCH NEDERLAND

Caribisch Nederland beschikt momenteel over twee moderne datacenters. Op Bonaire staat in een gebouw van SSO-CN een kleine, recent gemoderniseerde datacenterfaciliteit waar centrale systemen draaien voor departementale units. Hier bevinden zich onder andere (een deel van) de Active Directory, file-servers en applicaties die lokaal op Bonaire moeten blijven. De voorzieningen omvatten airconditioning, noodstroomvoorziening en basis toegangsbeveiliging. De ruimte is echter qua vloeroppervlakte vol, wat uitbreiding binnen het huidige gebouw niet mogelijk maakt. Het datacenter voldoet niet aan Tier-III of hogere specificaties en heeft slechts één stroomfeed en generator, wat de redundantie beperkt.

Figuur 1: Datacenter SSO-CN Bonaire

Voor aanvullende redundantie maakt de Rijksdienst Caribisch Nederland (RCN) op Bonaire gebruik van het datacenter van Flamingo TV. Deze voorziening is modern maar kleinschalig en kent geen fysieke scheiding van racks of ruimten. De systemen van RCN zijn verdeeld over beide datacenters op Bonaire in een gestretchte twin-datacenteropstelling. Daardoor is een solide basis voor continuïteit aanwezig: bij uitval van één locatie blijft downtime beperkt tot enkele minuten, zonder blijvende impact op de systeemprestaties of gebruikerservaring. De Rijksdienst op Saba en Sint Eustatius draait eveneens via deze dark fiber ring mee op dezelfde datacenters als Bonaire, waardoor de failover op systeemniveau daar op orde is. Voor de Rijksdienst ligt het resterende risico met name in de kwetsbaarheid van de verbindingen en de back-upverbindingen.

Voor de Openbare Lichamen Saba en Sint Eustatius is de situatie aanzienlijk kwetsbaarder. Hun IT-infrastructuur bestaat uit enkele gehuurde serverracks bij lokale telecomaanbieders en op eigen locaties, vaak met minimale voorzieningen die niet verder reiken dan een eenvoudige airco en beperkte noodstroom. In het verleden leidde dit tot downtime bij storingen. Er is geen volwaardige failoverlocatie, wat de continuïteit bij calamiteiten onder druk zet. Back-ups worden in sommige gevallen opgeslagen via derden, zoals NetPro (Curaçao), dat capaciteit huurt bij Flamingo TV.

Voor het Openbaar Lichaam Bonaire geldt een ander model: hier is een Cloud-tenzij beleid ingevoerd. Dat houdt in dat het OL primair gebruikmaakt van externe datacenters bij commerciële leveranciers verspreid over de wereld. Deze aanpak biedt flexibiliteit maar brengt ook afhankelijkheden en geopolitieke risico's met zich

mee, omdat lokale gegevensopslag niet structureel is geborgd en de zeggenschap grotendeels bij externe partijen ligt.

NETWERK EN VERBINDINGEN

De eilanden zijn aangesloten op de wereldwijde digitale infrastructuur via onderzeese glasvezelkabels en aanvullende verbindingen. Bonaire beschikt over twee verbindingen, beide richting Curaçao, waarmee het eiland is gekoppeld aan de internationale backbones. Saba en Sint Eustatius zijn via het Saba Statia Cable System (SSCS) verbonden met zowel Sint Kitts en Nevis als Sint-Maarten. Via deze SSCS-kabel kan dataverkeer vanaf Saba of Statia worden doorgestuurd naar St. Kitts of St. Barths, waar het aansluit op andere internationale backbones.

Een rechtstreekse dataverbinding tussen alle BES-eilanden onderling of met Europees Nederland ontbreekt, waardoor al het dataverkeer via omwegen verloopt, veelal via knooppunten in de Verenigde Staten. Mede hierdoor wordt in de praktijk in een hoge latency ervaren, met aanzienlijke vertragingen in het geval van verstoringen op de route. Volgens geïnterviewden is deze latency bovendien niet stabiel en loopt deze regelmatig op. Dit is volgens sommige geïnterviewden vooral merkbaar bij applicaties die afhankelijk zijn van (near) real-time datavoorziening, toepassingen die muisprecisie vereisen of videoconferencing. De afhankelijkheid van interinsulaire- en transatlantische infrastructuur vergroot de digitale kwetsbaarheid van de eilanden. Daarbij kent de huidige kabelinfrastructuur een aantal kwetsbare punten, waarbij schade aan één enkele kabel, bijvoorbeeld door een anker of een orkaan, kan leiden tot verbindingsproblemen, en in een uiterst geval mogelijk vrijwel volledige internetisolatie van een eiland.

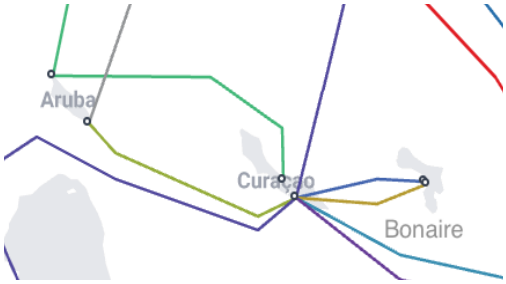
De Rijksoverheid heeft vastgesteld dat de huidige verbindingen qua capaciteit en beschikbaarheid tekortschieten. In de Kamerbrief van september 2024 wordt benadrukt dat veel zeekabels verouderd zijn en dat de markt rond Bonaire wordt gedomineerd door één buitenlandse partij, waardoor er weinig sprake is van prijsconcurrentie. Dit beperkt de digitale autonomie en vergroot de afhankelijkheid van externe infrastructuur. Zelfs bij een robuust ingerichte architectuur vormt het ontbreken of uitvallen van betrouwbare verbindingen een wezenlijk risico. Zonder stabiele en veilige connectiviteit komen de continuïteit van digitalisering, digitale dienstverlening en kritieke processen onder druk te staan.

De zeekabels die in de volgende figuren worden weergegeven, vormen de publieke internetbackbone in de Caribische regio rondom de BES eilanden. Deze kabelsystemen worden hoofdzakelijk gebruikt voor regulier internetverkeer dat via internationale transit providers wordt gerouteerd. Een uitzondering hierop: de SSCS (Saba Statia Cable System), die eigendom is van de Nederlandse overheid.

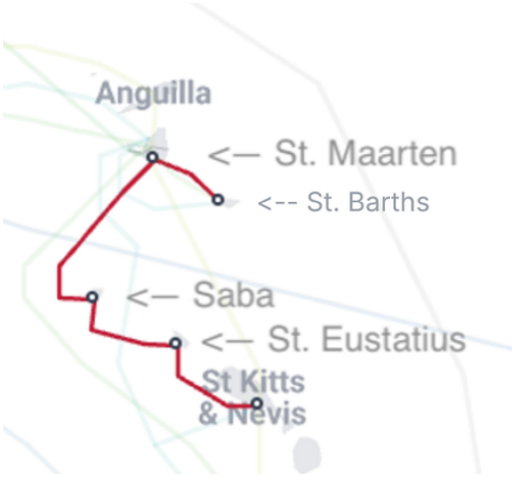
Voor toepassingen die vragen om hoge betrouwbaarheid, voorspelbare latency en gegarandeerde bandbreedte, zoals realtime datacentersynchronisatie, replicatie of failover tussen twin-datacenters, wordt over het algemeen aangeraden om gebruik te maken van dedicated of gegarandeerde capaciteit op één of meerdere van deze zeekabelverbindingen. Dit vereist doorgaans aparte commerciële afspraken met de exploitanten van de kabels, los van standaard internettransit.

Het is daarom van strategisch belang dat in toekomstige infrastructuurontwikkeling nadrukkelijk wordt gekeken naar de mogelijkheden voor privé interconnectie, om de continuïteit, prestatie, veiligheid en soevereiniteit van vitale digitale diensten te kunnen waarborgen.

Hieronder treft u een aantal figuren aan. Eerst wordt er ingezoomd op de BES eilanden, waarna we uitzoomen in de bovenwindse regio.

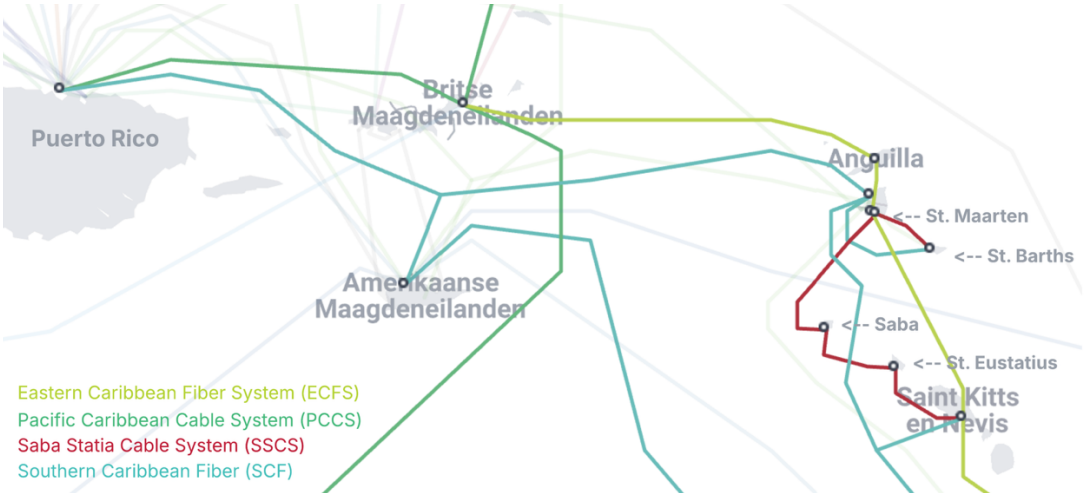


Figuur 3.1: Connectiviteit Bonaire. Op de onderzeekabelkaart is te zien dat Bonaire alléén verbonden is met Curaçao. Dit zorgt voor een grote afhankelijkheid van Curaçao en diens voorzieningen. Vanuit Curaçao kan er via vergelijkbare kabels gecommuniceerd worden met Aruba, Zuid-Amerika en Noord-Amerika. De meest voorkomende en efficiënte route naar Europa gaat via Curaçao → Puerto Rico (VS) of de Britse Maagdeneilanden → Miami of Jacksonville (VS) → New York (VS) → Nederland (al dan niet via het Verenigd Koninkrijk).



Figuur 3.2: De rode lijn in de figuur geeft het tracé van het Saba Statia Cable System (SSCS) weer. Deze onderzeese verbinding vormt de primaire digitale levensader van beide eilanden en is in handen van de Nederlandse overheid. De meest voor de hand liggende route voor communicatie met Bonaire loopt via St. Kitts of St. Barths → Puerto Rico (VS) of Britse Maagdeneilanden → Aruba en/of Curaçao → Bonaire. (Op de kaart is niet zichtbaar dat de SSCS voor de kust van Sint-Maarten een aftakking maakt richting St. Barths, waardoor Saba rechtstreeks met St. Barths is verbonden.)

Hoewel er theoretisch ook een route mogelijk is via Zuid-Amerika richting Curaçao en Bonaire, vereist deze route doorgaans tot wel acht netwerkhops via diverse zuidelijke eilanden en derde landen. Dit maakt de verbinding aanzienlijk minder efficiënt en minder robuust dan de noordelijke route via Puerto Rico of de Britse Maagdeneilanden.



Figuur 3.3: Regionale connectiviteit via SSCS, SCF, PCCS en ECFS.[1]

Voor de internationale en regionale netwerkverbindingen van Saba en Sint Eustatius is een combinatie van onderzeese glasvezelkabels van essentieel belang. In deze context toont Figuur 3 de inzet van vier belangrijke

[1] De originele bron gebruikt voor de visuele weergave van deze verbindingen is https://www.submarinecablemap.com/ Het materiaal is wel aangepast om te verduidelijken voor dit document.

kabelsystemen: SSCS, SCF, ECFS en PCCS. In de regio bevinden zich aanvullende kabelsystemen buiten de BES-eilanden, maar uit interviews blijkt dat de genoemde verbindingen momenteel de primaire routes vormen voor internationale connectiviteit vanuit Caribisch Nederland en onderlinge koppeling tussen de BES-eilanden. Deze verbindingen zijn operationeel en gebruikt voor dataverkeer richting de VS, Europa en andere regio's. Er is echter geen vanzelfsprekende toegang tot andere kabelsystemen in de regio, en het is onduidelijk of lokale internetproviders op de BES hierover afspraken hebben gemaakt. Daarom is in dit rapport uitgegaan van de hierboven benoemde kabelinfrastructuur als uitgangspunt.

De SSCS (St. Kitts–St. Eustatius–Saba) is dubbel uitgevoerd en van kritisch belang, aangezien dit op dit moment de enige zeekabelverbinding is die fysiek aan land komt op zowel Saba als Sint Eustatius. Via dit systeem hebben beide eilanden indirecte toegang tot andere netwerken:

- Op St. Kitts sluit de SSCS aan op de SCF (Southern Caribbean Fiber) en de ECFS (Eastern Caribbean Fiber System);
- Op St. Barths is er aansluiting met de SCF;
- Op St. Maarten is er aansluiting op de ECFS.

Vanuit deze regionale hubs kan het dataverkeer vervolgens verder worden geleid:

- Via de ECFS kan het verkeer worden doorgestuurd naar de Britse Maagdeneilanden, waar aansluiting mogelijk is op de PCCS (Pacific Caribbean Cable System). Deze kabel voert het verkeer door naar zowel Jacksonville (VS) als Puerto Rico (VS), maar biedt ook een route via Aruba naar Curaçao, waarmee verbinding wordt gemaakt met het bredere netwerk in het zuidelijk Caribisch gebied.
- De SCF maakt eveneens uitwisseling van dataverkeer mogelijk met onder meer Puerto Rico (VS), waarmee redundantie en route-optimalisatie kunnen worden gerealiseerd.

Deze kabelstructuur vormt de digitale levensader voor de bovenwindse eilanden, waarbij de sterke afhankelijkheid van de SSCS een aandachtspunt blijft voor robuustheid, redundantie en toekomstige uitbreiding. Er zijn recente ontwikkelingen rond de aansluiting van Bonaire op het CELIA-kabelsysteem, dat via Aruba naar Puerto Rico en de Verenigde Staten loopt. Omdat deze verbinding nog niet gerealiseerd is, is deze in dit onderzoek buiten beschouwing gelaten. Hoewel CELIA de internetconnectiviteit van Bonaire kan verbeteren, volgt het grotendeels hetzelfde pad via derde landen en levert het daardoor slechts beperkte bijdrage aan de doelstellingen van de datacenterstrategie, zoals directe interinsulaire of trans-Atlantische verbindingen onder Nederlandse regie. De meerwaarde ligt primair in een verbeterde internetverbinding voor Bonaire.

CAPACITEIT EN BETROUWBAARHEID DATACENTERS

De recent gemoderniseerde voorzieningen van de SSO-CN op Bonaire bieden basiszekerheden zoals noodstroom via dieselgeneratoren en UPS-systemen, evenals klimaatbeheersing en automatische blusinstallaties. Binnen deze architectuur is een mate van continuïteit gewaarborgd, zolang storingen zich beperken tot één locatie.

Op Saba en Sint Eustatius zijn de Openbare Lichamen, maar ook lokale (semi) overheidsdiensten zoals ziekenhuizen, water- en energiebedrijven, Lucht- en zeehaven e.d. daarentegen sterk afhankelijk van de lokale, maar beperkte, faciliteiten. Door hun ligging in de orkaanzone is het risico op schade groot, terwijl er geen volwaardige alternatieve locaties beschikbaar zijn. Back-ups van de Openbare Lichamen worden deels extern opgeslagen, op Bonaire (niet bij SSO-CN) maar ook in Europese of Amerikaanse cloudomgevingen, maar bij uitval is de hersteltijd onduidelijk en risicovol.

DATAVERKEER EN GEBRUIK

De vraag naar stabiele en snelle verbindingen neemt toe. Rijksdiensten zoals de Belastingdienst, IND, KMar en DJI zijn fysiek aanwezig op de eilanden en maken gebruik van centrale systemen in Europees Nederland. Deze afhankelijkheid van interinsulaire en -continentale verbindingen legt extra beslag op de internationale

connectiviteit (bandbreedte), verhoogt de gevoeligheid voor vertragingen en is relatief duur vanwege internationale transit- en bandbreedtetarieven.

HUIDIGE CLOUD-GEBRUIK

Vanwege het ontbreken van kennis, kunde, en een modulaire dienstverlener wordt er door de Openbare Lichamen steeds vaker gebruikgemaakt van cloudoplossingen. Hetgeen wordt versterkt omdat er vanuit de Rijksoverheid geen IT-dienstverlening geleverd kan/mag worden aan lokale of semi overheden. (Bijvoorbeeld door het SSO-CN)

Voor lokale departementale onderdelen van de Rijksoverheid geldt het algemene cloudbeleid van het Ministerie van BZK. Andere overheidsorganisaties, zoals de Openbare Lichamen voeren hierin een eigen beleid.

Voorbeelden voor de openbare lichamen zijn Office 365 en andere SaaS-diensten die gehost worden in Europese of Amerikaanse datacenters. Deze inzet gebeurt ad hoc, zonder overkoepelende strategie, vanuit een praktische behoefte aan capaciteit en beschikbaarheid.

Op Saba (OLS) en Sint Eustatius (OLE) is deze ontwikkeling versneld door het beperkte IT-personeel en de fysieke afstand tot de hosting en cloud locaties in de VS, wat ten opzichte van Europa relatief lage latency oplevert. Tegelijkertijd betekent dit dat lokale overheidsdata al buiten de eilanden wordt opgeslagen, onder de eigen bevoegdheid van de Openbare Lichamen.

De bouwstenen voor een moderne infrastructuur zijn in de basis bij RCN aanwezig, maar verdere professionalisering, centralisatie en regie zijn noodzakelijk. De volgende hoofdstukken beschrijven de strategische keuzes om deze infrastructuur toekomstbestendig te maken.

3 OVERZICHT VAN RELEVANTE ONTWIKKELINGEN

Zowel in de regionale context van het Caribisch deel van Nederland als in de bredere wereld van (overheids-)IT zijn er ontwikkelingen die richtinggevend zijn voor de datacenterstrategie. We onderscheiden (3.1) relevante internationale en landelijke ontwikkelingen, en (3.2) specifieke ontwikkelingen in het Caribisch gebied en Europees Nederland die van belang zijn.

3.1 Internationale en landelijke ontwikkelingen

DIGITALE AUTONOMIE EN DIGITALE SOEVEREINITEIT

De afgelopen jaren is het gebruik van public cloud (IaaS, PaaS en SaaS) sterk toegenomen. Organisaties hebben hierdoor minder eigen hardware nodig en maken steeds vaker gebruik van oplossingen zoals Microsoft 365 en Google Workspace. In Europees Nederland heeft dit geleid tot grootschalige cloudmigraties en het centraliseren van datacenters binnen de rijksoverheid.

Tegelijkertijd nemen de zorgen toe over digitale soevereiniteit: de juridische en politieke zeggenschap over overheidsdata en digitale infrastructuur. Bij opslag van data in de cloud bij buitenlandse aanbieders buiten de EU gelden vaak andere wetten. Zo kan de Amerikaanse Patriot Act (2001) opsporingsdiensten toegang geven tot data van Europese klanten. Dit roept vragen op over veiligheid, privacy (AVG-naleving) en regie.

Digitale autonomie verwijst naar de mate waarin een overheid of organisatie zélf keuzes kan maken over haar digitale infrastructuur, onafhankelijk van een specifieke leverancier of buitenlands platform. Autonomie draait om technische en operationele vrijheid, terwijl soevereiniteit betrekking heeft op juridische en bestuurlijke controle. De voordelen van de cloud – flexibiliteit, schaalbaarheid en innovatie – moeten dan ook zorgvuldig worden afgewogen tegen de risico's van afhankelijkheid.

Op Europees niveau worden initiatieven ontplooid om die afhankelijkheid te verkleinen. Projecten zoals GAIA-X en de EU Data Act zijn gericht op het vergroten van digitale autonomie en het versterken van de technologische onafhankelijkheid van lidstaten.

Geopolitieke spanningen en incidenten zoals cyberaanvallen onderstrepen de urgentie. Op 12 maart 2025 debatteerde de Tweede Kamer hierover naar aanleiding van een kritisch rapport van de Algemene Rekenkamer. Kamerleden spraken hun zorgen uit over de dominante positie van Amerikaanse techbedrijven en pleitten voor Europese alternatieven. Staatssecretaris Szabó kondigde daarop een onderzoek aan naar een soevereine overheidscloud. Nederland wil zijn digitale autonomie versterken, meer eigen regie voeren en tegelijkertijd zijn digitale soevereiniteit waarborgen: volledige zeggenschap over publieke data en infrastructuur. Dit vereist minder afhankelijkheid van buitenlandse cloudleveranciers en meer controle over waar en hoe data wordt opgeslagen en beheerd.

EUROPESE REGELGEVING EN STANDAARDEN

De EU heeft de laatste jaren ingezet op regelgeving rond digitale infrastructuur. De AVG stelt hoge eisen aan privacy en dataopslag. De NIS2-richtlijn verplicht lidstaten om de digitale weerbaarheid van vitale sectoren, waaronder overheids-IT en datacenters, te verhogen. Deze richtlijn wordt ook in Nederland omgezet in wetgeving, met onder meer minimumeisen voor beveiligingsmaatregelen en verplichte incidentrapportage. Daarnaast krijgen de European Cloud Code of Conduct en het EUCS-certificeringsschema een leidende rol. Hoewel het Caribisch deel Nederland geen onderdeel is van de interne markt van de EU en deze EU-regelgeving dus niet van toepassing is, past de Rijksoverheid Europese standaarden toe op lokale onderdelen van de Rijksdienst en neemt het Europese standaarden als uitgangspunt voor beleid op de BES eilanden. Dit vloeit voort uit artikel 132a van de Grondwet en uit het comply-or-explain-beleid van het kabinet.

De bewaartermijnen sluiten aan bij de AVG: alleen bewaren zolang noodzakelijk. Ondanks dat besluitvorming en doorvoering lang duurt wordt in dit rapport uitgegaan van de situatie dat de overheden in Caribisch Nederland zich moeten conformeren aan de Europese wet- en regelgeving en bijbehorende best practices op het gebied van security, continuïteit en gegevensbescherming.

REGELGEVING EN STANDAARDEN BES

De Wbp BES vereist dat persoonsgegevens adequaat worden beschermd, ook bij opslag buiten de BES-eilanden. Dit vraagt om aantoonbare beveiliging, doelbinding en (bij gebruik van derden zoals cloudproviders) een verwerkersovereenkomst en expliciete risicobeoordeling bij doorgifte aan landen met andere privacyregels.

DIGITALISERING VAN DIENSTVERLENING

Burgerverwachtingen ten aanzien van digitale overheidsdienstverlening blijven groeien. Mensen willen 24/7 onlinezaken kunnen doen met de overheid, en verwachten snelheid en betrouwbaarheid vergelijkbaar met commerciële diensten. Voor Caribisch Nederland speelt bovendien mee dat digitale diensten een oplossing kunnen bieden voor eilandelijke knelpunten en de afstand tot Europees Nederland, met goede digitale infrastructuur kan men op de BES eilanden toch gebruikmaken van centrale voorzieningen. Dit vraagt om een robuuste verbinding en infrastructuur. Wanneer systemen traag of vaak offline zijn, ondermijnt dat het vertrouwen en gebruik. De gepubliceerde Nederlandse Digitaliseringsstrategie (NDS) beoogt dat iedereen, ongeacht locatie, veilig en efficiënt digitale overheidstaken kan uitvoeren. De strategie is om als "één overheid" te werken en geen digitale kloof te laten ontstaan. Voor de BES-eilanden is het daarom belangrijk aan te haken op de nationale digitaliseringsagenda, zodat overheden en semi-overheden dezelfde kwaliteit van dienstverlening kunnen bieden als in Europees Nederland.

EDGE COMPUTING

Edge computing is een vorm van hosting waarbij rekenkracht, opslag en dataverwerking zo dicht mogelijk bij de eindgebruiker wordt geplaatst, om de prestaties van digitale diensten te verbeteren en afhankelijkheid van centrale infrastructuur te verminderen. Dit is met name van belang voor toepassingen die gevoelig zijn voor vertraging (latency), zoals videoconferencing, real-time monitoring, interactieve webapplicaties of operationele systemen van overheden.

In de context van Caribisch Nederland biedt edge computing een potentieel aantrekkelijke manier van IT-dienstverlening, vooral vanwege de hoge latency naar Europese of Amerikaanse datacenters. Edge computing is echter geen losstaande oplossing, maar een specifieke inrichting van IT-infrastructuur waarbij rekenkracht dichter bij de gebruikers wordt geplaatst. Om dit mogelijk te maken is een robuuste datacenterinfrastructuur op de locatie zelf een vereiste. Zonder adequate fysieke voorzieningen – zoals klimaatbeheersing, noodstroom, brandveiligheid, fysieke beveiliging en redundante netwerkverbindingen – is het niet haalbaar om edge computing betrouwbaar en veilig te implementeren. 'Edge' is daarom niet een op zich staande oplossing, want er is en blijft datacenter infrastructuur noodzakelijk.

Aangezien dergelijke infrastructuur op Saba en Sint Eustatius ontbreekt of zeer beperkt is zul je ook voor edge computing, datacenter infrastructuur moeten bouwen. Daarbij moet ook deze infrastructuur voldoen aan alle kaders, richtlijnen en wet- en regelgeving. Zonder bestaande datacenterbasis blijft edge computing vooral een theoretische optie, en geen pragmatische oplossing in deze context.

ARTIFICIAL INTELLIGENCE (AI)

Een belangrijke ontwikkeling die invloed heeft op de datacenterstrategie is de opkomst van kunstmatige intelligentie (AI), en in het bijzonder generatieve AI. AI biedt grote kansen voor efficiëntere dienstverlening, beter datagedreven beleid en snellere besluitvorming. Voor Caribisch Nederland betekent dit dat ook de datacenterinfrastructuur voorbereid moet zijn op de opslag, verwerking en governance van AI-toepassingen. Dat vereist schaalbare en betrouwbare systemen, heldere afspraken over datagebruik, en aansluiting bij rijksbrede kaders. Zodat de eilanden de voordelen van AI kunnen benutten zonder de risico's uit het oog te verliezen.

5G

De wereldwijde uitrol van mobiele netwerken op basis van 5G technieken zal op termijn ook de Cariben bereiken. Hoewel een grootschalige uitrol op de BES-eilanden momenteel nog niet rendabel lijkt, is het aannemelijk dat ook deze regio op langere termijn toegang krijgt tot 5G-netwerken. Dit opent de deur naar nieuwe latency gevoelige digitale diensten zoals smart city-toepassingen, telemedicine, en geavanceerde mobiliteitsoplossingen. Het is niet ondenkbaar dat de Openbare Lichamen, de zorg, en Rijksdiensten op den duur gebruik willen maken van gelijksoortige toepassingen. Voorwaarde is wel dat de onderliggende infrastructuur — zoals glasvezelverbindingen, datacenters en energievoorziening — hierop voorbereid is.

INTERNET OF THINGS (IOT)

Het Internet of Things verwijst naar de groeiende hoeveelheid slimme apparaten die via het internet communiceren, van afvalcontainers tot medische apparatuur en water- of energiemeters. Ook in Caribisch Nederland neemt het belang hiervan toe, bijvoorbeeld voor efficiënter overheidsbeheer, duurzame energievoorziening of toerismetoepassingen. Dit vraagt om betrouwbare netwerkinfrastructuur en lokale dataverwerking, wat het belang van stabiele, goed uitgeruste digitale voorzieningen nabij de gebruiker onderstreept.

3.2 Ontwikkelingen in Caribisch Nederland en Europees Nederland

ZEEKABELS

Een belangrijke ontwikkeling in de digitale infrastructuur is de actieve inzet van het kabinet op de versterking van internationale connectiviteit via nieuwe onderzeese glasvezelkabels. Voor Caribisch Nederland werd in 2024 een afzonderlijk onderzoek uitgevoerd naar de huidige en toekomstige data-ontsluiting van de BES-eilanden. Hieruit bleek dat een groot deel van de bestaande kabelinfrastructuur in de regio sterk verouderd is: circa 45% van de Caribische kabels t.b.v. Bonaire is ouder dan 25 jaar en naderen hun technische einde. Daarbij is een groot deel van de capaciteit in handen van één marktpartij (met name rondom Bonaire), wat leidt tot beperkte concurrentie op prijs en kwaliteit.

Een bijkomende kwetsbaarheid is het ontbreken van directe kabelverbindingen tussen Caribisch Nederland en Europa. Al het verkeer verloopt via derde landen, zoals o.a. de Verenigde Staten, wat niet alleen zorgt voor extra latency, maar ook betekent dat storingen, geopolitieke spanningen of interceptie door derde landen directe impact kunnen hebben op overheidscommunicatie en digitale dienstverlening binnen Nederland. Mede daarom worden er alternatieve routes verkend, zoals een rechtstreekse kabel naar Europa of een zuidelijke route via Zuid Amerika. Hoewel realisatie hiervan meerdere jaren zal vergen, bieden dergelijke opties structureel perspectief op veiligere, snellere en meer onafhankelijke verbindingen.

Tegelijkertijd biedt de geografische ligging van Caribisch Nederland een unieke strategische kans. In een wereld waarin digitale infrastructuur steeds meer onder druk staat door internationale spanningen en toenemende dreigingen in de Noord-Atlantische regio, kan Caribisch Nederland op termijn dienen als uitwijklocatie voor Europees Nederland. Dit geeft een extra dimensie aan de noodzaak voor directe, zogenaamde geo-landonafhankelijke verbindingen tussen beide delen van Nederland. Door ook buiten het Europese vasteland te investeren in robuuste digitale toegang, wordt de continuïteit van essentiële overheidsprocessen en communicatielijnen beter gewaarborgd.

In dat licht krijgt ook de aanleg van nieuwe regionale kabelprojecten, zoals de CELIA-CETC-kabel waarbij Setar samenwerkt met marktpartijen, bredere betekenis. Deze kabel verbindt Aruba met onder meer Martinique, Puerto Rico en de Verenigde Staten, en draagt daarmee bij aan de versterking van de digitale infrastructuur in het Caribisch gebied. Hoewel de BES-eilanden geen directe landingspunten zijn binnen de huidige projecten voor nieuwe trans-Atlantische kabels, profiteren zij op korte termijn van de aanleg van de nieuwe zeekabel tussen Aruba en Bonaire. Deze verbinding vergroot de routediversiteit en verlaagt de kosten voor datatransport. Verdere afstemming en investeringen in regionale koppelingen via Curaçao en andere tussenstations blijven wenselijk. Op langere termijn biedt de versterking van de digitale infrastructuur op de BES-eilanden kansen om Caribisch Nederland te positioneren als strategische regionale hub binnen het Koninkrijk. In een tijd van mondiale spanningen en toenemende zorgen over digitale soevereiniteit is dat geen overbodige luxe, maar een noodzakelijke bouwsteen in een veerkrachtige, overheidsbrede digitale strategie.

LOKALE IT-ECOSYSTEEM EN MARKT

Op de BES-eilanden zelf ontwikkelt de ICT-markt zich geleidelijk. Tot voor kort waren er nauwelijks lokale bedrijven met ervaring in datacenters of cloud diensten. De markt was te klein en de overheid deed veel zelf of via Europees Nederland. Nu is te zien dat telecom- en internetaanbieders op de eilanden (zoals Telbo en Flamingo TV op Bonaire, SATEL op Saba en EUTEL op Sint Eustatius) investeren in hun netwerken en interesse tonen in aanverwante diensten. Er zijn enkele lokale IT-bedrijven ontstaan die bijvoorbeeld managed services aanbieden aan het MKB. Dit is relevant, omdat samenwerking met of uitbesteding aan zo'n partij een optie zou kunnen zijn ("Lokale outsourcing"). Echter, wil men de grenzen van de Aanbestedingswet en marktwerking

zoveel mogelijk respecteren.[2] In de praktijk betekent dit dat als de overheid in Caribisch Nederland kiest om een extern bedrijf in de arm te nemen voor het datacenter, dit via een open aanbesteding of tenminste een marktconsultatie zal lopen. Een gezonde marktwerking is gewenst. Voorkomen moet worden dat de overheid één lokale partij exclusief bevoordeelt, wat andere marktpartijen uitsluit. Tegelijkertijd is de markt zeer klein. Een ander alternatief is om aan te sluiten bij een overheidsbrede overeenkomst of een overheidsdienst (bijv. ODC-Noord of SSC-ICT) om de dienstverlening te leveren, waarbij de Aanbestedingswet ruimte biedt voor interbestuurlijke samenwerking zonder aanbesteding. Deze ontwikkelingen vragen om een zorgvuldige weging in de strategie, bijvoorbeeld door in CN lokaal diensten te kopen waar het kan om de economie en lokale kennisontwikkeling te steunen (bijvoorbeeld applicatieontwikkeling, cybersecurity en functioneel beheer) en centraal waar het moet om kwaliteit en continuïteit te borgen. Recent is vanuit EZ en BZK een subsidie geregeld voor de aanleg van glasvezel ("Fiber to the Home") op de BES-eilanden, waarmee de digitale infrastructuur verder wordt versterkt en het lokale ICT-ecosysteem ruimte krijgt om te groeien.

VERANDERENDE VRAAG VAN AFNEMERS

De behoefte aan digitale dienstverlening in Caribisch Nederland groeit snel. Overheidsorganisaties op de eilanden en in Den Haag worden steeds afhankelijker van een robuuste datacenterstrategie (zie hoofdstuk 4). Steeds meer rijksdiensten, zoals Justis en RVO, breiden hun taken uit naar de BES-eilanden. Tegelijk zetten de openbare lichamen in op eigen digitaliseringsplannen, zoals e-loketten en digitale raadsplatforms. De vraag naar ICT groeit daarmee in breedte (meer partijen) en diepte (hogere eisen, complexere diensten). Daarnaast neemt de integratie met systemen in Europees Nederland toe. Voorbeelden zijn de aansluiting op DigiD, MijnOverheid, de berichtenbox voor bedrijven, en koppelingen met P-Direkt. Dit vraagt om betrouwbare verbindingen en goede afstemming.

Stakeholders geven aan volledige ontzorging te willen, men wil zich kunnen focussen op de eigenlijke publieke taak en verwacht dat het datacenter en de bijbehorende IT-dienstverlening "gewoon werkt". Tegelijk hebben sommige grote gebruikers (zoals de Belastingdienst Caribisch Nederland (BCN) en SZW) hun eigen informatiemanagement-afdelingen met specifieke wensen en standaarden, zij willen soms controle houden over bepaalde componenten of zelf bepaalde applicaties (laten) beheren. Deze diversiteit aan wensen vereist dat een toekomstige oplossing flexibiliteit in het dienstenaanbod heeft. Het is niet one-size-fits-all, voor sommige afnemers zullen partijen in het datacenter alles beheren (inclusief de hosting van applicaties), voor andere slechts de housing en basis-infra, terwijl zij zelf de bovenliggende systemen beheren. Een modulair model ("keuzemenu" voor diensten) is een ontwikkeling die we in de behoeften zien terugkomen.

DUURZAAMHEID EN ENERGIE

Ten slotte is er groeiende aandacht voor duurzaamheid op de eilanden. Bonaire, Saba en Sint Eustatius streven naar meer hernieuwbare energie en bescherming van hun kwetsbare milieu. Datacenters staan bekend om hun hoge energieverbruik, waardoor lokale stakeholders benadrukken dat de ecologische impact zorgvuldig moet worden meegewogen. Zij vinden het belangrijk dat een datacenter past binnen de duurzame ambities van het eiland en vragen aandacht voor de ecologische voetafdruk in de besluitvorming. Volgens het CBS draaien de elektriciteitscentrales op de drie eilanden op hybride energiebronnen. Op Bonaire is diesel dominant; op Saba en Sint Eustatius is diesel vooral back-up. In 2023 kwam de hernieuwbare opwek uit op respectievelijk 22%, 30% en 28%, afkomstig van wind (Bonaire) en zon (Saba, Sint Eustatius). Door de hoge energieprijzen is energie-efficiëntie en lokale opwek, zoals zonnepanelen op het datacenter, zowel financieel als maatschappelijk relevant. Ook in Europees Nederland is hier aandacht voor: de Rijksinspectie Digitale Infrastructuur kijkt nadrukkelijk naar de beschikbaarheid én duurzaamheid van digitale netwerken. Bovendien zijn er rijksbrede CO_2-reductiedoelen, waar ook de ICT-sector aan moet bijdragen. Deze ontwikkelingen vormen input voor onze strategie: hoe kunnen we een toekomstig datacenter zo duurzaam mogelijk ontwerpen en exploiteren? In Bijlage C (Duurzaamheid) gaan we hier dieper op in.

[2] Formeel vallen de BES-eilanden buiten het directe toepassingsbereik van de Europese aanbestedingsrichtlijnen. Bonaire, Sint-Eustatius en Saba zijn niet opgenomen in het douanegebied of de interne markt van de Europese Unie, zoals bedoeld in de EU-verdragen. Nederland heeft ervoor gekozen om die regels (deels) vrijwillig te hanteren.

4 BEHOEFTEN EN EISEN VAN STAKEHOLDERS

In dit hoofdstuk bekijken we de behoeften, eisen en zorgen van de belangrijkste stakeholders voor de datacenterstrategie. De stakeholders omvatten onder meer de openbare lichamen, uitvoeringsdiensten van de Rijksoverheid, ZBO's die actief zijn in Caribisch Nederland, uitvoeringsorganisaties uit Europees Nederland met lokale dienstverlening of vestigingen, stichtingen, de centrale ministeries in Den Haag met bestuurlijke verantwoordelijkheid, en indirect ook burgers en bedrijven die afhankelijk zijn van goed functionerende overheidssystemen.

4.1 Openbare lichamen

De drie eilanden Bonaire, Sint Eustatius en Saba hebben als openbaar lichaam hun eigen lokale bestuursorganisatie. Zij zijn enerzijds vergelijkbaar met gemeenten, en behartigen de belangen van lokale (semi) overheidsorganisaties (waarin de OL's in deelnemen) zoals o.a. de brandweer, ziekenhuizen, water- en energiebedrijven en lucht- en zeehavens. Hun behoeften ten aanzien van ICT en datacenters zijn tweeledig:

BETROUWBARE ICT-BASISVOORZIENINGEN

De openbare lichamen (OL) willen er zeker van zijn dat essentiële applicaties (bijv. bevolkingsadministratie en financiële systemen) altijd beschikbaar zijn. Uitval van ICT legt het lokale bestuur lam. Voor de OL is hoge beschikbaarheid en redundantie essentieel. Omdat de eilanden geïsoleerd liggen, betekent dit dat er voldoende lokale voorzieningen moeten zijn om tijdelijk zelfstandig te opereren als de connectiviteit naar buiten wegvalt.

LOKALE ZEGGENSCHAP EN FLEXIBILITEIT

De openbare lichamen hechten waarde aan lokale autonomie. In de geest van het Huis van Thorbecke is lokale democratie belangrijk. Dit vertaalt zich in de wens om inspraak te hebben in de inrichting van digitale voorzieningen. Ze willen niet volledig afhankelijk worden van de Rijksoverheid, in het Europees deel van Nederland of van Bonaire, voor elke wijziging of storing. Idealiter voorziet de oplossing in een governance-structuur waarin de eilanden mede sturing kunnen geven. Dat kan bijvoorbeeld door deelname in een stuurorgaan of het kunnen bepalen van prioriteiten in dienstverlening. Ook flexibiliteit is genoemd, als Bonaire bijvoorbeeld een eigen e-loket wil hosten met specifieke behoeften, moet dat in het datacenter gefaciliteerd kunnen worden zonder dat ze tegen centrale beperkingen aanlopen.

Daarnaast hebben de eilandbesturen belang bij kostenbeheersing. De begrotingen zijn klein, nu betalen ze vrij hoge kosten voor verbindingen en losse IT-oplossingen. Ze hopen dat een gezamenlijke datacenteraanpak op termijn schaalvoordeel oplevert en de kosten per dienst omlaag brengt. Ook willen ze ontzorgd worden op technisch vlak, niet elk eiland wil een heel IT-team voor serverbeheer opzetten of heeft de mogelijkheden om dit te doen. Men ziet graag een scenario waarbij basisdiensten centraal geregeld zijn en zij zich kunnen richten op het functionele gebruik.

4.2 Rijksdiensten op de eilanden

Verschillende Nederlandse rijksdiensten opereren in Caribisch Nederland. Voorbeelden zijn de Belastingdienst CN (BCN), Douane, Politie (KPCN), IND, Marechaussee (KMar), Rechtshandhaving/OM, Zorg en Jeugd Caribisch Nederland (ZJCN), Rijksvastgoedbedrijf (RVB) en RCN-unit SZW. Hun behoeften zijn grotendeels gedreven door hun moederorganisaties in Europees Nederland:

AANSLUITING OP HET RIJKSNETWERK

De Rijksdiensten op de eilanden zijn uitvoeringsorganisaties van ministeries. Ze hebben vaak verbindingen nodig met departementaal specifieke systemen, en veilige koppelingen via het Rijksnet/Diginetwerk. In de toekomst is de verwachting dat met het verdere digitaliseren van Caribisch Nederland de vraag naar deze koppelingen steeds verder toeneemt. Een duidelijke wens is dat de infrastructuur in CN deze connectiviteit betrouwbaar kan leveren. Nu gaan er veel privéverbindingen via VPN over het internet. Men zou bij voorkeur gelijkwaardig aan een regionaal kantoornetwerk in Europees NL worden aangesloten. Dat vereist dat de

datacenters in CN als hub kunnen dienen met redundante, goed beveiligde verbindingen naar de betreffende overheidsnetwerken in Europees Nederland.

Vanuit Caribisch Nederland is het van groot belang om aangesloten te zijn op verschillende rijksnetwerken die in Europees Nederland de basis vormen voor veilige communicatie en digitale overheidsdiensten. Het Rijks OverheidsNetwerk (RON) biedt een beveiligde infrastructuur voor rijksorganisaties en vormt de ruggengraat voor veel interne communicatie. Diginetwerk maakt veilige gegevensuitwisseling mogelijk tussen overheden en ketenpartners, bijvoorbeeld voor sociale zekerheid, justitie of onderwijs. De Generieke Digitale Infrastructuur (GDI) omvat onder andere DigiD, MijnOverheid en Suwinet, die cruciaal zijn voor de digitale dienstverlening aan burgers en bedrijven. Daarnaast zijn koppelingen met zorgnetwerken, zoals het Landelijk Schakelpunt (LSP), en justitiële netwerken zoals JustID noodzakelijk voor een goede samenwerking in het veiligheids- en zorgdomein. Deze netwerken zijn doorgaans alleen toegankelijk via besloten verbindingen, wat de noodzaak onderstreept van een stabiele en goed beveiligde digitale infrastructuur tussen Caribisch en Europees Nederland.

NALEVING VAN RIJKSBELEID EN SECURITY-EISEN

Rijksdiensten hanteren de BIO (Baseline Informatiebeveiliging Overheid) en strikte privacyregels. Daarnaast hanteert het ministerie van BZK voor organisaties die gebruik maken van DigiD voor identificatie en authenticatie van burgers en bedrijven die willen inloggen op hun klantenportaal een aparte set van DigiD beveiligingsnormen die eisen stelt aan de informatiebeveiliging van zowel de applicatie als de onderliggende datacenter-infrastructuur. Vereist is dat elke datacenteroplossing in CN daaraan voldoet, zodat de dataverwerking net zo veilig is als in een datacenter in het Europees deel van Nederland. Bijvoorbeeld logging, monitoring, netwerkscheiding, incident response en toegangsbeveiliging moeten op vergelijkbaar niveau zijn als in Europees Nederlandse ODC's. Dit betekent onderdeel uitmaken van het nationale cybersecuritystelsel en het verkrijgen van een (sectorale) CSIRT. Ten aanzien van het gewenste niveau is in het kader van dit rapport geen nader onderzoek gedaan. De ABDO-eisen (Algemene Beveiligingseisen voor Defensieopdrachten) kunnen worden ingezet als sprake is van een hoger dreigingsniveau. De ABDO richt zich op statelijke actoren, waarvoor ook BIO-Basisbeveiligingsniveau (BBN) 3 was beoogd. De ABDO hanteert daarbij het begrip 'Te Beschermen Belang' (TBB) en kent 4 niveaus van bescherming van specifieke informatie en fysieke objecten: TBB-4 Departementaal Vertrouwelijk, TBB-3 Confidentieel, TBB-2 Geheim, TBB-1 Zeer Geheim. Dit is zowel een eis (ze mogen anders de systemen niet plaatsen in CN) als een behoefte (men wil gerustgesteld zijn dat er geen zwakke schakel is. Uit de DigiD Pre-Check blijkt dat de Caribische organisaties vaak nog niet in staat zijn om te voldoen aan de gestelde criteria om basisvoorzieningen zoals DigiD zelfstandig te implementeren.

PERFORMANCE EN BESCHIKBAARHEID

Sommige rijksdiensten verwerken real-time gegevens (bijv. de IND bij grenscontroles, de Marechaussee bij (lucht)havencontroles, de politie bij raadplegen van opsporingssystemen). Zij hebben behoefte aan lage latency naar hun centrale databases. Dit kan betekenen dat bepaalde kritieke applicaties een lokale cache of kopie krijgen om vertraging te minimaliseren. Voorbeeld: de Authenticatie en Autorisatie infrastructuur (zoals DigiD of ID-bridge) moet vlot werken, mogelijk is daarvoor een lokale proxy of server nodig. Daarnaast mag uitval van de connectie met Europees Nederland niet meteen betekenen dat de dienst stopt. Een lokale fail-over of offline modus voor kernfuncties is gewenst (denk aan de mogelijkheid om tijdelijk paspoorten te verlenen of opsporingshandelingen te doen zonder verbinding met de centrale server, en later te synchroniseren). De beschikbaarheid van betrouwbare, lokale digitale infrastructuur op de BES-eilanden versterkt niet alleen de dienstverlening in Caribisch Nederland, maar bevordert ook de connectiviteit met andere delen van het Koninkrijk, zoals Aruba, Curaçao en Sint-Maarten. Dit is van belang voor onder andere Defensie en de Koninklijke Marechaussee, die op al deze eilanden actief zijn en gebruikmaken van gezamenlijke opsporings- en informatiesystemen. De Stichting Beheer ICT Rechtshandhaving (SBIR) op Curaçao speelt hierbij een centrale rol, door voorzieningen op de BES-eilanden te koppelen aan zowel regionale als landelijke systemen in Europees Nederland. Daarmee wordt ook het grensoverschrijdende karakter van deze diensten beter verankerd in de Nederlandse kaders voor gegevensbescherming en toezicht, en wordt voldaan aan de eisen voor zorgvuldige omgang met persoonsgegevens binnen het Koninkrijk.

ONDERSTEUNINGSTAKEN

Rijksdiensten op de eilanden geven aan dat het hen niet uitmaakt wie de ICT precies levert, zolang storingen maar snel worden opgelost en er één duidelijk aanspreekpunt is. Men wil geen kastje-muur tussen een lokale dienstverlener en een landelijke dienstverlener. Daarom zijn heldere werkafspraken essentieel. SSO-CN kan optreden als lokaal aanspreekpunt voor het datacenter, terwijl de daadwerkelijke exploitatie en het technische beheer in samenspraak plaatsvindt met de verantwoordelijke beheerorganisaties, zoals SSC-ICT, van de ODC's of Logius, afhankelijk van het type dienst of infrastructuurlaag.

INFORMATIEMANAGEMENT

Naarmate de digitalisering toeneemt en meer ketensystemen worden uitgerold, groeit ook de complexiteit van de dienstverlening. Dit vraagt om versterking van de governance, met daarin een duidelijke rol voor informatiemanagement. Informatiemanagers binnen de diensten vervullen een regierol richting de leveranciers, stemmen behoeften en prioriteiten af, en bewaken de aansluiting bij rijksbrede en overheidsbrede voorzieningen en standaarden. Zij zorgen ervoor dat digitale keuzes in lijn zijn met het beleid, de veiligheidseisen en de operationele behoeften van hun organisatie. Zonder deze schakel ontstaat ruis in de afstemming en blijft structurele verbetering uit. De inrichting van deze regiefuncties is dus cruciaal voor stabiele en toekomstbestendige dienstverlening.

APPLICATIELANDSCHAP

De diversiteit aan overheidsdiensten vereist dat de datacenterstrategie aansluit op uiteenlopende applicatielandschappen, van standaard kantoorautomatisering tot specifiek maatwerk. Zo gebruikt de Belastingdienst andere applicaties dan bijvoorbeeld ZJCN (Zorg en Jeugd Caribisch Nederland). Het datacenter moet daarom generieke diensten leveren, zoals o.a. housing, virtuele servers, opslag en netwerkcapaciteit, waarop elke dienst zijn eigen technologie-stack kan draaien, bij voorkeur zonder zware beperkingen en met de mogelijkheid voor de betreffende organisatie om zelf maatwerk te kunnen ondersteunen of uit te besteden.

STANDAARDISATIE ALS UITGANGSPUNT

Standaardisatie moet het uitgangspunt zijn. Dit volgt het 'Pas toe of leg uit' beleid van het Forum Standaardisatie. Sommige belangrijke open standaarden worden te weinig gebruikt, waardoor de digitale samenleving kwetsbaar, inefficiënt of niet toegankelijk is voor iedereen. Daarom geldt voor deze standaarden het 'Pas toe of leg uit'-beleid. De verplichting geldt voor gemeenten, provincies, rijk, waterschappen en alle uitvoeringsorganisaties. Voor alle andere organisaties in de publieke sector geldt het gebruik van de 'Pas toe of leg uit'-standaarden als een dringend advies.

Pas toe

'Pas toe' betekent dat op het moment dat een ICT-product of dienst aangeschaft wordt of zelf wordt ontwikkeld de 'Pas toe of leg uit'-lijst moet worden geraadpleegd. Wanneer de aanschaf of ontwikkeling valt onder een toepassingsgebied dat voorkomt op deze lijst, moet de daar genoemde standaard(en) toegepast worden.

Leg uit

Over de naleving van het open standaarden beleid dient jaarlijks gerapporteerd te worden in de bedrijfsvoeringsparagraaf van het jaarverslag. Afwijkingen van het gebruik van de voorgeschreven standaarden dienen vermeld te worden. Afwijken van het landelijke beleid mag alleen als een standaard in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of om een andere reden die van bijzonder gewicht is. Dit is de betekenis van 'leg uit'.

Dus alleen wanneer zwaarwegende inhoudelijke of wettelijke redenen dit vereisen, kan gemotiveerd worden afgeweken. Om een overheidsdienstverlening te bieden die gelijkwaardig is aan andere delen van het Koninkrijk, zijn uniforme werkwijzen, samenhangende systemen en gedeelde voorzieningen essentieel. Afwijken van standaarden leidt tot versnippering, hogere kosten, complexere beheersituaties en risico's voor continuïteit en veiligheid. De specifieke context van de BES-eilanden vraagt soms om maatwerk, maar dat mag geen vrijbrief zijn voor uitzonderingsposities.

4.3 ZBO's in Caribisch Nederland

In tegenstelling tot rijksdiensten zijn zelfstandige bestuursorganen (ZBO's) formeel zelfstandig en vallen zij niet onder directe ministeriële aansturing. Ze voeren publieke taken uit, maar opereren op grotere afstand van het departement dat verantwoordelijk is voor het beleid. Op de BES-eilanden zijn diverse ZBO's actief, waaronder het Kadaster, Kamers van Koophandel en Nijverheid, De Nederlandsche Bank, het CBS, de Commissie bescherming persoonsgegevens BES, de Raad voor Rechtsbijstand en de AFM. Deze ZBO's hebben hun eigen wettelijke basis en bestuursstructuur, en hanteren soms afwijkende standaarden of werkprocessen ten opzichte van rijksdiensten. Ze maken wel gebruik van vergelijkbare digitale voorzieningen, zoals koppelingen met landelijke registraties en toegang tot beveiligde netwerken, maar ze vallen buiten de centrale regie van departementale ICT-sturing.

4.4 Centrale ministeries

De ministeries vervullen als beleidsmatige stakeholders een rol in het bewaken van het bredere overheidsbelang. Hun inbreng richt zich daarom primair op het stellen van kaders en randvoorwaarden, en niet op de dagelijkse operationele uitvoering.

RECHTMATIGHEID EN REGULERING

BZK (Directoraat Digitalisering) wil dat de oplossing voldoet aan wet- en regelgeving en past binnen architectuurkaders. Denk aan het voldoen aan het Nationaal beveiligingsbeleid, gebruik van open standaarden, en aansluiting op bestaande overheidsbrede voorzieningen (zoals de Rijkscloudstrategie, overheids-DNS, logging naar het SOC van de Rijksoverheid, etc.). Men vraagt bijvoorbeeld om verplichte veiligheidsassessments en privacy impact assessments vooraf, en om continu te monitoren dat de data van het Caribisch deel van Nederland onder Nederlands juridisch regime blijven. Soevereiniteit is voor de Rijksoverheid een belangrijk thema, data van Nederlandse burgers moeten in principe in Nederland of binnen de EER blijven, of anders met passende waarborgen elders.

KOSTENBEWUSTZIJN EN EFFICIËNTIE

De datacenteropzet moet kosteneffectief zijn en bij voorkeur op langere termijn besparingen opleveren door schaal en shared services ten opzichte van de huidige situatie. Investeringen moeten te verantwoorden zijn. Idealiter wordt ook gekeken of er synergie is met bestaande datacentra, bijvoorbeeld of de capaciteit van een Overheidsdatacenter in het Europees deel van Nederland benut kan worden voor het Caribisch deel van Nederland (redundantie) in plaats van dubbel investeren.

STAATKUNDIGE EN BELEIDSMATIGE POSITIE VAN DE BES-EILANDEN BINNEN NEDERLAND EN RELATIE MET DE CARIBISCHE LANDEN

De BES-eilanden maken integraal deel uit van Nederland. Burgers en bedrijven hebben daardoor dezelfde klassieke en sociale grondrechten als in Europees Nederland. Afwijkingen zijn alleen toegestaan wanneer er sprake is van bijzondere omstandigheden. Voor wetgeving en beleid geldt daarom het uitgangspunt van een gelijkwaardig voorzieningenniveau.

Nederland draagt géén verantwoordelijkheid voor digitalisering op Aruba, Curaçao en Sint-Maarten. Digitalisering – en aanverwante thema's – zijn bovendien geen Koninkrijksaangelegenheid. Voor de BES ligt de focus op volwaardige deelname aan de Nederlandse digitale overheid. Samenwerking met Aruba, Curaçao en Sint-Maarten kan nuttig zijn bij vergelijkbare uitdagingen, mits dit de ontwikkeling op de BES niet belemmert.

CONTINUÏTEIT VAN BELEID EN REGIE

Ministeries vragen om heldere sturingslijnen. Zij hebben behoefte aan een governancestructuur (uitgewerkt in hoofdstuk 10) waarin BZK de regie voert op de uitvoering en het beleid voor de digitale overheidsinfrastructuur, EZK verantwoordelijk is voor de marktordening en digitale connectiviteit in het Caribisch deel van Nederland, de openbare lichamen bestuurlijk meesturen en SSO-CN de operationele uitvoering verzorgt.

4.5 Burgers, bedrijven en overige indirecte stakeholders

Hoewel burgers en bedrijven niet direct betrokken zijn bij dit rapport, zijn zij uiteindelijk wél de eindgebruikers die de gevolgen ondervinden van de keuzes in de datacenterstrategie. De focus van dit rapport ligt op overheids-ICT, maar de effecten strekken zich uit naar bredere publieke dienstverlening in Caribisch Nederland. Instellingen met een publieke functie – zoals ziekenhuizen, brandweer, scholen, lucht- en zeehavens, water- en energiebedrijven – en de Openbare Lichamen zelf, zijn essentieel voor de leefbaarheid op de eilanden. Hun kritieke rol in de lokale infrastructuur vraagt om betrouwbare digitale ondersteuning. Deze organisaties moeten daarom kunnen meeliften op de centrale datacenterfunctionaliteiten en connectiviteit, al dan niet via de Openbare Lichamen. De kwaliteit van deze digitale infrastructuur bepaalt mede hoe effectief de overheid haar dienstverlening aan burgers en bedrijven kan verbeteren.

BETERE DIENSTVERLENING

Uitgangspunt van dit rapport is dat burgers en bedrijven verwachten dat de fysieke- en digitale diensten van de overheid betrouwbaar en probleemloos functioneren. Of het nu gaat om het aanvragen van een uittreksel, digitaal belastingaangifte doen of een zorgvergoeding aanvragen, als de achterliggende systemen traag of vaak offline zijn, frustreert dat en leidt het tot vertrouwensverlies. Ze hebben dus baat bij de verhoogde snelheid (lagere latency) en stabiliteit die een lokaal datacenter kan bieden voor diensten die nu wellicht ver weg gehost zijn. Tevens verwachten ze dat hun persoonsgegevens goed beschermd worden, ongeacht waar die opgeslagen zijn. Ze rekenen erop dat de overheid hun gegevens beschermt.

ECONOMISCHE IMPULS

Lokale bedrijven kunnen direct profiteren als de overheid haar ICT lokaal onderbrengt, via opdrachten in de bouw/voorziening van het datacenter, of via deelname in aanbestedingen voor beheer, etc. Indirect profiteren bedrijven als de kosten om zaken te doen afnemen, dat versterkt het vestigingsklimaat. Deze impliciete behoefte (economische ontwikkeling) betekent dat een datacenterproject idealiter ook de lokale economie niet schaadt maar juist kansen biedt. Bijv. door training van lokale IT'ers, of door de faciliteit eventueel ook beschikbaar te stellen als hub waar bedrijven hun servers kunnen 'co-locaten' in de toekomst – uiteraard onder voorwaarden.

SOCIAAL-MAATSCHAPPELIJK

De eilanden kennen een hechte gemeenschap. Men hecht belang aan eigen capaciteit opbouwen. Een overheidsdatacenter kan jonge professionals aantrekken of opleiden, wat past in het beeld van zelfredzaamheid van de eilanden. Aan de andere kant dienen inefficiënte investeringen voorkomen te worden. Dus er zal draagvlak ontstaan als men ziet dat het praktisch nut heeft (snellere service, minder storingen, lagere kosten voor internet). Transparante communicatie naar de bevolking over de voordelen is hierbij dus belangrijk.

RÉSUMER

In de verdere analyse houden we rekening met al deze stakeholders. Hun behoeften vertalen zich in criteria en uitgangspunten. De behoefte aan betrouwbaarheid en hoge beschikbaarheid leidt bijvoorbeeld tot het criterium continuïteit. De wens tot ontzorging en flexibiliteit vertaalt zich in de manier waarop we varianten beoordelen op beheerlast en schaalbaarheid.

Samenvattend geven de verschillende stakeholders aan dat hun voornaamste behoefte ligt bij een robuuste, veilige en toekomstbestendige oplossing. Dit benadrukt de noodzaak van een gezamenlijke aanpak om aan hun uiteenlopende verwachtingen te voldoen. De mogelijkheden die hierbij overwogen worden, variëren van het afnemen van eenvoudige housingdiensten tot het gebruik van een IaaS-, PaaS- of SaaS-platform, waarbij het beheer mogelijk bij een derde partij kan liggen. Bijvoorbeeld, applicatiebeheer kan worden uitbesteed via een IaaS-platform. De nuance tussen de stakeholders zit hem in de specifieke accenten die zij leggen: lokaal bestuur benadrukt het belang van lokale zeggenschap en lokale aanwezigheid, lokale rijksdiensten richten zich op security en aansluiting met andere systemen, de ministeries leggen de nadruk op regie en compliance, en de overheidsgebruikers, burgers en bedrijven verwachten vooral goede prestaties en gebruiksgemak. In de volgende hoofdstukken zullen we deze inzichten verder uitwerken door expliciet de strategische

uitgangspunten en randvoorwaarden te formuleren die tegemoetkomen aan de behoeften van alle betrokken partijen.

Stakeholder(s)	Belangrijkste behoeften / eisen	Bijzonderheden / Toelichting
Openbare Lichamen	- Betrouwbare basisvoorzieningen (hoge beschikbaarheid, lokale redundantie) - Lokale zeggenschap en flexibiliteit - Kostenbeheersing en ontzorging	Kleine budgetten en beperkte IT-capaciteit; behoefte aan functionele autonomie, gekwalificeerde en ervaren assistentie en schaalvoordeel
Rijksdiensten op de eilanden	- Aansluiting op Rijksnetwerken (RON, Diginetwerk, GDI) - Voldoen aan BIO security eisen (o.a.) - Performance/latency en lokale fail-over - Servicedesk, governance en standaardisatie	Afhankelijk van ministeries in Europees Nederland; eisen gelijkwaardig aan Europees-NL niveau
ZBO's	- Soortgelijke digitale voorzieningen als rijksdiensten - Eigen standaarden en processen	Formeel zelfstandig; vallen buiten departementale ICT-sturing.
Centrale ministeries	- Regie en compliance (wet- en regelgeving, architectuurkaders) - Kostenbewustzijn en efficiëntie	Beleidsmatig kaderstellend; bewaken bredere overheidsbelang, focus op standaardisatie
Burgers, bedrijven en indirecte stakeholders	- Verwachting van betrouwbare en snelle digitale dienstverlening - Vertrouwen in gegevensbescherming - Mogelijke economische impuls - Bijdrage aan sociale cohesie	Niet direct betrokken maar wel eindgebruikers. Verwachten goede prestatie, bescherming en communicatie

5 STRATEGISCHE UITGANGSPUNTEN

Voor de vormgeving van de datacenterstrategie is een set strategische uitgangspunten vastgesteld. Deze zijn gebaseerd op geldende wet- en regelgeving, rijks- en lokaal overheidsbeleid, en specifieke randvoorwaarden voor Caribisch Nederland. De uitgangspunten zijn gezamenlijk ontwikkeld en gevalideerd binnen de werkgroep en kerngroep, waarin inhoudelijke expertise uit beleid, uitvoering en techniek bijeen is gebracht. Ook de kennis en ervaring van Highberg is hierin meegenomen. Het resultaat is een zorgvuldig onderbouwde set van uitgangspunten die richtinggevend is voor de strategische keuzes. In dit hoofdstuk worden deze uitgangspunten toegelicht. Ze vormen het toetsingskader voor de scenario-varianten; varianten die hiermee in strijd zijn, worden als onwenselijk beschouwd.

1. EU-REGELGEVING ALS LEIDRAAD, DATA-OPSLAG BINNEN EER OF OP EU-NIVEAU IN CN

Hoewel het Caribisch deel van Nederland buiten de EER valt is het wenselijk om EU-regelgeving wel als leidraad te nemen. Dat komt doordat Europees Nederland wél moet voldoen aan EU-regelgeving, en overheidsdiensten in Caribisch Nederland in toenemende mate moeten koppelen met systemen en netwerken in Europees Nederland. Naarmate de Europese compliance-eisen verder toenemen, wordt het zonder aansluiting op deze regelgeving steeds moeilijker – zo niet onmogelijk – om veilig, rechtmatig en efficiënt samen te werken binnen ketens die EU-compliant zijn. Zo hanteert de Rijksoverheid voor zichzelf de AVG als uitgangspunt om een gelijkwaardig beschermingsniveau van persoonsgegevens te waarborgen. Daarnaast wordt wetgeving voorbereid om de huidige bescherming van persoonsgegevens op de eilanden voor iedereen te verhogen tot AVG-niveau. Zolang het wettelijke beschermingsniveau op de eilanden nog niet op AVG-niveau zit geldt dat voor de Rijksoverheid de opslag of verwerking van persoonsgegevens buiten de EER alleen acceptabel is als aanvullende juridische waarborgen, zoals Standaard Contractuele Clausules (SCC's) of een DPIA, worden toegepast. De voorkeur gaat uit naar opslag binnen Nederland of de EER, tenzij aan alle beveiligings- en privacy-eisen wordt voldaan. Voor andere overheidsorganisaties, zoals gemeenten, ZBO's of uitvoeringsinstanties die opereren in Caribisch Nederland, geldt in de praktijk vaak hetzelfde uitgangspunt: aansluiting bij het AVG-niveau is wenselijk of zelfs noodzakelijk om koppelingen met rijksvoorzieningen mogelijk te maken en compliant te blijven met Nederlandse en Europese standaarden. De BES-eilanden vallen onder de Wet bescherming persoonsgegevens BES (Wbp BES), die vergelijkbare eisen stelt als de AVG, maar niet een gelijkwaardig beschermingsniveau biedt. Voor gegevensverwerking buiten de EER moeten extra waarborgen worden genomen.

2. INFORMATIEBEVEILIGING VOLGENS CYBERSECURITYSTELSEL, BIO VERSIE 2 EN NIS2-READY ARCHITECTUUR

De datacenterstrategie vereist aansluiting op het overheidsbrede cybersecuritystelsel, met BIO versie 2 als norm en een 'NIS2-ready' architectuur als ontwerpeis. Dit is noodzakelijk om aantoonbaar invulling te geven aan de digitale zorgplicht en voorbereid te zijn op strengere wetgeving zoals de Cyberbeveiligingswet.

BIO versie 2 – gebaseerd op ISO 27001 – is leidend voor de Rijksoverheid en stelt eisen aan fysieke, logische en organisatorische beveiliging. Deze normen gelden ook wanneer diensten deels buiten Caribisch Nederland worden gehost. Hoewel de NIS2- en CER-richtlijnen momenteel nog niet gelden in CN, worden deze vanaf 2025 via de Wet aanpak digitale bedreigingen (Wadb) geïntegreerd in BIO. Daarmee ontstaat bestuurlijke verantwoordelijkheid voor digitale weerbaarheid, ook voor lokale uitvoeringsorganisaties.

De architectuur moet daarom aantoonbaar informatiebeveiliging borgen vanaf ontwerp ("security by design") en voldoen aan toetsbare normen. Verantwoording over de staat van beveiliging moet mogelijk zijn op basis van meetbare standaarden. Verder is de aanwezigheid van een Security Operations Centre (SOC) en aansluiting op een Computer Emergency Response Team (CERT) essentieel om incidenten tijdig op te vangen. Ook als dat juridisch (nog) niet verplicht is, geldt het als noodzakelijke invulling van risicobeheersing en zorgplicht.

Gebruik van Amerikaanse cloudleveranciers is alleen toegestaan onder strikte voorwaarden, zoals volledige encryptie, een uitgevoerde DPIA en een expliciete risicoafweging. Leveranciers die niet kunnen aantonen dat zij voldoen aan certificerings- en auditvereisten vallen buiten de strategie – dit in lijn met het huidige en toekomstige Rijksbrede cloudbeleid.

3. DIGITALE SOEVEREINITEIT

De strategie stelt als harde voorwaarde dat overheidsdata onder Nederlandse regie en juridische controle blijft, via eigen of Nederlandse/EU-infrastructuur. Dit is nodig om toegang door buitenlandse wetgeving – zoals de Amerikaanse Cloud Act – te voorkomen en publieke informatie beschermd te houden.

Zonder soevereiniteit over locatie, toegang en beheer kan een buitenlandse partij afdwingen dat data wordt vrijgegeven. Dit is onwenselijk bij bijvoorbeeld public cloud-constructies waarbij de overheid onvoldoende controle heeft over de opslag, encryptie of doorgifte van data. Daarom moeten technische en juridische afhankelijkheden van niet-EU partijen waar mogelijk actief worden vermeden. Constructies waarbij dataverkeer via derde landen verloopt of een private partij alle beheersrechten heeft zonder tegenmacht vanuit de overheid, zijn ontoelaatbaar.

Alleen wanneer versleuteling is toegepast met sleutels die uitsluitend de overheid bezit ("sovereign controls"), en data aantoonbaar binnen de EU blijft, kan gebruik van buitenlandse infrastructuur eventueel worden overwogen. Maar zelfs dan gaat de voorkeur uit naar oplossingen met volledige zeggenschap: een overheidsdatacenter (ODC) of een eigen twin-datacenter scoort het hoogst op soevereiniteit, terwijl generieke public cloud, zeker van niet-EU partijen, het laagst scoort.

De mate waarin deze digitale soevereiniteit daadwerkelijk kan worden gewaarborgd, hangt nauw samen met de fysieke en juridische controle over netwerkverbindingen. De verdere uitwerking van deze connectiviteitsstrategie, inclusief de afweging tussen nieuwe rechtstreekse verbindingen en het benutten van bestaande kabelsystemen met dedicated capaciteit, is opgenomen in hoofdstuk 7.

4. PASSEND BIJ CONTEXT CARIBISCH NEDERLAND

De strategie kiest expliciet voor een opzet die past bij de schaal, omstandigheden en bestuurlijke context van Caribisch Nederland. Een generiek model gebaseerd op Europese infrastructuur is ongeschikt; de situatie vraagt om maatwerk dat werkbaar en uitvoerbaar is binnen de lokale realiteit.

De BES-eilanden kennen unieke omstandigheden zoals een tropisch klimaat, beperkte lokale IT-capaciteit (in kennis, mensen en middelen), en kwetsbare logistieke ketens. Dat maakt het onmogelijk om simpelweg bestaande rijksmodellen over te nemen. De oplossing moet schaalbaar en onderhoudbaar zijn, en juist niet te grootschalig, complex of afhankelijk van externe expertise.

Scope CN is daarom méér dan een technische afbakening: het is ook een bestuurlijke randvoorwaarde. Governance moet zodanig worden ingericht dat de belangen van Caribisch Nederland structureel zijn geborgd binnen het bredere overheidsbrede ICT-domein. Dit vereist duidelijke afspraken tussen BZK en de Openbare Lichamen, ZBO's, uitvoeringsorganisaties en overige stakeholders over serviceniveaus, escalatielijnen en mandaten. Samenwerking is wenselijk, maar deelname moet niet automatisch worden verondersteld. De autonomie van de eilanden moet worden gerespecteerd; er mag geen impliciete verplichting uitgaan van centrale keuzes.

Generieke varianten die geen rekening houden met lokale risico's – zoals de impact van een kabelstoring op Saba – missen realiteitszin. Wat in de Randstad werkt, kan in CN disproportioneel of zelfs onhoudbaar zijn. In de praktijk ervaren de eilanden momenteel een lagere prioriteit vanuit Europees Nederland. Daarom moet governance ook zó worden ingericht dat prioritering inzichtelijk, toetsbaar en gedeeld tot stand komt.

5. AANSLUITEN OP VOORGENOMEN BELEID

De datacenterstrategie wordt expliciet gepositioneerd als verlengstuk van het nationale digitaliseringsbeleid, met nadruk op publieke regie, interoperabiliteit en aansluiting op de Generieke Digitale Infrastructuur (GDI). Deze koers sluit aan op recente beleidsverschuivingen waarin publieke waarden en zeggenschap over data centraal staan.

Waar het eerdere cloudbeleid nog ruimte liet voor decentrale keuzes, is de lijn sinds 2023 aangescherpt. Onder invloed van rapporten van de Algemene Rekenkamer en aangenomen Kamerbreed gesteunde moties is de Rijksoverheid overgegaan op een strakker afwegingskader. Publieke controle, transparantie en het beperken van buitenlandse afhankelijkheden wegen daarin zwaarder dan voorheen. Deze herijking raakt direct aan de

keuzes voor Caribisch Nederland: de strategie mag geen geïsoleerde, eilandgerichte voorziening zijn, maar moet aantoonbaar passen binnen het overheidsbrede raamwerk van de GDI.

Dat betekent ook dat bestaande publieke voorzieningen en bouwstenen, zoals DigiD, CSIRT of koppelingen met Overheidsdatacenters, leidend zijn zodra die beschikbaar zijn. Lokale alternatieven of eigenstandige oplossingen zijn alleen passend als die in lijn zijn met het landelijke referentie-architectuurkader (NORA) en voorbereid zijn op integratie met toekomstige generieke voorzieningen.

De strategie moet daarom niet alleen technisch, maar ook bestuurlijk ingebed zijn in overheidsbrede digitaliseringsambities. Geen lokale improvisatie, maar hergebruik van bewezen standaarden, consistentie met landelijk beleid, en expliciete borging van publieke belangen vormen de kern.

6. WEERBAARHEID EN CONTINUÏTEIT

Elke strategische variant moet aantoonbaar bestand zijn tegen storingen of aanvallen zonder langdurige uitval van publieke dienstverlening. Weerbaarheid en continuïteit zijn geen wens, maar harde ontwerpcriteria: technische en organisatorische maatregelen moeten vanaf de start integraal zijn meegenomen.

Dat betekent dat de architectuur minimaal moet bestaan uit redundante datacenters, noodstroom, dubbele verbindingen, en een beheeromgeving die bij calamiteiten direct kan schakelen. Denk aan scenario's waarin een orkaan een eiland treft: systemen moeten kunnen blijven functioneren of direct kunnen worden hersteld. Ook bij een cyberaanval zoals ransomware moet de infrastructuur toegang hebben tot veilige offline backups en uitwijkmogelijkheden. De gestelde continuïteitseisen (zoals RTO en RPO) vormen daarbij het toetsingskader.

In gesprekken met stakeholders is uitgesproken dat maximaal 24 uur uitval acceptabel is – het liefst minder. Deze eis wordt daarom niet slechts als uitgangspunt gehanteerd, maar als harde beoordelingsmaatstaf voor scenario's in hoofdstuk 9. Sommige varianten bieden immers structureel betere continuïteit dan andere. Alleen varianten met minimaal twee geografisch gescheiden locaties en concrete noodgevalsvoorzieningen komen in aanmerking.

Tot slot geldt dat technische maatregelen alleen niet volstaan. Ook de organisatorische paraatheid moet op orde zijn: inrichting van een Security Operations Centre (SOC) en aansluiting op een CERT zijn noodzakelijk om snel te reageren wanneer de continuïteit onder druk komt te staan.

7. ONTWIKKELKRACHT EN CAPACITEIT IN CN

De strategie kiest voor een datacenteropzet die uitvoerbaar is met de beschikbare capaciteit op de eilanden. Omdat het aantrekken en behouden van gespecialiseerd personeel al jaren een knelpunt vormt, mag continuïteit niet afhankelijk zijn van schaarse experts.

Het ontwerp moet daarom zo worden ingericht dat lokale medewerkers beheertaken op termijn zelfstandig kunnen uitvoeren, ondersteund door opleiding, taakverdeling en waar nodig ondersteuning op afstand. Tegelijk moet de infrastructuur voorbereid zijn op toekomstige groei: schaalbaar in capaciteit, modulair uitbreidbaar en beheerbaar zonder overbelasting.
Volledig door externe partijen beheerde varianten kunnen efficiënt zijn, maar leveren weinig kennisoverdracht. Andersom overschrijden volledig lokaal beheerde modellen vaak de draagkracht van kleine organisaties. De juiste balans ligt in benutting van bestaande capaciteit (zoals SSO-CN en lokale resources), gecombineerd met een realistische inschatting van wat lokaal haalbaar is – nu én over vijf jaar.
Deze balans tussen uitvoerbaarheid en ontwikkelkracht moet expliciet worden vastgelegd in de verdere uitwerking van de strategie, zodat rollen, verantwoordelijkheden en ontwikkeltempo helder zijn.

8. CENTRALE REGIE EN DUIDELIJKE AFSPRAKEN

De datacenterstrategie vereist één duidelijke regierol, bij voorkeur belegd bij BZK, om afstemming tussen Rijk, Openbare Lichamen en uitvoeringsorganisaties te waarborgen. Heldere governance voorkomt versnippering, voorkomt onduidelijkheid over verantwoordelijkheden, en maakt uitvoering bestuurlijk beheersbaar.

Omdat het programma meerdere bestuurslagen raakt, is een gedeeld sturingsmodel essentieel. Dit betekent: duidelijke afspraken over verantwoordelijkheden, financiële bijdragen, escalatiestructuren en eigenaarschap. Denk aan centrale afspraken in de vorm van Service Level Agreements (SLA's), Dienstafnameprofielen (DAP's) per partij en een stuurgroep waarin Rijk én eilanden zijn vertegenwoordigd. Bij voorkeur sluit dit aan op bestaande structuren zoals het Bestuurlijk Overleg Koninkrijksrelaties, of wordt er een specifiek overleg ingericht gericht op digitalisering in Caribisch Nederland.

Ook richting marktpartijen geldt: één regiepunt. Fragmentatie, waarbij lokale en landelijke partijen elkaar bij problemen de verantwoordelijkheid toeschuiven, moet worden voorkomen. Dit principe sluit direct aan op de bredere Rijksdoelstelling om "als één overheid" te opereren richting burgers en organisaties. Intern mag het beheer gedifferentieerd zijn, maar bestuurlijk en operationeel moet het als één geheel functioneren.

Varianten die qua regie en governance complex zijn, met bijvoorbeeld veel verschillende leveranciers en onduidelijk eigenaarschap, zijn daarom minder aantrekkelijk binnen deze strategie.

Bovenstaande acht strategische uitgangspunten vormen de toetsingscriteria op de varianten in hoofdstuk 9.

6 TOEKOMSTIGE HUISVESTING VAN DATACENTERFACILITEITEN BES

Een kernvraag in de datacenterstrategie is waar de fysiek-technische infrastructuur ("housing") het beste kan worden ondergebracht. Dit hoofdstuk richt zich daarom op de huisvesting van datacenterfaciliteiten binnen Caribisch Nederland. Er wordt verkend welke locaties potentie hebben, welke eisen het klimaat en de omgeving stellen, en wat de voordelen en beperkingen zijn van lokale huisvesting. De nadruk ligt hierbij op wat er nodig is voor de realisatie van een datacenter op Bonaire, Sint Eustatius en/of Saba.

Strategische varianten die uitgaan van datacenterfaciliteiten buiten de BES-eilanden worden behandeld in hoofdstuk 10 (Samenwerkingsmogelijkheden). Hoewel de formele toetsing aan de strategische uitgangspunten pas in hoofdstuk 9 plaatsvindt, worden in dit hoofdstuk al verschillende aspecten verkend die nauw op die uitgangspunten aansluiten.

6.1 Mogelijke locaties en opzet

Van de drie BES-eilanden is Bonaire het meest geschikt als primaire locatie voor een centraal datacenter. Bonaire is het grootste eiland qua bevolking en economie, heeft de beste bestaande infrastructuur (relatief stabiel stroomnet, voldoende ruimte) en ligt geografisch iets zuidelijker, net buiten het hart van de orkaanzone (al blijft voorbereiding op zware stormen vereist). Een logisch uitgangspunt is daarom dat een datacenter op Bonaire staat. Een mogelijke locatie is de huidige serverfaciliteit(en) van RCN/SSO-CN in Kralendijk, daar is al een basis. Echter, die ruimte is beperkt. Een nieuwbouw of verbouw is waarschijnlijk nodig. Denkbaar is een locatie nabij Kralendijk met goede verbindingen, bijvoorbeeld op of naast het terrein van het water- en energiebedrijf (WEB) waar al redundante stroomvoorzieningen zijn, of op een van de overheidskavels bij het ZKV (Zakenkantoor) waar veel overheidsdiensten zijn geconcentreerd. Een andere optie is het terrein bij de telecommunicatietoren van TELBO, aangezien daar glasvezel samenkomt. In alle gevallen moet de locatie hoog genoeg liggen (om niet door zeewater/overstroming bedreigd te worden) en goed bereikbaar zijn voor onderhoud en verbindingen. Bouw een locatie vanaf de fundering op als een datacenter, met het eigendom volledig (of zover mogelijk) in eigen hand, op een veilige en beveiligde locatie. Bijvoorbeeld op of nabij de Politie- of militair terrein.

Voor Saba en Sint Eustatius geldt dat deze qua schaal kleiner zijn en meer uitdaging hebben in nutsvoorzieningen (de stroomproductie is kleinschalig, er zijn vaker uitvalmomenten). Deze eilanden komen in beeld als potentiële locatie voor eventueel een kleiner datacenter. Dit datacenter zal echter aan dezelfde gestelde eisen moeten voldoen als de locatie op Bonaire. Plaatsing op een bewaakt terrein, zoals politie of militair terrein vult reeds een aantal eisen in. Bijvoorbeeld een robuuste container-datacenterunit(s) nabij het lokale telecomknooppunt, die dienst kan doen om kritieke en lokale diensten draaiende te houden als de verbinding met Bonaire wegvalt. Zo'n locatie kan de systemen bevatten die lokaal op Saba en Statia gebruikt worden, voor latency gevoelige toepassingen en de latency zo laag mogelijk te houden, maar ook de back-up voor Bonaire. Als Bonaire door een storing tijdelijk onbereikbaar is, kunnen Saba en Sint Eustatius grotendeels zelfstandig blijven functioneren. Tegelijkertijd fungeert het datacenter op de bovenwindse eilanden als uitwijklocatie voor Bonaire. Zodra de connectiviteit is hersteld, kunnen de systemen worden gesynchroniseerd, waardoor de continuïteit van gegevens en dienstverlening behouden blijft. Data of systemen die niet zo cruciaal zijn dat deze specifieke uitwijkvoorzieningen nodig hebben, kunnen alleen op Bonaire draaien, omdat daar meer capaciteit beschikbaar is. Back-ups kunnen in alle gevallen wel over-en-weer geografisch veiliggesteld worden.

Een alternatief scenario voor huisvesting is om te kijken naar regionale hubs buiten BES. Curaçao heeft bijvoorbeeld een modern datacenter (Blue NAP Americas) dat hurricane-proof is gebouwd en regionaal diensten aanbiedt. In theorie zou Caribisch Nederland capaciteit kunnen inkopen of samen exploiteren in zo'n faciliteit. Dit valt echter onder uitbesteding en verplaatst de huisvesting dus naar een buurland, wat gevolgen heeft voor jurisdictie en regie-mogelijkheden.

Gebruik van defensieterrein is nog genoemd als mogelijkheid, op Bonaire is er bijvoorbeeld defensie-infrastructuur (de Marinekazerne/Marinierscampus in ontwikkeling). Het verdient de aanbeveling om de mogelijkheden tot een Gemeenschappelijke Strategische Samenwerking (GSS) nader te onderzoeken. De scope

van dit rapport is primair een datacenter voor civiel (niet-militair) gebruik. Echter wordt dit door de scope van de strategie niet beperkt tot alleen civiel gebruik.

6.2 Eisen aan faciliteit en ontwerp

Een datacenter op de eilanden moet voldoen aan een reeks technische en operationele eisen, grotendeels vergelijkbaar met een datacenter in Europees Nederland, maar met enkele tropische accenten:

BOUW EN ORKAANBESTENDIGHEID

Het gebouw (of container) moet bestand zijn tegen extreem weer, met name orkaanwinden van categorie 4-5 en vliegend puin. Dit betekent dikke muren of een betonnen behuizing, extra verankering van daken, luiken voor ramen of liever geen ramen, en plaatsing van kritieke hardware niet op begane grond i.v.m. mogelijke wateroverlast. Blue NAP op Curaçao is een voorbeeld van zo'n hurricane-proof design. Daar zijn o.a. speciale stormluiken en redundante koeling geplaatst. Voor Bonaire geldt iets minder orkaanrisico dan op de bovenwindse eilanden, maar het moet toch meegenomen worden. Aardbevingen zijn weinig voorkomend, maar in de constructie van het datacenter wordt geadviseerd dit toch mee te nemen (zeker op Saba of Sint Eustatius die iets dichter bij de vulkanische regio liggen).

STROOMVOORZIENING

Betrouwbare elektriciteit is cruciaal en uitdagend op de eilanden. Uitval komt vaker voor dan in Europees Nederland. Daarom moet een datacenter minimaal een noodstroomaggregaat hebben met ruime brandstofvoorraad voor enige dagen, en UPS-batterijen om de paar seconden tot minuten te overbruggen tussen netuitval en generatorstart. Daarnaast is het zinvol om te investeren in duurzame energie ter plaatse. Zonnepanelen op het dak van het datacenter kunnen een deel van het verbruik compenseren. Dat vermindert niet alleen kosten, maar biedt ook enige continuïteit als het net uitvalt (overdag). De capaciteit van stroomvoorziening moet worden berekend op de verwachte belasting plus groei. Wellicht wordt in eerste instantie maar een deel van het rackoppervlak gevuld met apparatuur, maar de transformatoren, bekabeling en koeling moeten al ontworpen zijn op volledige bezetting.

KOELING EN KLIMAATHUISHOUDING

Het tropische klimaat (gehele jaar ~30°C, hoge luchtvochtigheid) stelt andere eisen aan koeling dan Europees Nederland. Free-to-air koeling (koude buitenlucht doorlaten) is nauwelijks mogelijk, behalve misschien 's nachts een paar graden koeler. Dus efficiënte airconditioning of vloeistofkoeling is nodig. Redundante koeling (N+1 of 2N) is vereist zodat bij uitval van één airco de ander het kan overnemen. Men moet ook rekening houden met zout in de lucht dicht bij zee vanwege corrosiegevaar. Luchtfilters en mogelijk overdruk in de serverruimte kunnen helpen om zoute, vochtige lucht buiten te houden.

NETWERKVERBINDINGEN

De locaties moeten aangesloten worden op zoveel mogelijk beschikbare telecominfrastructuren. Idealiter komen er twee (of meer) geografisch gescheiden kabeltracés het datacenter binnen, bijvoorbeeld in het geval van Bonaire, één tracé vanuit de kabellanding bij Harbour Village, één vanaf een alternatieve route en naar de lokale telecomaanbieders. Bij Saba en Statia kan gekozen worden voor landingsplaatsen anders dan die van de bestaande SSCS. Samenwerking met lokale telecompartijen zoals Telbo/UTS, FTV, Satel en Eutel zijn nodig om redundante last-mile verbindingen te realiseren en lokale verkeersafhandeling voor de inwoners en bedrijven mogelijk te maken. Binnen het datacenter moet netwerkapparatuur redundant uitgevoerd en verbonden zijn met zowel de lokale internetproviders als de dedicated verbindingen voor de eilanden onderling, en naar Europees Nederland (als die worden gerealiseerd).

FYSIEKE BEVEILIGING EN SEGMENTERING

Toegang dient beperkt te zijn tot geautoriseerd personeel. Dit vraagt om een degelijke omheining (indien standalone gebouw), cameratoezicht, toegangscontrole (Bijv. badges, biometrie) en 24x7 monitoring. Overwogen kan worden om remote monitoring (deels) vanuit Europees NL te laten plaatsvinden, en periodiek fysieke controlerondes via beveiligingsdienst ter plaatse.

Daarnaast dient de mogelijkheid te bestaan het datacenter in verschillende ruimten in te delen. Binnen de BIO (Baseline Informatiebeveiliging Overheid) worden verschillende Beveiligingsniveaus (BBN's) gehanteerd om de vereiste beveiligingsmaatregelen af te stemmen op het belang en de gevoeligheid van de informatie. Er zijn vier niveaus: BBN1 (laag), BBN2 (gemiddeld), BBN3 (hoog) en eventueel ABDO/TBB (defensie), waarbij elk niveau strengere eisen stelt aan onder meer fysieke beveiliging, toegangscontrole, detectie en monitoring. Voor datacenters betekent dit onder andere dat bij hogere BBN's strengere eisen gelden voor bouwkundige beveiliging, zoals zwaarbeveiligde (mogelijk gescheiden) ruimtes, toegangsregistratie met meerfactorauthenticatie, continue cameratoezicht en het beperken van toegang tot geautoriseerd personeel. Zo moet bij BBN3 bijvoorbeeld sprake zijn van 24/7 toezicht, inbraakdetectie en gecontroleerde bezoekersregistratie, om de vertrouwelijkheid, integriteit en beschikbaarheid van overheidsinformatie te waarborgen. Zo zou er een scheiding gemaakt kunnen worden van waar bijvoorbeeld overheidsdata met hogere BBN-classificatie geplaatst is, en ruimten waar ook derde partijen vrijer toegang krijgen en het beheer over overheidssystemen mogen uitvoeren (indien gewenst door de betreffende instanties).

OPERATIONS-RUIMTE EN WERKPLEK

Naast de technische ruimte (machine room) dient het datacenter te beschikken over een functionele kantoor- en werkruimte die is ingericht voor beheerders en ondersteunend personeel. Deze ruimte moet voorzien zijn van basisvoorzieningen zoals werkplekken met toegang tot beheersystemen, opslagmogelijkheden voor reserveonderdelen en verbruiksartikelen, en faciliteiten voor het ontvangen, tijdelijk opslaan en verzenden van apparatuur. Zeker in situaties waarin medewerkers regelmatig ter plaatse zijn of bezoekers zoals technici of leveranciers ontvangen worden, is een dergelijke werkomgeving onmisbaar voor een efficiënte en veilige exploitatie.

Aan deze facilitaire randvoorwaarden wordt overigens op dit moment al grotendeels voldaan binnen de bestaande datacenterfaciliteit op Bonaire. Deze praktijkervaring vormt een goed uitgangspunt voor toekomstige locaties op bijvoorbeeld Sint Eustatius of Saba, waar vergelijkbare voorzieningen voorzien moeten worden.

Daarnaast is het sterk aan te bevelen om gebruik te maken van zowel digitale dashboards (op afstand benaderbaar) als fysiek zichtbare schermen op locatie, bijvoorbeeld in de vorm van televisieschermen in de werkruimte. Deze dashboards maken het mogelijk om continu de status van essentiële systemen, zoals stroomvoorziening, koeling, netwerkactiviteit en fysieke beveiliging, te monitoren. Dit draagt bij aan operationeel inzicht, snelle respons bij afwijkingen en een professionele beheersomgeving.

Door zowel digitale als fysieke faciliteiten op deze wijze te integreren, wordt de betrouwbaarheid, veiligheid en werkbaarheid van het datacenter als geheel versterkt.

SCHAALBAARHEID

Het datacenter dient voor lange termijn gebouwd te worden, dus te bouwen op een plek waar uitbreiden mogelijk is. Als over 10 jaar de belasting verdubbelt, of juist de hoeveelheid apparatuur in formaat en hoeveelheid inkrimpt, moet die flexibiliteit in schaalbaarheid gerealiseerd kunnen worden zonder een compleet (nieuw) pand te moeten (ver)bouwen. Wellicht is modulair bouwen een optie of anders ruimte reserveren voor groei.

TIER-NIVEAU DATACENTERS

Formeel is een Tier-IV datacenter niet vereist (dat is het allerhoogste met volledig dubbel uitgevoerde infra, geen enkele single point of failure en het meest onderscheidende; twee verschillende elektriciteitsnetten voor toelevering). Tier-III, wat tolerant is voor 1 component-failure, is een realistisch streven. Tier-III betekent 99.982% beschikbaarheid (max ~1,6 uur downtime per jaar). Tier-III wordt ook in Europees Nederland gezien als het minimum waaraan een overheidsdatacenter dient te voldoen, het advies is dan ook Tier-III als uitgangspunt te hanteren voor eventueel nieuw te bouwen datacenters.

6.3 Voor- en nadelen van lokale huisvesting

VOORDELEN

Een eigen datacenter op de eilanden geeft controle, performance en minder afhankelijkheid van van derde partijen zoals zeekabelaanbieders en transitproviders. De data is "dichtbij" onder eigen beheer, wat goed scoort op soevereiniteit en performance voor lokale gebruikers. Het laat ook zien dat de overheid investeert in de eilanden, wat politiek-bestuurlijk een voordeel kan zijn. Tevens kan het dan exact op maat ontworpen worden voor de behoeften, zonder afhankelijkheid van externe commerciële datacenters die wellicht features hebben die niet nodig zijn of andersom. In geval van isolatie (kabelbreuk) kunnen de eilanden lokaal blijven draaien op de kritieke systemen, dat is de grootste winst t.o.v. volledige cloud in Europa. Bovendien kan de faciliteit gedeeld worden. In principe zou bijvoorbeeld het lokale ziekenhuis of andere instellingen ook racks kunnen plaatsen als dat gewenst is (Multi-tenancy is een eis). Lokale bouw en onderhoud creëren werkgelegenheid en kennisontwikkeling, het is een impuls aan de digitalisering en de social return is hierbij hoog. Het biedt ook de mogelijkheid om vanuit Europees Nederland deze datacenters te gebruiken als uitwijk, back-up of archief locatie. (Geografische spreiding, veiligstelling en bescherming in tijden van oorlog of cyberaanvallen in Europa)

NADELEN

Tegenover deze voordelen staan ook nadelen: ten eerste de kosten. Het bouwen en exploiteren van een Tier-III datacenter op Bonaire is kostbaar door import van materiaal, schaalnadeel en de behoefte aan redundante systemen. De initiële investeringen (gebouw, generator, koeling, etc.) zijn aanzienlijk, en door het relatief kleine schaalvoordeel zijn de jaarlijkse operationele kosten per rackunit veel hoger dan in een groot datacenter in Europees Nederland. Daarnaast vergt lokaal beheer specialistische technische kennis die nu beperkt voorhanden is op de eilanden. Personeel moet worden opgeleid of ingehuurd, wat weer de afhankelijkheid van externe partijen vergroot als daar lokaal geen continuïteit in zit. Een aandachtspunt bij een puur lokale opzet is dat de BES-eilanden buiten de Europese Economische Ruimte (EER) vallen. Dat maakt dat data-opslag daar juridisch en compliance-technisch aanvullende waarborgen vereist onder de AVG, zoals een afsprakenstelsel, een DPIA en passende contractuele afspraken. Zonder deze borging voldoet opslag op de BES mogelijk niet aan Europese privacywetgeving. Om aan dat uitgangspunt te voldoen, dit voert de complexiteit en kosten verder op. Ook op duurzaamheid scoort een eigen datacenter potentieel minder goed vergeleken met gebruik van grote cloudproviders die zeer efficiënt met energie omgaan, tenzij er fors geïnvesteerd wordt in lokale groene energie kan de PUE (Power Usage Effectiveness) ongunstiger uitvallen. Ten slotte is er het risico van overcapaciteit of onderbenutting, als de vraag minder hard groeit dan verwacht, dan zit CN met een relatief duur eigen datacenter dat niet volledig wordt benut (geld dat ook anders ingezet had kunnen worden).

CONCLUSIE LOKAAL HUISVESTEN

Het huidige datacentrum kent beperkingen voor groei. Nieuwe datacenter(s) op de BES- bied(t)(en) voordelen in de onafhankelijkheid van centrale besluitvorming en continuïteit ter plekke, maar daar staan kosten tegenover en organisatorische uitdagingen. Hoofdstuk 8 en 9 laten zien hoe de varianten met lokale huisvesting scoren.

7 RANDVOORWAARDEN VOOR NETWERKINFRASTRUCTUUR

Datacenters zijn sterk afhankelijk van de netwerken die het verbinden met de gebruikers en met elkaar. Ten aanzien van Caribisch Nederland is de netwerkinfrastructuur een cruciale factor vanwege de geografische afstanden en huidige beperkingen (zoals eerder beschreven in hoofdstuk 2 en 3). Dit hoofdstuk beschrijft de randvoorwaarden en aandachtspunten voor het netwerk ten behoeve van de datacenterstrategie. We behandelen uitdagingen rond latency en bandbreedte (7.1) en continuïteit en redundantie van verbindingen (7.2), plus mogelijke optimalisaties om de prestaties te verbeteren (7.3).

7.1 Latency-uitdagingen en optimalisatie

De grote geografische afstand tot Europa vormt de grootste uitdaging voor latency vanwege de duizenden kilometers en schakels via verschillende netwerken en landen (hops). Voor real-time toepassingen als cloud-desktops, transacties in applicaties of beveiligingstoepassingen (met time-outs) is dit merkbaar en vaak hinderlijk. Een randvoorwaarde voor gebruiksvriendelijke en betrouwbare dienstverlening is dat latency zoveel mogelijk wordt beperkt. Dit betekent concreet dat gekozen moet worden voor kortere of rechtstreekse verbindingen, bijvoorbeeld via eigen onderzeese glasvezel, en omleidingen via derde landen te vermijden.

LOKALE VERWERKING EN CACHING

Lokale caching wordt gezien als noodzakelijke maatregel om latency en IP-transitkosten te beperken. Door content zoals software-updates, video's, cloudbestanden en andere veelgevraagde data lokaal op de BES-eilanden op te slaan, hoeven deze niet telkens via internationale verbindingen te worden opgehaald. Het huidige gebrek aan caching (met name op Saba en Sint Eustatius) veroorzaakt meetbare vertraging en vormt een structureel knelpunt. Tegelijkertijd is op Sint Eustatius een lokale caching-/charging-voorziening in ontwikkeling; totdat deze operationeel is, blijft het knelpunt bestaan. Daarom wordt geadviseerd om cachingcapaciteit standaard op te nemen binnen de datacenterfaciliteiten op de eilanden. Deze kunnen fungeren als regionale cache voor alle publieke en semipublieke stakeholders. Dit is niet alleen gunstig voor latency, maar ook voor het verlagen van datatransportkosten, een relevante overweging gezien de hoge IP-transittarieven in het gebied.

Ook overheidsspecifieke distributie, (zoals updates en standaardsoftware) kan hierdoor efficiënter verlopen. Hoewel caching functioneel meer richting netwerk- en dienstenlaag valt dan de core datacenterinfrastructuur, is het een direct verbonden voorziening die de gebruikservaring sterk kan verbeteren en kosten helpt reduceren.

OPTIMALE ROUTING EN PEERING

Voor een betrouwbare en toekomstbestendige digitale infrastructuur in Caribisch Nederland is het essentieel dat netwerkverkeer zoveel mogelijk via directe, korte en voorspelbare routes verloopt. Dit geldt zowel voor verkeer tussen de BES-eilanden onderling als voor verbindingen met Europees Nederland. Tot voor kort verliep het merendeel van het verkeer van Saba en Sint Eustatius naar Bonaire via St. Maarten, St. Barths of St. Kitts en vervolgens, eventueel via de Britse Maagdeneilanden, naar Puerto Rico (VS) en Curaçao. Met de komst van het CELIA-kabelsysteem, dat via St. Barths een alternatieve route naar Bonaire mogelijk maakt, verbetert de connectiviteit en neemt de afhankelijkheid van de bestaande keten gedeeltelijk af. Omdat CELIA een route via derde landen is en geen directe interinsulaire verbinding onder Nederlands beheer biedt, blijft de noodzaak voor een eigen, redundante en soevereine netwerkstructuur onverminderd van strategisch belang.

Het internetverkeer op Bonaire verloopt momenteel grotendeels via één transitprovider, wat leidt tot kwetsbaarheid bij storingen of uitval. De aansluiting op de nieuwe CELIA-zeekabel, gepland voor 2027, moet deze afhankelijkheid verminderen en extra redundantie bieden. Daarnaast wordt gewerkt aan voorzieningen voor lokale traffic-uitwisseling tussen providers om de digitale veerkracht verder te versterken.

Om route-efficiëntie en netwerkbetrouwbaarheid te waarborgen, is het advies dat het netwerkontwerp voldoende ondersteuning biedt voor route-optimalisatie en peeringmogelijkheden. Dat houdt in dat verkeer tussen de BES-eilanden onderling, maar ook met Europees Nederland, zoveel mogelijk via directe en korte routes verloopt, zonder onnodige tussenstappen via derde landen. Daarbij is het wenselijk dat infrastructuurkeuzes ondersteuning bieden voor onderlinge uitwisseling van verkeer tussen lokale providers, en

dat er mechanismen aanwezig zijn om afhankelijkheden van enkele transitproviders te beperken waar mogelijk. Netwerkvoorzieningen zoals internetexchanges, peeringfaciliteiten of lokale traffic-uitwisseling dragen bij aan een toekomstvaste infrastructuur die schaalbaar, veerkrachtig en minder storingsgevoelig is.

De strategie stelt als randvoorwaarde dat verkeer van en naar Caribisch Nederland via een betrouwbare, snelle en schaalbare verbinding met het Rijksnet verloopt. Op termijn betekent dit de aanleg van een nieuwe, directe primaire dataverbinding tussen Bonaire (via Saba of Sint Eustatius) en Europees Nederland. Tot die tijd zal van bestaande internationale netwerkroutes/hubs gebruikt gemaakt moeten worden die later wellicht als secundaire routes kunnen fungeren (Curaçao, St. Kitts, St. Barths, Puerto Rico/Britse Maagdeneilanden, Miami, New York, (evt. via VK) naar Europees Nederland). Het netwerkontwerp dient te voorzien in een optimale gateway naar het Rijksnet, bijvoorbeeld via een node nabij waar de zeekabel aan land komt en/of via een VPN over meerdere paden. Om latencygevoelige diensten zoals spraakverkeer, videoconferencing en telemedicine te waarborgen, zijn aanvullende netwerkvoorzieningen vereist. Denk aan Quality of Service (QoS), gescheiden datastromen via DWDM of gereserveerde bandbreedtekanalen voor vitale toepassingen.

DNS EN NAAMRESOLUTIE

Een toekomstbestendige infrastructuur vereist dat domeinnaamoplossingen (DNS-resolutie) snel, betrouwbaar en onafhankelijk worden afgehandeld. Omdat DNS-resolve tijden direct invloed hebben op de internetervaring van eindgebruikers, geldt als randvoorwaarde dat deze resolutie lokaal of regionaal op de BES-eilanden moet kunnen plaatsvinden.

Hiervoor moeten voorzieningen worden getroffen, zoals het inrichten van lokale DNS-resolvers of het toepassen van anycast-technologie. Deze maatregelen verkorten de reactietijd tussen overheidsdiensten en gebruikers op de eilanden, en vergroten de operationele veerkracht wanneer verbindingen met externe netwerken instabiel zijn of tijdelijk uitvallen.

Lokale DNS-afhandeling draagt dus bij aan zowel performance als digitale autonomie, en moet als standaard worden meegenomen in de netwerkinrichting.

7.2 Redundantie, continuïteit van verbindingen en security

Vanwege de geografische ligging en het beperkte aantal verbindingstrajecten geldt als randvoorwaarde dat de netwerkarchitectuur van Caribisch Nederland volledig redundant is ingericht. Er mag nergens sprake zijn van een single point of failure – niet in de verbindingen tussen de eilanden, noch in de koppeling met Europees Nederland. Redundantie moet daarom zowel fysiek als logisch worden gerealiseerd, bijvoorbeeld door gebruik van meerdere zeekabelaanbieders, gescheiden IP-transitproviders, en routing via geografisch gespreide netwerken.

Daarnaast moet de infrastructuur voorzien in automatische failovermechanismen of dynamische routeomschakeling bij verstoringen, zodat bij uitval van de primaire route altijd een alternatieve, zij het mogelijk beperktere, route beschikbaar is. Dergelijke fallback-opties kunnen via bestaande hubs (zoals Curaçao, Puerto Rico of Miami) verlopen en moeten ten minste de continuïteit van vitale diensten zoals authenticatie, spraak en datareplicatie waarborgen.

De keuzes over welke datastromen bij verstoring worden omgeleid, en hoe snel en automatisch dit gebeurt (bijvoorbeeld via BGP failover, SD-WAN of routing policies), en welke veiligheidsvoorzieningen (zoals encryptie) getroffen dienen te worden. Dienen expliciet te worden vastgelegd in het netwerkontwerp en het bijbehorende crisis- en herstelprotocol.

INTERINSULAIR (TUSSEN DE EILANDEN)

Er moet ten minste één stabiele netwerkroute zijn die Bonaire, Saba en Sint Eustatius onderling verbindt. Om uitval op te vangen en continue replicatie mogelijk te maken, geldt als randvoorwaarde dat er bij voorkeur een redundante ringstructuur wordt ingericht, bijvoorbeeld in de vorm van een lus Bonaire – Sint Eustatius – Saba – terug naar Bonaire via een alternatieve route. De bestaande route via St. Kitts, Sint-Maarten, Puerto Rico en Curaçao dient in stand te blijven gezien deze voorziet in internetconnectiviteit, maar moet worden aangevuld met een nieuwe primaire directe route Sint Eustatius–Bonaire. Een situatie waarin Bonaire bij uitval van een

route volledig wordt afgesneden van de bovenwindse eilanden is alleen acceptabel als er sprake is van autonome voorzieningen op Saba en Sint Eustatius. Als er geen directe interinsulaire verbinding tussen Bonaire en Saba of Sint Eustatius tot stand komt, blijven de bovenwindse eilanden afhankelijk van omwegen via derde landen. Deze routes leiden tot hogere latency, verminderde voorspelbaarheid en bandbreedte en verhoogde risico's op verstoringen. Dit vormt een serieuze belemmering voor een robuuste en betrouwbare communicatie tussen datacenters op de eilanden onderling. Denk hierbij aan replicatieverkeer, synchronisatie van gegevens, back-upfaciliteiten of failovermechanismen die essentieel zijn voor continuïteit en veerkracht.

Het ontbreken van een directe route beperkt daarmee de mogelijkheid om bovenwindse datacenterlocaties volwaardig in te zetten als redundante of actieve componenten binnen een bredere hybride infrastructuur in Caribisch Nederland. In de praktijk vergroot dit de kwetsbaarheid van het geheel en vergroot het risico dat de bovenwindse eilanden niet mee kunnen ontwikkelen met benedenwindse locaties. Vanuit strategisch oogpunt is het daarom noodzakelijk om een directe interinsulaire verbinding als harde randvoorwaarde mee te nemen in alle toekomstige investeringen in digitale infrastructuur.

Voor het geval de primaire verbinding tussen de eilanden tijdelijk niet beschikbaar is, moet het netwerkontwerp voorzien in de mogelijkheid om dataverkeer voor bepaalde replicatieprocessen via alternatieve routes te laten verlopen. Dit is van belang om ook bij storingen of calamiteiten een minimale vorm van synchronisatie tussen datacenters in stand te houden. Tegelijkertijd moet in het ontwerp expliciet worden vastgelegd welke datastromen eventueel níet via deze alternatieve paden mogen of hoeven te verlopen, bijvoorbeeld vanwege informatiebeveiligingsrichtlijnen of de betrokkenheid van derde landen in de route. Dergelijke keuzes dienen vooraf beleidsmatig te worden afgewogen en vastgelegd in de netwerk- en beveiligingsarchitectuur.

Om de netwerkrobuustheid interinsulair verder te vergroten, verdient het aanbeveling een redundante verbinding te realiseren tussen Saba en Sint Eustatius, zoals ook weergegeven in de doelarchitectuur (bijlage A). Deze verbinding dient als alternatieve route naast de bestaande SSCS-koppeling en kan worden gerealiseerd via een tweede glasvezelkabel met een andere landingsplaats op beide eilanden, of – indien fysiek of financieel realistischer – via een microwave link. Een dergelijke redundantielaag draagt bij aan de veerkracht van het interinsulaire verkeer tussen Saba en Sint Eustatius, biedt extra zekerheid bij onderhoud of verstoringen op de SSCS hoofdroute tussen beide eilanden, en maakt het netwerk beter bestand tegen calamiteiten of tijdelijke uitval van verbindingen. Deze verbinding is van strategisch belang, aangezien in dit rapport wordt geadviseerd om op een van beide eilanden een primaire datacenterfunctie te positioneren. Voor de digitale continuïteit van de Bovenwindse eilanden is een betrouwbare en redundante verbinding tussen Saba en Sint Eustatius daarom essentieel.

TRANS-ATLANTISCH (NAAR EUROPEES NEDERLAND)

Voor een toekomstvaste infrastructuur is het een randvoorwaarde dat er minimaal twee routes tussen Caribisch Nederland en Europa operationeel zijn. Hoewel er momenteel een werkbare route via de Verenigde Staten bestaat, brengt deze route hogere latency en afhankelijkheid van niet-Europese partijen met zich mee. Alternatieve paden via bijvoorbeeld Zuid-Amerika zijn mogelijk, maar minder stabiel en minder voorspelbaar in performance (bandbreedte en latency.

Het netwerkontwerp dient redundantie en automatische routering bij uitval te ondersteunen, bijvoorbeeld via BGP-failover, en moet voorkomen dat beide verbindingen via hetzelfde landing station op Bonaire of andere gemeenschappelijke knelpunten verlopen. Daarnaast is het wenselijk dat internationaal verkeer zoveel mogelijk binnen de Europese Economische Ruimte (EER) blijft, en niet via derde landen verloopt vanwege implicaties voor gegevensbescherming en toezicht op datastromen.

Om deze randvoorwaarden structureel te kunnen borgen, wordt geadviseerd om een rechtstreekse verbinding met Europees Nederland te realiseren. Dit garandeert publieke regie, transparantie in eigendom en beheer, en waarborgt de beschikbaarheid en betrouwbaarheid van digitale diensten op de lange termijn.

De aanleg van een rechtstreekse onderzeese verbinding tussen Bonaire, Sint Eustatius of Saba en Europees Nederland biedt de grootste zekerheid voor continuïteit, digitale autonomie en beheer onder Nederlands recht. Daarmee blijft volledige controle behouden over beveiliging, onderhoud en prioriteitstelling. Deze optie vraagt echter aanzienlijke investeringen en kent een langere realisatietijd. Een alternatief is het benutten van

bestaande kabelsystemen, waarbij binnen meerdere routes dedicated capaciteit wordt vastgelegd en contractueel geborgd in meerjarige SLA's. Dit is sneller uitvoerbaar en financieel haalbaarder, maar blijft afhankelijk van commerciële partijen en buitenlandse jurisdictie, wat risico's met zich meebrengt bij storingen, politieke spanningen of wijzigingen in eigendomsstructuren. De voorkeur ligt daarom bij een hybride benadering: bestaande infrastructuur optimaal benutten met harde contractuele garanties op korte termijn, terwijl parallel wordt toegewerkt naar een structurele, rechtstreekse verbinding onder Nederlands beheer op middellange termijn. Zo worden zowel de betrouwbaarheid als de strategische autonomie van de digitale infrastructuur voor Caribisch Nederland versterkt.

Een directe trans-Atlantische verbinding met Caribisch Nederland biedt ook voordelen voor Europees Nederland. Caribisch Nederland biedt een unieke positie als veilige digitale uitwijklocatie buiten het Europese continent. Door directe, vertrouwde verbindingen te realiseren, wordt het mogelijk om vanuit Europees Nederland gevoelige data, digitale back-ups en strategische informatie te verplaatsen naar een locatie onder volledig Nederlands staatsgezag. In tijden van geopolitieke instabiliteit of (cyber)aanvallen/dreigingen op het Europese vasteland, vergroot dit de digitale weerbaarheid van het Rijk. Afhankelijk van de inrichting kan deze capaciteit in de toekomst mogelijk ook beschikbaar worden gesteld aan andere Europese landen (bijvoorbeeld Frankrijk) die behoefte hebben aan geografisch gespreide, betrouwbare datavoorzieningen binnen het Koninkrijk of de Europese rechtsorde.

LOKALE NETWERKEN EN UITVALSCENARIO'S

Het netwerkontwerp moet op basis van de strategische uitgangspunten zodanig worden ingericht dat de boven- en benedenwindse eilanden tijdelijk zoveel mogelijk zelfvoorzienend van elkaar kunnen functioneren, ook als externe verbindingen uitvallen. Een essentieel ontwerpprincipe voor het waarborgen van minimale beschikbaarheid en continuïteit bij netwerkstoringen.

SECURITY EN VERSLEUTELING

Onder de randvoorwaarden voor de netwerkinfrastructuur in Caribisch Nederland is beveiliging van gegevensverkeer een essentiële pijler. De netwerkverbindingen tussen de BES-eilanden onderling, én met Europees Nederland, vormen de ruggengraat van digitale dienstverlening. Een bijzonder aandachtspunt daarbij is de fysieke routing van internationale datastromen: veel van de huidige zeekabelverbindingen lopen via derde landen, zoals de Verenigde Staten of Zuid-Amerikaanse staten. Dit brengt inherente risico's met zich mee op het gebied van vertrouwelijkheid, beschikbaarheid en integriteit van overheidsdata.

Om hieraan tegemoet te komen, is versleuteling van dataverkeer, zowel in transit als bij verbindingsovergangen, een randvoorwaarde. Encryptie op netwerklaag (zoals IPsec, MACsec) of applicatielaag (zoals TLS) moet standaard worden toegepast om afluisteren, manipulatie of onbedoelde toegang te voorkomen. Zeker wanneer verbindingen buiten de Europese Economische Ruimte (EER) lopen, is dit niet alleen een technische noodzaak, maar ook een juridische. Alleen versleuteling toepassen op bestaande routes die via derde landen verlopen is echter geen garantie: ontwikkelingen in quantumtechnologie en decryptietechnieken maken bestaande versleutelingsstandaarden mogelijk nu al, maar zeker op termijn ontoereikend. De beveiligingsrisico's zijn daarmee niet alleen theoretisch, maar toekomstgericht reëel en materieel, wat de noodzaak voor directe verbindingen op langere termijn benadrukt.

Naast eisen aan redundantie, failover en betrouwbare latency- en bandbreedtegaranties geldt als randvoorwaarde dat netwerkbeveiliging expliciet wordt meegenomen in het ontwerp. Zonder veilige, versleutelde verbindingen blijven andere voorzieningen kwetsbaar. Encryptie en integriteit van dataverkeer vormen daarmee een onmisbare bouwsteen voor een toekomstbestendige digitale infrastructuur in Caribisch Nederland.

CLOUDCONNECTIVITEIT

Wanneer gebruik wordt gemaakt van public cloudservices zoals Azure of AWS, bijvoorbeeld voor specifieke toepassingen of dataopslag, geldt als randvoorwaarde dat de netwerkconnectiviteit redundant en voorspelbaar is ingericht. Vanwege mondiale spanningen en afhankelijkheden moet worden vermeden dat cloudverkeer over onbetrouwbare of ongecontroleerde routes loopt. Het netwerkontwerp moet in dat geval voorzien in minimaal twee onafhankelijke routes richting cloudinfrastructuur, bij voorkeur via redundante internetontsluitingen of private connecties zoals Azure ExpressRoute of AWS DirectConnect. Dergelijke hubs zijn op dit moment niet

fysiek beschikbaar op Bonaire, maar zouden via een Point of Presence op Curaçao of Puerto Rico kunnen worden ontsloten – mits daar een geschikte cloud exchange of peeringlocatie beschikbaar is. Verkeer naar cloudomgevingen moet via gescheiden paden kunnen worden gerouteerd, eventueel via zowel Europa als de Verenigde Staten. Private routing of versleutelde tunnels zijn aanbevolen om beschikbaarheid, performance en datasoevereiniteit te waarborgen.

7.3 Capaciteit, prestaties en kwaliteitsafspraken

Naast latency en redundantie is voldoende ruwe netwerkcapaciteit, oftewel beschikbare bandbreedte, cruciaal voor een toekomstbestendige digitale infrastructuur. Het netwerk moet niet alleen stabiel en snel functioneren, maar ook schaalbaar zijn in termen van datavolume en piekbelasting.

De verwachte groei in dataverkeer wordt mede veroorzaakt door videocommunicatie, centralisatie van IT-processen en opkomst van data-intensieve toepassingen zoals AI, IoT, real-time monitoring en externe back-up of disaster recovery richting of vanuit Europees Nederland. Een tekort aan bandbreedte leidt niet alleen tot tragere overdracht, maar beïnvloedt direct de latency en dus de performance van kritieke diensten.

De datacenterstrategie dient daarom expliciet te anticiperen op capaciteitsgroei en de inzet van schaalbare netwerkarchitecturen. Dit vereist investeringen in hoogwaardige verbindingen, slimme verkeersverdeling en, waar technisch haalbaar, directe verbindingen met minimale hops of buitenlandse omwegen.

HUIDIGE VS TOEKOMSTIGE CAPACITEIT

Toenemende digitalisering binnen de overheid en het gebruik van datagedreven toepassingen, zoals videoconferencing en e-learning, kunnen leiden tot een sterke stijging in de vraag naar bandbreedte. Om aan toekomstige capaciteitsbehoeften te voldoen, is het noodzakelijk dat de hoofdverbindingen met internet en Europees Nederland ontworpen worden op een schaal van ten minste >10 Gbit/s, met ruimte voor opschaling.

Bij het ontwerp van nieuwe zeekabels wordt reeds uitgegaan van terabit-schaal capaciteit. Dit biedt voldoende bandbreedtemarge over de levensduur van de infrastructuur. Binnen het datacenter, en tussen meerdere datacenterlocaties, is eveneens ruime netwerkcapaciteit noodzakelijk vanwege datastromen zoals replicatie, back-ups en failovermechanismen. Deze stromen komen bovenop het reguliere gebruikers- en productiegerichte verkeer. Technisch kan schaalbaarheid worden bereikt via het inzetten van meerdere (dedicated) glasvezelpaden, of via wavelength-multiplexing waarbij afzonderlijke lichtgolflengten op een gedeelde glasvezel worden gebruikt om parallelle datastromen te scheiden en te routeren.

QUALITY OF SERVICE EN SLA'S

Voor een betrouwbare en vitale netwerkinfrastructuur in Caribisch Nederland is het essentieel dat afspraken over kwaliteit van dienstverlening (Quality of Service) formeel worden vastgelegd. Randvoorwaarden zijn onder meer: lage packet loss (<0,1%), stabiele latency (met jitter onder een vastgestelde grens), en korte hersteltijden bij verstoringen (bijvoorbeeld binnen 48 uur een werkende bypass bij kabelbreuk). Omdat dergelijke SLA's momenteel beperkt zijn of ontbreken op de eilanden, is het advies hier in toekomstige netwerkcontracten rekening te worden gehouden.

INTEGRATIE MET DIGINETWERK

Binnen de Nederlandse overheid vormt Diginetwerk de verbindende infrastructuur tussen verschillende overheidsnetwerken. Organisaties die gebruikmaken van generieke voorzieningen zoals DigiD, Digipoort of de BRP, hebben hiervoor doorgaans een aansluiting op Diginetwerk nodig. Voor Caribisch Nederland geldt dat instellingen met een publieke taak in toenemende mate afhankelijk zijn van dergelijke voorzieningen, waardoor aansluiting op Diginetwerk noodzakelijk is om digitale overheidsdiensten correct en veilig te ontsluiten.

Technisch betekent dit dat verkeer tussen Caribisch Nederland en Europees Nederland via besloten, hoogwaardige netwerkpaden moet verlopen, in plaats van over het publieke internet. Voor deze koppeling zijn verschillende opties beschikbaar, waaronder een IPsec-tunnel of een dedicated lijn richting een Rijksknooppunt, bijvoorbeeld via een bestaande verbinding van Justitie of Defensie.

Door het verkeer via gecontroleerde paden te laten verlopen, wordt de voorspelbaarheid van latency verhoogd en kunnen beveiligingsrisico's worden beperkt. Daarnaast biedt dit voordelen voor de performance van toepassingen die afhankelijk zijn van verbindingen met overheidsdatacenters in Europees Nederland.

UITBREIDING VAN MONITORING EN BEHEER OP NETWERKGEBIED

Om te zorgen dat de netwerkkwaliteit voldoet, is intensieve monitoring op het gehele netwerk essentieel. Er dient een NMS (Network Monitoring System) te zijn dat latency, throughput en uitval op alle trajecten (inclusief zeekabels) meet. Idealiter wordt monitoring gedistribueerd uitgevoerd vanaf meerdere locaties om een volledig beeld te krijgen van eventuele degradaties of verstoringen. Zo kunnen trends gezien worden en kan men proactief handelen als de kwaliteit zakt. Dit draagt bij aan operationele stabiliteit. In het kader van incidentvoorbereiding is het daarnaast relevant dat procedures beschikbaar zijn voor het reserveren of prioriteren van bandbreedte, bijvoorbeeld voor essentiële toepassingen zoals crisiscommunicatie, tijdens extreme weersomstandigheden of dreigende verstoringen.

RESUMER

De in dit hoofdstuk beschreven netwerkrandvoorwaarden dragen bij aan het realiseren van robuuste, snelle en flexibele connectiviteit. Deze aspecten vormen belangrijke technische en operationele kaders voor het beoordelen van mogelijke scenario's in de datacenterstrategie voor Caribisch Nederland. Varianten waarbij netwerkverbeteringen beperkt blijven, bieden minder zekerheid ten aanzien van prestatie, continuïteit en schaalbaarheid.

In het onderzoek "Research into Data Subsea Cables: Enabling Caribbean Netherlands digitally" wordt onderstreept dat investeringen in fysieke kabelinfrastructuur aanzienlijke impact kunnen hebben op de digitale ontwikkelmogelijkheden van de regio.

8 STRATEGISCHE VARIANTEN

Met de context, uitgangspunten en randvoorwaarden in beeld, kunnen we de concrete strategische varianten uitwerken. In dit hoofdstuk presenteren we de mogelijke varianten voor de datacenterstrategie van Caribisch Nederland. Onder een variant verstaan we een samenhangend scenario van waar de datacenters staan (lokaal of extern), hoe de diensten worden afgenomen (eigen beheer vs. cloud), en eventuele bijzondere keuzes (zoals edge opzet of mix per workload).

8.1 Distinctie tussen housing en hosting

Voordat we de scenario's beschrijven, is het van belang om duidelijk te definiëren wat wordt verstaan onder housing en hosting. Tijdens gesprekken en een workshop met stakeholders kwam nadrukkelijk naar voren dat er een helder onderscheid nodig is tussen enerzijds de fysieke datacenterhuisvesting (housing) en anderzijds de IT-diensten (hosting) die binnen deze infrastructuur worden geleverd en beheerd.

HOUSING

Dit onderdeel gaat over alle fysieke en technische faciliteiten van een datacenter. Denk aan het datacenter als een veilig en goed ingericht 'huis' voor de apparatuur. Het gaat hierbij onder andere om de stroomvoorziening, koeling, noodstroom, racks, bekabeling buiten de racks, fysieke beveiliging, branddetectie en -blussing. In dit verband hoort daar ook de mogelijkheid bij om gebruik te maken van netwerkverbindingen naar buiten (externe connectiviteit).

Dit alles vormt de gedeelde infrastructuur van het datacenter, die beschikbaar is voor alle partijen die er gebruik van maken. Het datacenter levert in de meeste gevallen een leeg rack, inclusief alle benodigde faciliteiten, waarin de klant zelf zijn apparatuur kan plaatsen en aansluiten op stroom. De externe netwerkverbindingen (zoals koppelingen met het internet of andere netwerken) worden via patchkabels door het datacenter tot in het rack gebracht. (patches op zaal, patches naar 'meetmerooms')

HOSTING

Veel datacenters bieden naast huisvesting ook hostingdiensten aan. Een voorbeeld van een housingprovider is Flamingo TV op Bonaire, terwijl ODC-Noord in Groningen zowel datacenterfaciliteiten als hosting levert. SSO-CN beheert op Bonaire een eigen datacenter, maar stelt dit niet beschikbaar aan derden. Zij leveren uitsluitend (managed) hostingdiensten, waarbij het datacenter enkel de fysieke basis vormt om de eigen diensten te kunnen aanbieden.

Hosting betreft wat er daadwerkelijk in het datacenter wordt geplaatst: apparatuur en – bij virtualisatie of containerisatie – soms ook systeemsoftware die de dienstverlening mogelijk maakt. Dit zijn doorgaans servers en ondersteunende systemen van dienstverleners, die daar hun IT-diensten op laten draaien. Organisaties kunnen dit ook zelf beheren, zonder tussenkomst van externe partijen.

Voorbeelden zijn ODC-Noord, dat Infrastructure as a Service (IaaS) aanbiedt, en Logius, dat via het Standaard Platform Platform as a Service (PaaS) levert. Hosting omvat dus alles bovenop de basisinfrastructuur van het datacenter, zoals servers, opslag, netwerken en beheer. Bij Logius wordt het platform tot en met het containerplatform beheerd; de verantwoordelijkheid voor de containers zelf ligt bij de afnemer.

MANAGED HOSTING

Een stap verder is managed hosting. Hierbij wordt het volledige beheer uit handen genomen, bijvoorbeeld van besturingssystemen (zoals installatie en updates), middleware, databases, applicaties en ook gebruikersgerichte diensten zoals werkplekbeheer, servicedesk, beveiligingsmonitoring (SOC/SIEM) en periodieke controles of audits. Zulke diensten kun je afnemen bij commerciële partijen, cloudproviders of overheidsdienstverleners zoals Logius, SSO-CN, SBIR of SSC-ICT. Hierdoor hoef je je als klant niet meer bezig te houden met het dagelijkse beheer van je IT-infrastructuur – tot aan het technisch applicatiebeheer toe. Een klant kan zich dan richten op functioneel beheer.

Daarnaast zijn er hybride varianten van hosting mogelijk en denkbaar, waarbij een dienstverlener bijvoorbeeld tot op Operating System niveau beheert, of een hypervisor (virtueel) of container platform beheert, waar de klant het beheer van de virtuele machines, de containers en applicatie op zich neemt. (zie voorbeeld Logius onder 'hosting'.)

Het is belangrijk om dit onderscheid te maken, omdat sommige varianten meer decentralisatie of uitbesteding in housing betekenen, terwijl andere dat juist in (managed) hosting doen (of beide). Sommige stakeholders gaven aan het niet uit te maken waar de grens ligt, zolang zij maar volledig worden ontzorgd. Anderen willen juist zelf controle houden over bepaalde lagen, of per onderdeel kunnen kiezen van wie ze diensten afnemen. Daarom is het van belang om per variant duidelijk te hebben: wie doet de housing en wie de hosting? Bijvoorbeeld variant 8 (lokale outsourcing) betekent housing én hosting door een lokale partij. Variant 2 (twin DC in CN) betekent housing door de overheid zelf op beide locaties, maar hosting zou door verschillende partijen kunnen gebeuren, dat is nog in te vullen.
Bij de variantenbeschrijvingen hieronder benoemen we expliciet of de housing lokaal, nationaal of bij een derde ligt. Dit helpt om een goed vergelijk te maken. In de praktijk kan natuurlijk een mix: men kan housing in eigen hand houden maar hosting (beheer) grotendeels uitbesteden. Dat nuanceverschil komt tot uiting in de score op bijvoorbeeld het criterium "Ontzorging" en "Governance" in hoofdstuk 9.

8.2 De strategische varianten

In de werkgroep, kerngroep, documentanalyse en de workshop van 26 maart 2025 zijn tien hoofdvarianten voor de datacenterstrategie ontwikkeld. Deze zijn systematisch bepaald langs drie inhoudelijke denklijnen: locatie van de infrastructuur, type beheermodel en architectuuropzet. Onhaalbare of tegenstrijdige combinaties zijn vooraf uitgesloten. Tabel 2 geeft een overzicht van de overgebleven varianten, die vervolgens kort worden toegelicht op kenmerken, voordelen en nadelen.

Tabel 2 - Overzicht van de 10 varianten – zie bijgevoegd schema varianten uit fase 1 concept

Variant	Korte omschrijving
1	Lokale datacenters per eiland (decentralisatie) Ieder BES-eiland beschikt over een eigen fysiek datacenter met lokale housing. De infrastructuur en dienstverlening zijn volledig gescheiden per eiland.
2	Twin-datacenter in Caribisch Nederland (Benedenwinds & Bovenwinds) Er is een datacenter gevestigd op Bonaire en een datacenter op Saba of Sint Eustatius. De datacenters zijn elkaars backup en uitwijk.
3	Lokaal datacenter met edge computing en uitwijk in Europa (hybride DR) Het datacenter op Bonaire fungeert als primaire housinglocatie, edge computing-voorziening op Saba en/of Sint Eustatius, met een actieve back-up of uitwijkvoorziening in Europees Nederland. Data wordt gesynchroniseerd tussen de locaties.
4	Primair Europees datacenter, lokaal noodplatform De primaire housing van diensten vindt plaats in een datacenter in Nederland of elders binnen de EER. Op Bonaire of een ander BES-eiland is een lokaal platform aanwezig voor noodgebruik bij verbindingsuitval.
5	Volledig private cloud (NL Rijksoverheid) Alle digitale overheidsdiensten van Caribisch Nederland worden gehost in bestaande datacenters of cloudomgevingen van de Nederlandse Rijksoverheid in EN. Er is geen lokale housing- of infrastructuurvoorziening op de eilanden zelf.
6	Volledig public cloud (wereldwijd) Alle digitale diensten draaien bij een commerciële publieke (wereldwijde) cloudprovider. Er wordt gebruikgemaakt van standaard clouddiensten via het internet.
7	Managed private cloud (Europese leverancier, soevereine cloud) Een Europese IT-dienstverlener biedt een op maat gemaakte private cloudomgeving voor Caribisch Nederland. Deze wordt beheerd op een afgescheiden infrastructuur, binnen Europese jurisdictie.
8	Outsourcing naar lokale partij in CN (bijv. lokale telecom of regionaal datacenter) Een lokale (bijv. telecom) of regionale (bijv. op Bonaire gevestigde) partij levert housingdiensten voor overheidsdata. De infrastructuur bevindt zich fysiek in Caribisch Nederland.
9	Hybride cloud (mix van lokale servers en cloud diensten) Afhankelijk van de aard van de toepassing wordt gekozen voor lokale housing of cloud-diensten binnen de EU. De IT-omgeving bestaat uit een combinatie van lokale infrastructuur en publieke of private cloud.
10	Twin-datacenter CN / EN (DC Bonaire – DC Europees Nederland) Er is een datacenter gevestigd op Bonaire en een datacenter in Europees Nederland. De datacenters zijn elkaars backup en uitwijk.

De varianten lopen van volledig lokaal (variant 1 en 2) tot volledig extern (variant 6-7) en hybride mengvormen (varianten 3, 4, 8, 9, 10). In de onderstaande subparagrafen is een beschrijving opgenomen.

8.3 Variant 0: Voortzetten huidige situatie (as-is)

Zolang er geen expliciete beleidsmatige keuze wordt gemaakt voor een toekomstige inrichting van datacenter- en hostingvoorzieningen in Caribisch Nederland, blijft de huidige situatie feitelijk van kracht. Dit impliceert dat er geen sprake is van een gezamenlijke koers, geen formeel vastgesteld architectuurkader, en geen gecoördineerde sturing op investeringen, beveiliging of continuïteit. Organisaties die gebruik maken van deze datacenter- en hostingvoorzieningen kunnen ook niet voldoen aan de beveiligingsnormen die DigiD stelt voor hun te realiseren DigiD implementatie. In die context moet de bestaande situatie worden beschouwd als een impliciete strategische variant, een 'stilzwijgende voortzetting' van hoe het nu is. De afwezigheid van besluitvorming of regie ís daarmee zelf een variant, met concrete gevolgen voor governance, risicobeheersing, kosten, innovatievermogen en dienstverlening. Dit is de variant "huidige situatie" en is daarmee het nulpunt waaraan andere scenario's worden getoetst.

BESCHRIJVING

Deze variant gaat uit van het behouden van de bestaande situatie waarin overheidsorganisaties binnen Caribisch Nederland verantwoordelijk zijn voor hun eigen datacenter- en hostingvoorzieningen, binnen een bredere context van toenemende centrale afstemming en regie vanuit het CIO-office. Deze situatie kent een hybride karakter: uitvoering en beheer liggen decentraal, terwijl op strategisch en coördinerend niveau steeds meer gezamenlijke sturing plaatsvindt. Rijksoverheden kunnen terecht bij het SSO-CN. Voor wat betreft CIO Office en SSO CN ICT worden de kaders van de Rijksoverheid (BZK KR) gehanteerd. Er is echter geen uniform beleid of kader over de verschillende departementen heen. Er bestaat in deze variant géén integrale datacenterstrategie voor Caribisch Nederland. Het geheel is gebaseerd op centrale afstemming, zonder gezamenlijke langetermijnvisie.

KENMERKEN

Deze variant wordt gekenmerkt door een hoge mate van organisatorische autonomie. Iedere partij maakt in principe eigen keuzes ten aanzien van IT-infrastructuur, dataverwerking en digitale dienstverlening. Tegelijkertijd is er vanuit het RCN en het CIO-office sprake van toenemende coördinatie en afstemming, al is er nog geen formele, gezamenlijke governancestructuur die toeziet op harmonisatie, compliance en toekomstbestendigheid. Een integrale visie op digitale soevereiniteit, dataopslag, security en duurzaam beheer is in ontwikkeling, maar nog niet breed verankerd of operationeel doorvertaald. Capaciteit, expertise en budget verschillen per organisatie, wat leidt tot variatie in het niveau van dienstverlening. De afwezigheid van een vastgesteld overkoepelend kader maakt het lastig om scherp te sturen op samenhang, prioritering en gezamenlijke innovatie.

VOORDELEN

Een voordeel van deze variant is dat organisaties ruimte behouden om eigen keuzes te maken en snel in te spelen op specifieke behoeften of beleidsprioriteiten. Deze autonomie kan besluitvorming op korte termijn versnellen en maakt het mogelijk om lokale dienstverleners in te zetten voor kleinschalige trajecten, wat de lokale economie ten goede komt. Tegelijkertijd vraagt deze flexibiliteit om duidelijke kaders en afstemming, zodat centrale uitgangspunten vanuit het CIO-office en RCN, zoals uniformiteit in beveiliging en duurzame beheersbaarheid, niet onder druk komen te staan.

NADELEN

Hoewel het RCN CIO-office inmiddels een regierol vervult binnen de rijksdienst op de eilanden, blijft de praktijk gefragmenteerd. Organisaties binnen de RCN-kolom beheren deels hun eigen datacenter- en hostingvoorzieningen, met verschillen in volwassenheid, schaalgrootte en technische capaciteit tot gevolg. Hierdoor is het lastig om binnen de Rijksoverheidskaders strategisch samenhang aan te brengen in zaken als beveiliging, lifecyclebeheer, innovatie en duurzaamheid. Een integrale datacenterstrategie ontbreekt, waardoor gezamenlijke sturing op interoperabiliteit, kostenefficiëntie en risicobeheersing beperkt blijft. Dit vergroot de kwetsbaarheid voor cyberdreigingen, datalekken en operationele uitval. Deze versnipperde praktijk sluit onvoldoende aan op het rijkscloudbeleid, de Nederlandse Digitaliseringsstrategie, de eisen die DigiD stelt en de toezichteisen van de Rijksinspectie Digitale Infrastructuur. Marktwerking vindt momenteel grotendeels ad hoc plaats, hoewel steeds vaker coördinatie gezocht wordt. Aanbestedingskaders uit Europees Nederland worden doorgaans gevolgd, maar een centrale, gezamenlijke langetermijnvisie op de digitale infrastructuur ontbreekt. Hierdoor ontstaat het risico op wildgroei, afhankelijkheid van niet-gecertificeerde leveranciers en suboptimale

investeringsbeslissingen. De huidige situatie is bovendien capacitair begrensd: bestaande voorzieningen bieden onvoldoende ruimte om groei en toenemende digitale afhankelijkheid op te vangen. Daarnaast ontbreekt een gestructureerd afwegingskader voor de plaatsing van systemen in Caribisch Nederland (lokaal, regionaal of in Europees Nederland), wat leidt tot ad-hocbesluiten en suboptimale keuzes. Zolang er geen structurele integratie plaatsvindt van centrale kaders, rollen en verantwoordelijkheden, blijft de digitale infrastructuur kwetsbaar en versnipperd.

CONCLUSIE

De variant waarin de huidige situatie wordt gecontinueerd en géén datacenterstrategie voor Caribisch Nederland wordt vastgesteld, is vanuit beheergemak op korte termijn aantrekkelijk voor individuele organisaties, maar wordt door stakeholders gezien als onhoudbaar voor de middellange en lange termijn. De variant voldoet niet aan de strategische uitgangspunten die binnen dit traject zijn vastgesteld en scoort zeer laag op vrijwel alle inhoudelijke en operationele criteria. De variant voldoet, zonder aanvullende maatregelen, ook niet aan de eisen die DigiD stelt aan de informatiebeveiliging van de datacenter-infrastructuur. Het ontbreken van schaalgrootte, gezamenlijke investeringen én visie maakt deze variant inefficiënt, risicovol en ongeschikt als fundament voor verdere digitale ontwikkeling in Caribisch Nederland.

8.4 Variant 1: Lokale datacenters voor Bonaire, Saba en Sint Eustatius

BESCHRIJVING

Bonaire, Sint Eustatius en Saba krijgen hun eigen volwaardige datacenter. Er is geen centraal datacenter, wel zouden de drie kunnen synchroniseren, maar primair werkt het op elk eiland zelfstandig. Dit is de meest decentraliseerde optie. Housing is lokaal op Bonaire, Sint Eustatius en Saba. Hosting is de lokale verantwoordelijkheid.

KENMERKEN

Men bouwt op elk eiland een datacenter met lokale redundantie. Bijvoorbeeld Bonaire een iets grotere, Saba en Sint Eustatius kleinere. Elke overheidstaak draait op het eigen eiland, met eventueel replicatie van data tussen de eilanden voor uitwijk of backup. Bij uitval van één datacenter kunnen de anderen beperkt bijspringen via kopieën van data, maar feitelijk is er geen echte uitwijk, hoogstens neemt Bonaire een deel van de load over van Saba/Sint Eustatius als die plat zijn, en vice versa.

VOORDELEN

Zeer soeverein en zelfstandig per eiland, weinig afhankelijkheid van interinsulaire verbindingen voor primaire processen. Latency is laag binnen elk eiland, lokale gebruikers hebben hun data lokaal. Politiek geeft het maximale zeggenschap aan de Openbare Lichamen. Ook risico's van één point of failure zijn verminderd, als Bonaire DC faalt, blijven Saba en Sint Eustatius door eigen DC's draaien (zij het alleen hun eigen processen). Verder levert het maximale lokale werkgelegenheid (drie locaties bemensen).

NADELEN

Deze variant is duur en minder efficiënt. Drie separate datacenters op +/-20k, +/-3k en +/-2k inwoners is schaaltechnisch extreem klein. Investeringen moeten driedubbel gebeuren. Daarnaast is het beheer complex, er zijn onvoldoende gekwalificeerde mensen op de eilanden en voor bijvoorbeeld SSO-CN geldt dat men drie omgevingen synchroon moet houden met zeer beperkt personeel. Het voldoet nu niet aan het principe "Data in EER of op EU-niveau binnen CN omdat de eilanden nu niet op EU-niveau zitten. Continuïteit is moeilijker te garanderen, elk eiland heeft maar één locatie, dus geen uitwijk per eiland (behalve backuppen bij de twee andere eilanden, maar die infrastructuur zou weer extra zijn). Ook application management wordt complex, als de Belastingdienst iets uitrolt, moet het op 3 plekken gebeuren, wat foutgevoelig is. Governance-wise is er nauwelijks centrale regie, dat druist in tegen het uitgangspunt van één overheidsbrede aanpak. Op Saba en Sint Eustatius is zo weinig IT-personeel dat een datacenter daar runnen enorme afhankelijkheid van enkele individuen creëert (single points of human failure). Ook dient ieder datacenter aan dezelfde hoge eisen te voldoen die er binnen de juridische en beleidskaders gesteld worden, wat de opzet extra complex en kostbaar maakt.

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant lijkt op de huidige situatie in de zin dat ook hier iedere entiteit zelfstandig opereert. Echter, er wordt wél bewust gekozen voor lokale fysieke voorzieningen per eiland met mogelijk betere voorzieningen dan nu. Dit zorgt voor een minimale kwaliteitsimpuls, maar de fragmentatie en het gebrek aan centrale regie blijven grotendeels bestaan. De schaalproblemen en risico's op versnippering blijven identiek aan de huidige situatie.

CONCLUSIE

Scenario 1 is een optie omdat het maximale lokale beschikbaarheid en onafhankelijkheid biedt, ook bij uitval van onderlinge of externe verbindingen, een cruciaal aspect gezien de geografische isolatie en kwetsbare infrastructuur van de eilanden. Aandachtspunten zijn kosten, organisatie, weerbaarheid en uitdagingen ten aanzien van de bestuurlijke verantwoordelijkheid. Op dit moment wordt ook niet voldaan aan EU wet- en regelgeving of data in de EER.

8.5 Variant 2: Twin Data Center in Caribisch Nederland

BESCHRIJVING

Er komen twee datacenters, beide gelegen in Caribisch Nederland, elk op een ander eiland om geografische spreiding en minder afhankelijkheid van verbindingen te waarborgen. Eén datacenter wordt voorzien op Bonaire en het tweede op Sint Eustatius of Saba. De nader te maken keuze tussen Sint Eustatius of Saba is o.a. ingegeven door de aanwezige basisinfrastructuur, stabiele elektriciteitsvoorziening, de beschikbaarheid van ruimte, inwoneraantal en de aanwezigheid van kennis en expertise. In dit onderzoek is ervan uitgegaan dat Sint Eustatius de meest geschikte locatie betreft, echter heeft er geen fysiek bezoek aan Saba of Sint Eustatius plaats gevonden. Nader onderzoek op geschiktheid is gewenst om hier uitsluitsel over te geven. Deze twee datacenters kunnen functioneren als een twin-datacenter, in actief-actief opstelling samenwerken. Housing wordt lokaal ingericht, waarbij bijvoorbeeld de overheden beneden- en bovenwinds (deels) hun eigen voorzieningen beheren. Hostingdiensten kunnen centraal, deels op afstand, door overheidsdienstverleners worden verzorgd.

KENMERKEN

De term twin-datacenter is een dienstverleningsterm die verwijst naar een opzet waarbij twee datacenters parallel worden ingezet. Hostingdiensten kunnen daarbij zodanig worden ingericht dat sommige systemen actief-actief over beide locaties draaien. Dit verhoogt de beschikbaarheid en borgt continuïteit bij uitval of onderhoud. Belangrijk is dat het 'twin-datacenter' een keuze is in de inrichting van dienstverlening, en niet per definitie bestaande locatie gebonden voorzieningen vervangt, zoals colocatie of minder kritieke toepassingen.

In de praktijk betekent dit bijvoorbeeld dat dienstverlening voor afnemers op Bonaire normaal gesproken primair vanuit het datacenter op Bonaire wordt geleverd, terwijl voor Saba en Sint Eustatius het datacenter op één van de beide bovenwindse eilanden als primaire locatie fungeert. Bij uitval van één locatie neemt de andere automatisch de dienstverlening over (failover). Op deze manier zijn alle drie de eilanden verbonden binnen het twin-datacenter netwerk.

VOORDELEN

Hoge beschikbaarheid kan worden gerealiseerd binnen Caribisch Nederland, twee geografisch gescheiden centra betekent dat een ramp op één locatie de diensten niet totaal onderbreekt. De latency tussen de twee datacenters (via interinsulaire verbinding) is relatief laag, dus near real-time synchronisatie van data kan mogelijk werken. Soevereiniteit is hoog voor de organisaties binnen Caribisch Nederland (alles blijft in het eigen gebied). De datacenters op de eilanden blijven operationeel zelfs als de verbindingen met Europees NL wegvallen, zolang beide datacenters in CN blijven draaien. Het benut de schaal door middelen te concentreren in twee plekken i.p.v. drie (beter dan variant 1). Het geeft ook Bonaire wat ontlasting omdat de tweede site op Sint Eustatius of Saba is, zo worden verantwoordelijkheid en misschien economische impuls verdeeld. Daarnaast biedt de opzet de mogelijkheid om de huidige en toekomstige Rijksoverheidsinitiatieven (bijv. Rijkscloud) tevens te hosten in deze datacentra, alsmede om back-up van systemen in Europees Nederland, geografisch veilig te stellen in Caribisch Nederland. (Transcontinentale back-uplocatie met nationale zeggenschap, ook wel Geo-soevereine back-uplocatie genoemd.)

NADELEN
Hoewel beter dan 1, nog steeds kostbaar. Twee kleinschalige datacenters onderhouden is kostbaar, zeker vergeleken met gebruik van een bestaande faciliteiten in EN. Ook deze variant zit met de Data in EER eis: data staat in CN (buiten EER). Verder blijft afhankelijkheid van lokale resources hoog: er is nog steeds relatief weinig kritische massa qua IT-team op de eilanden om twee centers te runnen, al kun je ze centraal aansturen. Qua weerbaarheid tegen orkanen is het iets beter als de sites gespreid worden (bijv. Bonaire en Sint Eustatius/Saba liggen ver uit elkaar, de kans dat beiden tegelijk door een orkaan getroffen worden is klein). Nadeel is dat de netwerkverbinding tussen beide locaties een kritieke afhankelijkheid vormt: deze moet voldoende betrouwbaar en stabiel zijn om synchronisatieproblemen te voorkomen. Wel kunnen de datacenters zo worden ingericht dat ze bij een tijdelijke onderbreking zelfstandig kunnen blijven functioneren, ieder als afzonderlijke voorziening. Die verbinding gaat echter nu via externe routes (Sint Eustatius/Saba-Bonaire gaat via meerdere hops (en andere landen) in de regio). Dit is een risico. Governance: centraler dan variant 1, maar nog steeds twee datacenterlocaties met mogelijk eigen dynamiek, wat vraagt om strakke regie.

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE
Deze variant vormt een gedeeltelijke breuk met de huidige situatie. Door te investeren in twee geografisch verspreide, redundant opererende datacenters wordt de continuïteit over de boven- en benedenwindse eilanden sterk verbeterd, net als de schaalbaarheid en efficiëntie. Er ontstaat een platform voor gezamenlijke regie, standaardisatie en lifecyclemanagement. Deze variant sluit beter aan op overheidsbeleid en biedt ruimte voor coördinatie en groei. Hergebruik en eventuele uitbreiding van bestaande faciliteiten op Bonaire behoren tot de mogelijkheden, wat ook een tijdelijke optie kan zijn wanneer er wordt ingezet op de bouw van een nieuwe locatie.

CONCLUSIE
Variant 2 komt dicht in de buurt van wat we wensen qua zeggenschap en continuïteit lokaal, maar heeft uitdagingen met compliance-issues (niet in EER) en kosten. Het is een serieuze kandidaat in de analyse.

8.6 Variant 3: Lokaal DC + edge + EU back-up

BESCHRIJVING
Deze hybride variant combineert een primair lokaal datacenter op Bonaire, aangevuld met kleine edge-locaties op Saba en Sint Eustatius, en een back-up locatie in Europees Nederland (bijvoorbeeld in een overheidsdatacenter of cloud) voor disaster recovery. Met andere woorden: alles is lokaal, maar er is toch een backup in NL achter de hand.

KENMERKEN
Bonaire DC draait alle productie-workloads. Saba en Sint Eustatius hebben micro-datacenters (zoals omschreven in 6.1) voor caching en kritieke lokale taken. Daarnaast wordt periodiek of real-time data weggeschreven naar een datacenter in Europees Nederland (bijvoorbeeld ODC-Noord) als veilige achtervang. Die E-NL-locatie staat koud of draait laagbelast mee, en zou pas bij een calamiteit in Caribisch gebied actief de diensten overnemen (dit zou ingewikkeld zijn gezien de latency, dus meer waarschijnlijk is dat dit alleen voor data-back-up is en niet voor live failover).

VOORDELEN
Deze variant probeert het beste van twee werelden: maximale performance en zelfstandigheid lokaal, plus het comfort dat als er echt iets misgaat (bijv. een orkaan verwoest Bonaire datacenter) de data veilig is in Nederland en men eventueel vanuit daar kan doordraaien in beperkte vorm. Latency voor gebruikers is goed (want primair blijft lokaal). De edge op Saba/Sint Eustatius zorgt voor nog fijnmaziger goede performance en vangt eilandisolatie deels op. Soevereiniteit is goed geborgd (primair in CN, backup in NL is ook eigen beheer).

NADELEN
De complexiteit is hoog: drie lagen (Bonaire, meerdere edges, NL backup). Het vraagt een architectuur die consistent over deze lagen synchroniseert, dat is lastig en kans op fouten is groter. BIO/NIS2 compliance kan een punt zijn: de 'edge' locaties zullen als volwaardige datacenters gebouwd moeten worden om aan deze compliancy en richtlijnen te voldoen, waardoor deze optie meer gaat lijken op variant 1. Kosten zijn ook hoger:

je investeert zowel in lokale infra als in een hele E-NL omgeving (al kan dat bij een bestaand DC). Deze variant kan wat over-engineered zijn: wellicht gebruik je de NL backup nooit, maar je betaalt er wel voor. Continuïteit is zeer hoog, maar heb je werkelijk zowel lokaal als op afstand volwaardig nodig? Geschiktheid van workloads op deze basis (edge) hangt heel erg af van de applicatie of toepassing, het is dus niet zo dat elke applicatie of toepassing zich leent voor een dergelijk scenario.

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant is technisch gezien een verbetering omdat het voorziet in moderne hybrid cloud-principes en disaster recovery. De lokale regie blijft echter versnipperd. De structuur is complexer dan in de huidige situatie, en zonder centrale aansturing kan dit juist leiden tot grotere risico's en inefficiënties.

CONCLUSIE

Variant 3 is een ambitieuze hybride. Hij haalt de uitgangspunten nagenoeg, maar tegen prijs van complexiteit en kosten. In de afweging blijkt dat deze variant in feite een voorloper is van variant 10, maar dan met extra edge-locaties. Je zou variant 10 kunnen uitbreiden met edges zonder dat als aparte variant te zien. Daarom is variant 3 in latere fase minder benadrukt, we bekijken edge-faciliteiten als onderdeel van uitvoering in elk scenario in plaats van als apart strategisch besluit.

8.7 Variant 4: Primair EU, lokaal noodplatform

BESCHRIJVING

Het omgekeerde van variant 3: de primaire datacenters staan in Europees Nederland (bijv. rijkscloud of commercieel datacenter in EU), en op de eilanden is enkel een klein lokaal noodplatform aanwezig dat bij een verbroken verbinding basale functies overneemt.

KENMERKEN

Dit scenario is feitelijk het werken zoals bij de Rijksoverheidsorganisaties in Europees Nederland al gebeurt. De servers draaien in Europees NL (Den Haag, Amsterdam of cloud), gebruikers op de BES benaderen die via het internet. Voor Caribisch Nederland wordt dan een lokaal "noodplatform" (kleine kritische voorziening op één plek in CN) ingericht, voor het geval de verbinding wegvalt. Op dit platform draaien minimale diensten om de tijd van de calamiteit te overbruggen, bijv. een cache van essentiële data en een offline modus voor registratie van gebeurtenissen, die later gesynchroniseerd wordt. Housing ligt dus in NL hoofdzakelijk, hosting vermoedelijk bij een Nederlandse partij (ODC/SSC-ICT), en lokaal is zowel housing als hosting minimaal (een noodomgeving door SSO-CN beheerd). Hiervoor kan het huidige datacentrum gebruikt worden, al zal deze dan grotendeels leeg zijn.

VOORDELEN

Deze variant minimaliseert investeringen lokaal. Het benut schaalvoordelen en bestaande infrastructuur in E-NL maximaal. Data is in EER, beveiliging op het niveau van de grote overheidsdatacenters, en beheer gebeurt door ervaren teams in E-NL. Voor compliance en standaarden is dit "eenvoudig" want men plaatst de BES in de reguliere rijkscloudomgeving. Kosten kunnen lager uitvallen qua investering (al zal operationeel wel betaald moeten worden voor gebruik van overheidsdatacenters of cloud, maar geen eigen gebouw etc.). Voor de ministeries is dit overzichtelijk: CN wordt een regio in hun systeem.

NADELEN

Continuïteit bij verbindingsuitval is zeer problematisch, ook al is er een noodplatform, dat kan nooit alle diensten bevatten. Bij een kabelbreuk kunnen burgers misschien nog basis zaken lokaal doen maar alles wat centralistisch is ligt plat. Die risico's zijn onacceptabel. Ook latency is permanent hoog voor gebruikers, wat gebruikerservaring en functionaliteit die zowel tijdige als real-time input vereisen belemmert. (Sommige applicaties werken niet goed door hoge en onvoorspelbare latency. Dit is de reden waarom dit nu (meestal) ook niet gebeurt. Daarnaast zijn sommige applicaties vanwege risico/veiligheidsinstellingen onwerkbaar gebleken vanwege korte systeemresponsetijden op beveiligingchallenges. (Het verzoek van authenticatie en de tijd dat het duurt dat de authenticatie heen en weer gaat blijkt te groot om snel genoeg te kunnen reageren.) Lokale soevereiniteit is nihil, alles ligt bij EN. Dit kan politiek en qua wendbaarheid lastig zijn (de eilanden zouden bij elke aanpassing naar EN moeten leunen). Bovendien wordt ontwikkelkracht CN niet vergroot, men blijft

afhankelijk. Variant 4 voldoet strikt genomen wel aan veel uitgangspunten (AVG/EER, centrale regie), maar schiet tekort op weerbaarheid en wellicht op maatwerk voor de eilanden. Het is ook de vraag of de openbare lichamen en eventuele semi-overheid van de datacenterdienstverlening in Europees Nederland gebruik kunnen maken, vanwege de focus van Rijksoverheidsdienstverleners op het leveren van diensten aan alleen de Rijksoverheid en de specifieke wetgeving voor BES die afwijk van EN (o.a. AVG, WDO, Wabb).

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant biedt op een aantal punten winst ten opzichte van het huidige landschap: betere compliance, lifecyclebeheer, beveiliging en kostenbeheersing door consolidatie in een Europees datacenter. Echter in de praktijk biedt deze variant geen meerwaarde op zowel (netwerk)technisch als functioneel gebied, en een achteruitgang ten opzichte van de huidige situatie. De afhankelijkheid van externe verbindingen (o.a. zeekabels) maakt deze variant kwetsbaarder bij uitval en resulteert in grote performancerisico's.

CONCLUSIE

Variant 4 is een low-effort oplossing die echter in crisisomstandigheden en qua lokale gevoeligheden tekortschiet. Het zou een bewuste keuze zijn als kosten en eenvoud boven alles gaan, maar gelet op het belang van continuïteit is dit geen voorkeursoptie. Weinig stakeholders zijn gecharmeerd van "alles in de cloud, we zien wel bij storingen" – de Openbare Lichamen, burgers en bedrijven hebben te vaak ervaren wat het is als verbindingen eruit liggen.

8.8 Variant 5: Volledig private Cloud (NL Overheidsomgeving)

BESCHRIJVING

Alle diensten worden in een private cloudomgeving van de Nederlandse overheid ondergebracht. Dit kan bijvoorbeeld in de ODC's (Overheidsdatacenters) zijn of een nieuw te creëren eigen cloudomgeving (conform de verwachting in de NDS). Er is geen eigen DC op de eilanden en alle communicatie verloopt over internet. Feitelijk lijkt dit op variant 4, maar benadrukt dat het een private cloud van de overheid is en geen generieke publieke cloud.

KENMERKEN

Housing gebeurt in Nederlandse staatsdatacenters, hosting ook door de overheid (SSC-ICT, ODC-beheer). De Openbare Lichamen en lokale rijks uitvoeringsorganisaties loggen in op systemen die in Europees Nederland draaien. Netwerk via beveiligde verbindingen over het internet.

VOORDELEN

Maximale uitnutting van bestaande investeringen, ODC-Noord en andere datacenters zijn aanwezig met strenge beveiliging en goede compliance. De schaalgrootte is goed (CN is klein aandeel, dus relatief makkelijk mee te nemen). Kosten per eenheid zijn lager omdat CN meedeelt in de massaliteit. Governance is eenvoudig, de BES-ICT valt volledig onder regie van BZK/SSC-ICT. Soevereiniteit, AVG, EER zijn allemaal geborgd. Het principe van één overheid wordt nageleefd doordat CN gewoon deel van de overehidscloud is.

NADELEN

De praktische nadelen zijn vrijwel gelijk aan variant 4: afhankelijkheid van internationale verbinding (geen lokale autonomie), hoge en onvoorspelbare latency (via internet). Ook levert deze variant geen lokale sociaaleconomische bijdrage. Integendeel, lokale IT-functies zouden eerder verdwijnen. Qua weerbaarheid bij een disconnect: net zo slecht als variant 4. Verschil is dat hier niet eens een lokaal noodplatform is voorzien. Men zou dat nog kunnen toevoegen maar dan komt het op variant 4 neer. Voor de Openbare Lichamen is dit waarschijnlijk niet te accepteren: ze hebben geen eigen faciliteiten meer waarbij lokale en cruciale overheidsdienstverlening bij calamiteiten of verbindingsproblemen compleet wegvallen. Ook hier is het de vraag of de openbare lichamen en eventuele semi-overheid van de datacenterdienstverlening in Europees Nederland gebruik kunnen maken, vanwege de focus van Rijksdiensteverleners op het leveren van diensten aan alleen de Rijksoverheid.

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant biedt de mogelijkheid om, ten opzichte van de huidige situatie, te voldoen aan juridische en informatiebeveiligingskaders op het gebied van compliance. Echter in de praktijk biedt deze variant geen meerwaarde op zowel (netwerk)technisch als functioneel gebied, en een achteruitgang ten opzichte van de huidige situatie. De afhankelijkheid van externe verbindingen (o.a. zeekabels) maakt deze variant kwetsbaarder bij uitval.

CONCLUSIE

Variant 5 volgt rijksbrede principes goed, maar negeert de lokale context. In evaluatie (hoofdstuk 9) zal blijken dat hoewel kosten (+), security (+) en governance (+) scoren, dit scenario onaanvaardbare risico's oplevert voor continuïteit en maatschappelijke acceptatie op de eilanden. Tenzij niets anders kan, is variant 5 daarom niet geprefereerd.

8.9 Variant 6: Volledig public cloud (publieke cloud in EER)

BESCHRIJVING

De gehele infrastructuur wordt ondergebracht bij één of meerdere publieke cloudproviders (zoals Microsoft Azure, Amazon Web Services, Google Cloud of een Europese public cloud aanbieder), met de expliciete voorwaarde dat data in Europese datacenters van die providers blijft (dus bijvoorbeeld Azure West-Europe region).

KENMERKEN

Geen eigen datacenter, geen eigen hardware, alles draait als IaaS/PaaS of SaaS in de cloud. De overheid configureert virtuele netwerken en servers bij de provider. Hosting taken kunnen deels door de provider (managed services) en deels door het overheidsteam gedaan worden, afhankelijk van de service-model (IaaS vs. SaaS).

VOORDELEN

Maximale schaal en wendbaarheid. Je kunt naar behoefte op- en afschalen. Nieuwe diensten zijn snel te activeren. Kosten kunnen lager lijken (geen kapitaalinvestering, pay-as-you-go), hoewel op lange termijn publieke cloud meestal niet de meest gunstige optie is. Innovatie: men kan moderne cloud tooling inzetten (AI, big data) makkelijker. Public cloud providers hebben doorgaans zeer geavanceerde beveiliging en is redundantie te bouwen – een AWS/Azure region heeft meerdere zones, 99.99% uptime e.d. Bovendien spreiden ze risico: zelfs een orkaan beïnvloedt de datacenters in Europa niet. Dit model vergt weinig eigen IT-infra kennis; het vermindert de operationele last op partijen zoals een SSO-CN (meer regie, minder beheer).

NADELEN

De nadelen zijn significant in termen van soevereiniteit en afhankelijkheid. Ook al kies je een EU-regio, de grote providers zijn vaak Amerikaans of hebben investeerders uit andere landen, wat juridische risico's geeft (Patriot/Cloud Act). De Autoriteit Persoonsgegevens uitte zorgen dat de Rijksoverheid onvoldoende plan heeft als zo'n cloudleverancier zou wegvallen. Dat risico zou hier volledig spelen, CN zou nagenoeg volledig afhankelijk worden van een handje vol buitenlandse 'big-tech' bedrijven. Daarnaast blijft het netwerkissue bestaan, gebruikers op de eilanden moeten via internet de cloud bereiken. Bij onderbreking is er geen lokale fallback tenzij men hybrid inzet (maar dat is dan niet "volledig" public cloud meer). Dus continuïteit bij kabeluitval is slecht. Ook performance hangt af van vaak onvoorspelbare internet latency en throughput. Een SaaS als Microsoft 365 werkt wel goed over internet, maar een volledig cloudgebaseerde werkplek met hoge interactiviteit lijdt eronder. Verder zijn er zorgen over aanbestedingsregels, dit zou een gunning aan een grote partij betekenen, wat Europees aanbesteed zou moeten worden. Marktwerking lokaal wordt gepasseerd. Tenslotte krijgen de eilanden geen lokale versterking, het geld gaat naar multinationals, niet naar lokale economie.

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant is op technisch vlak een sprong vooruit: schaalbaar, up-to-date, efficiënt. Vergeleken met de huidige situatie is dit een modern alternatief, maar governance en afhankelijkheid van marktpartijen zijn kritische aandachtspunten. Zonder centrale regie is het risico op wildgroei net zo groot als nu. In de praktijk

biedt deze variant geen meerwaarde op zowel (netwerk) technisch als functioneel gebied, en een achteruitgang ten opzichte van de huidige situatie. De afhankelijkheid van externe verbindingen (o.a. zeekabels) maakt deze variant kwetsbaarder bij uitval.

CONCLUSIE

Variant 6 is aantrekkelijk vanuit modern IT-perspectief, maar botst met een aantal strategische uitgangspunten (soevereiniteit, regie) en praktische eisen (verbinding). Bij de Rijksoverheid staat cloudgebruik inmiddels onder druk vanwege de huidige mondiale ontwikkelingen (VS, China, Rusland), in dit geval zouden te veel risico's samenkomen (connectiviteit, vendor lock-in). Zonder aanvullende maatregelen is deze variant ongeschikt als datacenterstrategie voor CN.

8.10 Variant 7: Private cloud in EU (managed dienstverlener)

BESCHRIJVING

Deze variant lijkt op variant 6, maar in plaats van grote publieke cloudproviders betreft het een private cloudoplossing bij een Europese partij. Bijvoorbeeld een managed datacenterdienst door een bedrijf als Equinix (Amerikaans), BIT, of een overheids-gezinde partij via een Europese aanbesteding. Data blijft in EU, provider is niet per se Big Tech maar een kleinere gespecialiseerde.

KENMERKEN

Zeer beperkte eigen DC op BES. Uitgangspunt is dat apparatuur bij de dienstverlener in Europa staat. Die partij levert IaaS of zelfs managed hosting. De overheid controleert op afstand via contracten.

VOORDELEN

Ten opzichte van public cloud iets meer maatwerk en wellicht betere juridische positie. Men kan in contract eisen stellen op maat (b.v. data blijft in NL, toetsing op Patriot Act risico, etc.). Wellicht kan men een constructie doen waarbij de infrastructuur feitelijk van de overheid blijft (onze eigen servers colocated), maar de partij beheert ze, dat geeft wat soevereiniteitsbehoud. De performance, schaal en kostenvoordelen zijn vergelijkbaar met variant 6 (deels). Men heeft minder investeringskosten upfront. En in EU dus wel compliance met AVG etc. Bovendien zou zo'n partij mogelijk bereid zijn een stukje dedicated verbinding te regelen (bijv. eigen capaciteit via zeekabels van Amsterdam naar Bonaire), wat performance iets verbetert.

NADELEN

Nog steeds geldt dat de primaire dienstverlening off-island is. Dus connectivity blijft problematisch en latency hoog en onvoorspelbaar. De afhankelijkheid is verplaatst van big tech naar een kleinere partij, maar als die faalt of het contract beëindigt, zit men ook met een probleem (al is exit wellicht makkelijker dan bij public cloud waar data in proprietary formaten kan zitten). Voor de lokale situatie is er weinig verschil, bij kabeluitval is men offline. Governance is enigszins eenvoudiger dan bij mega-cloud (je hebt accountmanagers etc.), maar alsnog minder directe controle dan eigen regie. Kosten kunnen hoger zijn dan zelf doen vanwege winstopslag, of ze kunnen lager zijn door efficiëntie, dat is situatieafhankelijk. In elk geval heb je structurele operationele kosten in valuta die wellicht niet direct op de rijksbegroting van CN drukken maar wel via contract betaald moeten worden. Ook deze variant vraagt een aanbesteding waarbij mogelijk internationaal ingeschreven wordt, niet per se gunstig voor lokale bedrijven (een lokale partij is onwaarschijnlijk geschikt om dit op EU-niveau te doen).

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant biedt structureel betere compliance, beveiliging en professionaliteit dan het huidige versnipperde landschap. De schaalbaarheid en continuïteit zijn aanzienlijk beter, met behoud van soevereiniteit. Mits goed ingericht, biedt het ook betere kostenbeheersing. Echter in de praktijk biedt deze variant geen meerwaarde op zowel (netwerk)technisch als functioneel gebied, en een achteruitgang ten opzichte van de huidige situatie. De afhankelijkheid van externe verbindingen (o.a. zeekabels) maakt deze variant kwetsbaarder bij uitval.

CONCLUSIE

Variant 7 is een middenweg tussen zelf doen en public cloud. In de praktijk zou dit kunnen werken, maar de vraag is of de meerwaarde groot genoeg is t.o.v. variant 5 of 6. Het lost niet het kernprobleem van verbinding op. Continuïteit (netwerkuitval) is onvoldoende geborgd en latency issues blijven bestaan. Het geeft iets betere

grip op jurisdictie dan 6, maar blijft minder dan varianten met een eigen aanwezigheid. In beoordeling zal variant 7 op veel punten neutraal scoren (≈), het is niet uitgesproken slecht of goed, meer een mogelijke pragmatische oplossing als de overheid zelf het niet wil doen maar ook niet naar Big Tech wil.

8.11 Variant 8: Lokale outsourcing CN

Beschrijving: De overheid besteedt het realiseren en exploiteren van een datacenter in Caribisch Nederland uit aan een marktpartij (of consortium) ter plekke. Dit kan een lokaal telecombedrijf zijn of een internationale datacenteroperator die in CN iets komt bouwen. De partij verzorgt housing en mogelijk ook hosting, de overheid is afnemer van diens diensten.

KENMERKEN

Er komt fysiek één of meerdere datacenters, maar het is eigendom van/gerund door een bedrijf. Dat bedrijf kan daarnaast ook andere klanten bedienen (als dat mag van de overheid). Deze manier van samenwerking wordt ook vaak als Publiek Private Samenwerking (PPS) ingestoken. De overheid sluit een SLA-contract af voor beschikbaarheid en krijgt racks of virtuele capaciteit in dat datacenter. Mogelijk blijven er ook kleine faciliteiten op Saba/Sint Eustatius als deel van contract (dat zouden subcontracts kunnen zijn met telco's daar).

VOORDELEN

De overheid hoeft zelf niet te investeren in vastgoed en technische opbouw, dat doet de marktpartij. Dit kan sneller en eventueel goedkoper (bedrijfsleven kan efficiënter bouwen soms, en ze kunnen kosten spreiden als ze meer klanten hebben). Het legt risico's (bv. van kostenoverschrijding of operationele problemen) deels bij de opdrachtnemer. Voor Caribisch Nederland biedt het potentieel een stimulans aan de markt. Een professioneel datacenter op Bonaire waar ook andere bedrijven gebruik van kunnen maken, kan een hub vormen. Het speelt in op de wens tot marktwerking en voorkomt een te grote overheidsinterventie in de markt. Soevereiniteit kan geborgd worden via contractuele eisen (bijv. dat data in CN blijft, en mogelijk dat Nederlands recht van toepassing kan zijn, etc.). De overheid kan zich focussen op regie voeren en niet op technisch beheer.

NADELEN

De markt op de eilanden is zeer beperkt. Feitelijk zijn er maar 1 of 2 spelers die in aanmerking zouden komen. Als zo'n partij alle kritieke systemen gaat hosten, ontstaat een monopolypositie en afhankelijkheid die potentieel nog groter is dan nu (nu heeft de overheid het zelf in de hand, dan niet meer). Ook is onzeker of lokale partijen voldoende expertise en continuïteit hebben voor een dergelijke taak, er is een reëel risico dat de overheid alsnog intensief moet ondersteunen (of in het ergste geval het overnemen als de partij faalt). Aanbestedings-technisch is dit complex, een EU-aanbesteding zou ook Europese firma's aantrekken die wellicht geen vestiging op de eilanden hebben, wat weer de uitvoerbaarheid beïnvloedt. Verder is er de kwestie van controle: voldoet de partij aan BIO/NEN7510 etc? Moet er extern toezicht op? De RDI zou bijvoorbeeld wel toezicht moeten kunnen houden, dus de contracten moeten dat regelen. Financiering kan een obstakel zijn, een bedrijf zal een langjarige garantie (contract van >10 jaar) willen voordat het miljoenen investeert. De overheid committeert zich dan voor lange tijd, wat flexibiliteit wegneemt. Ook het marktwerkingsaspect, als de overheid dit gunt aan één partij, sluit dat andere uit, mogelijk tot ongenoegen van niet-winnaars. Juridisch en politiek moet dat goed onderbouwd zijn.

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant sluit aan bij de huidige situatie, maar verschilt doordat het primaire datacenter geen eigen faciliteit meer is en de rol van lokale partijen structureel wordt vastgelegd. Er is meer kans op professionalisering, maar ook risico's rond marktverstoring, beperkte schaalgrootte en afhankelijkheid van één of meerdere marktpartij(en).

CONCLUSIE

Variant 8 is in theorie aantrekkelijk wegens ontzorging en lokale economie, maar in praktijk risicovol. We hebben immers te maken met een kleine markt zonder concurrentie, precies de situatie die al tot hoge internetprijzen leidde. Deze variant zou alleen goed gaan als er een zeer betrouwbare partner is en de overheid een waterdicht contract maakt. In de evaluatie zal variant 8 gemengde score hebben: goed op ontwikkelkracht (lokale bedrijvigheid), twijfelachtig op risico's en governance (afhankelijkheid van één leverancier). Transparantie en sturing moeten dan top geregeld zijn.

8.12 Variant 9: Hybride cloud per workload

BESCHRIJVING

In deze variant is er geen eenduidige keuze "alles hier of daar", maar wordt per applicatie of dienst besloten of deze lokaal draait of in de cloud. Het is feitelijk een mix van meerdere voorgaande varianten op het niveau van workloads. Bij een gedegen afweging kan altijd besloten worden een vorm van cloud af te nemen. Bijvoorbeeld: kritieke basisregistraties draaien lokaal op Bonaire, standaard zakelijke applicaties (mail, SharePoint) gaan naar Microsoft 365 cloud, een deel van systemen draait bij SSC-ICT in NL, een deel op een platform van een cloud-provider etc.

KENMERKEN

Het is een gedistribueerd model, sommige systemen in het bestaande DC op Bonaire, sommige in publieke cloud. De orkestratie gebeurt via goede netwerkintegratie en identity management, zodat gebruikers dat niet merken. De overheid fungeert als integrator van meerdere omgevingen. Housing/hosting is dus verdeeld: deels lokaal, deels extern, en de mix kan wijzigen over tijd.

VOORDELEN

Zeer flexibel en maatwerkgericht. Men benut voor elke toepassing de meest geschikte omgeving. Dit kan kosten optimaliseren (men zet zware workloads waar het goedkoopst is), prestaties optimaliseren (latencygevoelige dingen lokaal, rest remote) en risico's spreiden (niet alles op één plek of technologie). Bovendien kan men stapsgewijs moderniseren: legacy blijft on-prem, nieuwe dingen gaan cloud-native bijvoorbeeld. Het sluit ook goed aan bij de huidige werkelijkheid waarin sommige zaken al SaaS zijn en andere niet, het vereist geen rigide alles-of-niets beslissing.

NADELEN

De complexiteit van zo'n multi-cloud/hybrid beheer is hoog. Men moet personeel hebben dat zowel lokale infra als diverse cloudomgevingen kan managen. Ook beveiliging wordt lastiger, consistente beveiligingspolicies over meerdere platforms (denk aan identity, logging) is een uitdaging. Het vergt geavanceerde regie om te zorgen dat kosten niet uit de hand lopen en dat er geen "shadow IT" ontstaat (afdelingen die buiten de boot vallende apps in weer een andere cloud zetten). Voor Caribisch Nederland kan dit, gezien de beperkte capaciteit en kennis op dit terrein, al snel te veelomvattend zijn om beheersbaar te houden. Binnen een hybride cloudarchitectuur, waarbij verschillende componenten verspreid zijn over meerdere locaties en omgevingen, staat de consistentie van dienstverlening onder druk.
In het geval van bijvoorbeeld een netwerkstoring is het onduidelijk welke onderdelen van het systeem operationeel blijven. Sommige componenten – lokaal of in de cloud – kunnen nog functioneren, maar dat garandeert niet dat de dienst als geheel beschikbaar blijft. De kans is aanzienlijk dat de onderlinge afhankelijkheden zodanig zijn, dat het wegvallen van één of meerdere onderdelen elders alsnog leidt tot een verstoring of uitval van de totale dienstverlening. Vanuit de governance- moet men ook nog met meerdere leveranciers tegelijk dealen (Verschillende Public Cloud aanbieders, private cloud aanbieders, overheidsdienstverleners zoals SSC-ICT, enz.) wat onderhandelingen en contractmanagement intensief maakt.

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant overstijgt de huidige situatie door in te zetten op flexibiliteit en schaalbaarheid via hybride oplossingen. Deze variant vereist een strak regiekader als het gaat om duidelijke wet- en regelgeving, zeker gezien de huidige mondiale ontwikkelingen.

CONCLUSIE

Variant 9 is eigenlijk meer een operationele modus dan een strategische keuze, er wordt geen variant gekozen, alles is mogelijk. In de praktijk is dit mogelijk een situatie waar CN eindigt als er geen duidelijke keuzes gemaakt worden, danwel als variant 0 wordt gekozen. Hoewel het flexibiliteit geeft, is het moeilijk te besturen. In de weging zal variant 9 niet als beste uitkomen, omdat het op veel criteria middelmatig scoort: niets helemaal opgelost, maar wel veel complexiteit toegevoegd. Echter, elementen van variant 9 (hybrid werken) zullen hoe dan ook in realisatie voorkomen. Zelfs bij een duidelijke voorkeur voor variant 10 bijvoorbeeld, zul je nog steeds een hybride landschap hebben (je gebruikt ook SaaS etc.). Dus variant 9 als opzichzelfstaand scenario is minder een eindbeeld en meer een overgangsfase of aanvullende benadering.

8.13 Variant 10: Twin-datacenter Caribisch Nederland / Europees Nederland

BESCHRIJVING

Dit betreft de variant waarbij één datacenter op de BES (Bonaire) en één in Europees Nederland (bijvoorbeeld bij ODC-Noord in Groningen of een ander Overheids-DC) wordt gebruikt. Deze kunnen op dienstverleningsniveau (hosting) naar elkaar repliceren en samen als één logische datacentervoorziening dienen.

KENMERKEN

Hosting vindt plaats via overheidsorganisaties, bijvoorbeeld in samenwerking tussen SSO-CN en partijen als SSC-ICT (werkplekdiensten), ODC Noord (IaaS), DICTU of Logius (PaaS). Geadviseerd wordt de architectuur vanuit EN te hanteren zodat standaardisatie vanuit EN wordt doorgezet en ondersteuning in de 3e lijn mogelijk is. Het concept is vergelijkbaar met variant 2, maar de tweede datacenterlocatie ligt niet op Sint Eustatius of Saba, maar in Europees Nederland. Hierdoor staat data deels in CN en deels binnen de Europese Economische Ruimte (EER). De opzet kan actief-actief of actief-passief zijn, afhankelijk van voorkeur en ontwerp. Meestal zal Bonaire de primaire locatie zijn voor lokale diensten, terwijl de NL-locatie fungeert als hub voor koppelingen met andere systemen of partijen. Beide locaties kunnen elkaars functies overnemen bij uitval of onderhoud.

VOORDELEN

Deze variant scoort weliswaar op veel strategische uitgangspunten positief (echter vanuit het perspectief van de Openbare Lichamen Saba en Sint Eustatius zeker niet (zie nadelen)).
Data staat deels in de EER (EN-site) Tegelijk hebben we lokale aanwezigheid, dus bij kabelproblemen naar EN kan het DC op Bonaire Saba en Sint Eustatius blijven bedienen. Continuïteit is uitstekend voor Bonaire: twee volwaardige datacenters, geografisch gescheiden (een orkaan in de Cariben en een stroomstoring in EN zullen zelden tegelijk optreden). Weerbaarheid is dus geborgd (met uitzondering naar Saba en Sint Eustatius). Soevereiniteit blijft ook gewaarborgd, beide sites zijn onder Nederlandse overheid of jurisdictie. Governance kan goed geregeld worden, BZK kan regie voeren, met bijvoorbeeld SSC-ICT verantwoordelijk voor de EN-site exploitatie en SSO-CN voor Bonaire, onder één bestuur. Prioriteitsstelling voor BES-organisaties dient te worden vastgelegd in een Dienstverleningsovereenkomst (DVO), onder sturing van BZK. Ontwikkelkracht: een lokaal team krijgt het Bonaire DC onder zijn hoede, en kan leunen op EN-team voor de zwaarste taken. Tegelijk doet men ervaring op. Marktimpact: doordat een site in EN zit, hoeft men minder capaciteit op Bonaire te bouwen dan variant 2, wat het investeringsniveau daar drukt maar nog steeds substantieel is (dus een redelijke opdracht voor lokale bouw, maar geen monopolie voor lokale IT-bedrijf in exploitatie, de exploitatie is hoofdzakelijk intern rijksdienst, wat binnen de aanbestedingsregels past als "inbesteden"). Dit scenario is ook duurzaam te maken: veel kritieke systemen op E-NL site kunnen draaien op groene stroommix van EN, Bonaire site kan iets kleiner dus minder energieverbruik ter plaatse. Kosten: Hoewel twee sites duur klinken, kan in EN gebruikgemaakt worden maken van al bestaande capaciteit (ODC-Noord, SSC-ICT, Logius of zelfs RWS hebben ruimte). De hardware is nodig voor redundantie, of die nu op Sint Eustatius of Saba staat of in EN, qua stuks niet veel verschil.

NADELEN

Een belangrijk nadeel van deze variant is de afhankelijkheid van Bonaire voor de digitale dienstverlening aan Saba en Sint Eustatius. Om de continuïteit ook daar te waarborgen bij uitval of netwerkstoringen, is uitbreiding met edge-capaciteit op Sint Eustatius of Saba sterk aan te bevelen (variant 2).
Tegelijkertijd zijn er aanzienlijke technische en financiële uitdagingen. De afstand tussen de eilanden, in combinatie met de beperkte infrastructuur, kan leiden tot latency problemen, verminderde performance en verhoogde complexiteit in replicatie. Hoewel asynchrone replicatie van databases technisch mogelijk is, vergt dit zorgvuldige inrichting en beheer. Er is bovendien een reële kans dat kosten en inspanning niet in verhouding staan tot de baten.
Ook vanuit Bonaire blijft afhankelijkheid van de verbinding richting Europees Nederland een aandachtspunt, al is dit minder kritisch. Bij tijdelijke uitval kan Bonaire lokaal blijven functioneren, terwijl de site in Nederland de externe dienstverlening overneemt. Zodra de verbinding is hersteld, kan synchronisatie plaatsvinden. Daarmee is een deel van de kwetsbaarheid gemitigeerd. Wel vereist deze variant forse investeringen, onder meer in extra onderzeese netwerkcapaciteit. Een alternatief is het benutten van bestaande kabelsystemen, waarbij via meerdere routes dedicated capaciteit wordt vastgelegd en contractueel geborgd in meerjarige SLA's. Dit model

is sneller uitvoerbaar en financieel haalbaarder, maar blijft afhankelijk van commerciële partijen en buitenlandse jurisdictie, wat risico's oplevert bij storingen, politieke spanningen of wijziging van eigendomsstructuren.

TOETSING TEN OPZICHTE VAN HUIDIGE SITUATIE

Deze variant kan in vrijwel elk opzicht beter zijn dan de huidige situatie. Door een solide koppeling tussen CN en Europees Nederland ontstaat een robuuste, goed reguleerbare infrastructuur met sterke governance, betere beschikbaarheid en aansluiting op het Rijkscloudbeleid / Overheidscloudbeleid.

8.14 Toetsing varianten op huidige situatie en strategische uitgangspunten

De acht strategische uitgangspunten uit hoofdstuk 5 vormen knock-out criteria voor de 10 varianten uit dit hoofdstuk. In Tabel 3 hieronder (Strategische uitgangspunten vs. varianten) is globaal weergegeven welke varianten op welke punten afwijken. Zo zien we bijvoorbeeld dat variant 6 (volledig public cloud) tekortschiet op het gebied van "Soevereiniteit" (gegevens in handen van buitenlandse partij), maar ook aan andere uitgangspunten voldoet deze variant niet. Deze tabel diende om snel te identificeren welke opties afvallen.

Tabel 3 - Matrix strategische uitgangspunten vs. varianten

variant	EU regelgeving, data in EER	BIO/NIS2 architectuur	Soevereiniteit	Scope CN	Cloudbeleid NL	Weerbaarheid & continuïteit	Ontwikkelkracht CN	Centrale regie
0. Voortzetten huidige situatie	≈	X	X	V	X	X	V	X
1. Lokale DC's per eiland	≈	V	V	V	V	V	V	V
2. Twin DC CN	≈	V	V	V	V	V	V	V
3. Lokaal DC + edge + EU uitwijk	≈	X	V	V	V	V	V	V
4. Primair EU, lokaal noodplatform	≈	V	V	V	V	X	X	V
5. Volledig private cloud (NL Rijksoverheid)	V	V	V	X	V	X	X	V
6. Volledig public cloud (ww)	V	V	X	X	X	X	X	V
7. Private EU-cloud	V	V	V	X	V	X	X	V
8. Lokale outsourcing CN	≈	V	?	V	?	V	V	V
9. Hybride cloud (per workload)	V	V	?	V	X	X	V	V
10. Twin-datacenter CN / E-NL	≈	V	V	V	V	V	V	V

V – Voldoet aan strategisch uitgangspunt
X – Voldoet NIET aan strategisch uitgangspunt
≈ – BES valt juridisch niet onder EER, maar kan mogelijk gemitigeerd worden door harmonisatie van wetgeving en kan dan wel voldoen.
? – Aanvullende juridische borging mogelijk vereist
– Interessante variant op basis van de strategische uitgangspunten

Uit de tabel blijkt onder meer dat er geen enkele variant onmiddellijk en volledig voldoet aan de uitgangspunten. Wel dat enkele varianten hier dichtbij komen, waarbij deze varianten mogelijk met de nodige mitigatie wel kunnen voldoen.

De strategische uitgangspunten zijn 'must-have eigenschappen' van de uiteindelijke strategie, maar bij de gedetailleerde weging in Hoofdstuk 9 komen nog vergelijkende criteria aan bod die helpen om tussen de overgebleven varianten te kiezen.

TOETSING OP 0-VARIANT

De toetsing van de tien varianten is uitgevoerd aan de hand van strategische uitgangspunten, waarbij variant 0 dient als referentiepunt (de huidige situatie). Deze nulvariant wordt niet als volwaardig toekomstscenario beschouwd, maar uitsluitend gebruikt om andere varianten mee te vergelijken. Uit de analyse blijkt dat meerdere varianten significante verbeteringen bieden ten opzichte van de huidige situatie. Vooral variant 2

(Twin DC CN) en variant 10 (Twin DC CN / EN) scoren consistent beter op regie, toekomstbestendigheid, beveiliging en aansluiting bij rijksbeleid. Varianten 1, 3, 6, 8 en 9 blijven dichter bij de huidige situatie en bieden onvoldoende structurele oplossing voor de bestaande governance- en schaalproblemen.

Bij voortzetting van de huidige situatie, moet worden vastgesteld dat het onder deze omstandigheden zonder aanvullende maatregelen niet mogelijk is om cruciale voorzieningen zoals DigiD aan te bieden vanuit Caribisch Nederland. De bestaande datacenters op de eilanden voldoen nu niet aan de technische, juridische en beleidsmatige randvoorwaarden die door Logius en het ministerie van BZK worden gesteld. De netwerkverbindingen tussen Caribisch Nederland en Europees Nederland zijn instabiel en zij hebben een te hoge latency voor betrouwbare productie-integratie met rijksdiensten.

8.15 Conclusie strategische varianten

Op basis van de strategische uitgangspunten blijven drie varianten overeind als realistische richtingen voor de datacenterstrategie van Caribisch Nederland: variant 1 (lokale datacenters per eiland), variant 2 (twin datacenter binnen Caribisch Nederland) en variant 10 (twin datacenter tussen Caribisch Nederland en Europees Nederland). Deze varianten sluiten op verschillende manieren aan bij de fundamenten van de strategie: het borgen van data-soevereiniteit, het garanderen van informatiebeveiliging, het realiseren van weerbaarheid en continuïteit, het ondersteunen van ontwikkelkracht in CN, het expliciet meenemen van de lokale schaal en context, en het waarborgen van centrale regie binnen een heldere governance.

Variant 1 is strategisch verdedigbaar omdat het maximale robuustheid biedt binnen elk afzonderlijk eiland en volledige lokale controle mogelijk maakt. Dit past bij het uitgangspunt dat oplossingen moeten werken binnen de CN-context, ook bij beperkte verbindingen. Variant 2 bouwt daarop voort en vergroot de onderlinge samenhang binnen CN, met failovercapaciteit tussen Bonaire en Sint Eustatius of Saba. Daarmee wordt regionale weerbaarheid versterkt, zonder dat de controle of governance overgaat naar een externe partij. Variant 10 vormt de meest toekomstgerichte invulling van de strategische uitgangspunten: het combineert lokale verankering op Bonaire met centrale sturing en integratie in de overheidsbrede digitale infrastructuur via een tweede locatie in Europees Nederland. Zo wordt invulling gegeven aan centrale regie, aansluiting op overheidsbeleid, borging van publieke waarden en het werken als één overheid, terwijl tegelijkertijd de beschikbaarheid voor CN behouden blijft.

Alle drie de varianten nemen de belangen van Caribisch Nederland serieus en bieden ruimte voor verdere groei, schaalbaarheid en aansluiting op de bredere digitaliseringsambities van de overheid. Andere varianten sluiten aantoonbaar minder goed aan op deze strategische uitgangspunten en vallen daarmee af in het vervolg van dit rapport.

9 WEGING VAN DE VARIANTEN EN AFWEGING KOSTEN/BATEN

In dit hoofdstuk worden de in de vorige paragraaf beschreven varianten systematisch beoordeeld op inhoudelijke en praktische criteria. Deze criteria zijn afgeleid van de eerder beschreven behoeften van stakeholders en de strategische uitgangspunten uit hoofdstuk 4 en 5, en zijn aangevuld met relevante aspecten zoals kosten, duurzaamheid, continuïteit en uitvoerbaarheid. Het doel van deze analyse is om op gestructureerde wijze de baten, risico's en beperkingen van elke variant inzichtelijk te maken en zo een goed onderbouwde voorkeursrichting te bepalen.

De gehanteerde methode is gebaseerd op een kwalitatieve weging, passend bij de aard en scope van dit strategisch adviestraject. De analyse is bewust op hoofdlijnen gehouden, waarbij gebruik is gemaakt van relatieve inschattingen ten opzichte van elkaar. De benadering biedt voldoende inzicht om onderbouwde keuzes te maken, zonder te vervallen in overmatige detaillering. Het resultaat is een afgewogen totaalbeeld dat richting geeft aan de verdere besluitvorming over de datacenterstrategie voor Caribisch Nederland.

9.1 Criteria

In samenspraak met de werkgroep en kerngroep zijn in een workshop de volgende criteria vastgesteld:

KOSTEN

Op basis van een relatieve inschatting van kosten is dit criterium opgenomen. Het betreft een relatieve inschatting van zowel de investeringskosten (capex) als de operationele kosten (opex) over een langere termijn (bijv. 5-10 jaar). We houden daarbij rekening met de orde van grootte: vereist de variant hoge initiële investeringen op de BES of kan er gebruik worden gemaakt van bestaande middelen? Hoe verhouden de jaarlijkse exploitatiekosten zich? Daarnaast spelen indirecte kosten uiteraard ook een rol, zoals benodigde subsidies of onvoorziene kosten bij calamiteiten. Een uitwerking van de kosten per scenario zou als vervolg op deze datacenterstrategie kunnen volgen.

ORGANISATIECOMPLEXITEIT

De mate waarin de variant aansluit bij bestaande structuren, processen en de benodigde personele inzet. In hoeverre is de variant organisatorisch in te bedden? Dit betreft governance-complexiteit, aantal betrokken partijen, behoefte aan nieuwe structuren. Een variant die erg complex is (zoals hybride multi-cloud) scoort hier negatief, terwijl een eenduidig model (één beheerpartij) positief scoort.

DUURZAAMHEID

Relatieve impact op de ecologische voetafdruk (het milieu, energieverbruik, CO_2-uitstoot en gebruik van hernieuwbare bronnen). Hierbij spelen de volgende factoren: energie-efficiëntie (PUE), mogelijkheid tot gebruik van duurzame energie, CO2-uitstoot door transport van data of hardware, e-waste (levensduur apparatuur) en impact op lokale ecologie. Een groene variant (bijv. gebruikmakend van zeer efficiënte datacenters of lokale zonne-energie) scoort goed, een variant die tot veel dieselverbruik en koelingsproblemen leidt scoort slecht.

GOVERNANCE EN REGIE

Sluit aan bij organisatie, maar meer specifiek of de overheid voldoende regiemogelijkheid heeft en de variant past binnen bestuurlijke kaders. Varianten met veel afhankelijkheid van derden of buitenlands recht scoren laag; varianten met duidelijke centrale sturing vanuit de gezamenlijke overheden, met respect voor taak- en verantwoordelijkheidsverdelingen, scoren hoog.

RISICO'S

Beoordeling van de mate van risico's op verschillende terreinen: continuïteitsrisico (downtime, disaster recovery), securityrisico (kans op datalek/hack), afhankelijkheidsrisico (vendor lock-in, monopolie). Hoe groter/gevarieerder de risico's, hoe lager de score. Ingeschatte beheersbaarheid van die risico's telt mee.

FLEXIBILITEIT
Het vermogen van de oplossing om mee te groeien of zich aan te passen aan verandering. Een rigide variant (bijv. eentje die vastzit aan één technologie of niet makkelijk op te schalen is) scoort negatief. Een modulair, uitbreidbaar model scoort positief.

ONTZORGING (BEHEERLAST)
Hoeveel interne beheerlast blijft er bij de overheid? Een variant die de overheid volledig ontzorgt (outsourcing, SaaS) scoort hoog, een variant die intensief lokaal beheer vergt scoort laag. Echter "ontzorging" moet in balans met controle – maar dat zit al in governance criteria. Hier puur: operationele last.

ARBEID/CAPACITEIT
Dit criterium kijkt naar de personele implicaties. Enerzijds: hoeveel (kwalificeerde) FTE's zijn nodig en zijn die beschikbaar? Anderzijds: biedt het variant mogelijkheden voor lokale werkgelegenheid of juist niet? Een variant die 24/7 hooggekwalificeerd personeel ter plekke zou vergen (wat er nauwelijks is) scoort slecht. Een variant die juist lokaal personeel ontwikkelt in behapbare mate scoort beter.

CONTRACTEN
Hierbij gaat het om de juridische haalbaarheid en complexiteit van contracten. Bijvoorbeeld: moet er Europees aanbesteed worden en is dat ingewikkeld? Zijn er juridische onzekerheden (zoals data-soevereiniteit, contractduur) die de variant minder aantrekkelijk maken? Eenvoudige contractuele invulling (bv. interne samenwerking) scoort hoger dan een variant die een woud aan contracten en SLA's met verschillende partijen vereist.

PRESTATIE (KWALITEIT VOOR GEBRUIKERS)
Dit omvat technische prestaties (latency, throughput) en kwaliteit van dienstverlening (uptime, responstijden) zoals de eindgebruiker die merkt. Een variant die de hoogste snelheid en betrouwbaarheid voor eindgebruikers oplevert scoort maximaal. Varianten waar gebruikers hinder (latency, vaak storingen) van ondervinden scoren laag.

SCHAALBAARHEID
Het vermogen om op te schalen voor groei in vraag of technologische ontwikkelingen. Een variant die future-proof is (met gemak meer workloads of integratie nieuwe technologie aankan) scoort hoog. Een variant op maat van nu, maar niet voor later, scoort laag. Dit is verwant aan flexibiliteit maar doelt meer op kwantitatieve groei dan op aanpassingsvermogen.

SOCIAAL-MAATSCHAPPELIJK
Hier kijken we naar de effecten op de lokale maatschappij en economie. Draagt de variant bij aan lokale ontwikkeling (ICT-kennis, banen, toeleveranciers)? Versterkt het de autonomie van de eilanden of juist niet? Een variant die naast technisch succes ook sociaal gewenst is (bijv. werkgelegenheid, empowerment) scoort positief. Eén die alles buiten de eilanden plaatst scoort negatief. Er is een sterke relatie met het criteria arbeid/capaciteit.

CONTINUÏTEIT (<24U UITVAL)
Hoewel continuïteit al in risico's en prestatie zit, willen we dit expliciet als criterium hanteren omdat het een belangrijke eis is. Hier scoren we of de variant in staat is uitval te beperken tot minder dan 24 uur bij zware calamiteiten. Varianten zoals met twee of meer locaties scoren hier hoog, single points of failure scoren laag.

In de tabelbeoordeling (Tabel 3) is indicatief met plussen en minnen aangegeven hoe de resterende varianten (variant 1 (lokale DC's per eiland), 2 (Twin DC In CN: Bonaire Sint Eustatius of Saba) en 10 (Twin datacenter: Caribisch Nederland en Europees Nederland)) scoort per criterium, zonder exacte weegfactoren maar met een kwalitatieve inschatting. De toetsing van de overige varianten is volledigheidshalve opgenomen in bijlage D

	Kosten	Organisatie	Duurzaam	Governance	Risico's	Flexibel	Ontzorging	Arbeid	Contracten	Prestatie	Schaal	Sociaal	Continuïteit
1. Lokale DC's per eiland	--	--	--	--	-	-	--	--	--	++	--	+	++
2. Twin DC CN	-	≈	-	≈	+	≈	≈	+	≈	+	≈	++	+
10. Twin-datacenter CN / E-NL	+	++	++	++	--	++	-	+	+	≈	+	+	+

(Tabel 3: Beoordeling van de drie resterende varianten op criteria – legenda: "++" zeer positief, "+" positief, "≈" neutraal/gemiddeld, "–" negatief, "– –" zeer negatief.)

9.2 Vergelijking resterende varianten

Deze paragraaf bevat de beoordeling van de varianten aan de hand van de vastgestelde criteria. Per criteriumgroep is op hoofdlijnen aangegeven hoe de varianten zich tot elkaar verhouden. Deze kwalitatieve beoordeling maakt inzichtelijk waar de kracht of zwakte van een variant ligt en vormt de basis voor de strategische afweging.

KOSTEN

- **Variant 1** vereist drie zelfstandige datacenters, wat leidt tot hoge bouw-, beheer- en onderhoudskosten. Er is geen schaalvoordeel en efficiency is laag.
- **Variant 2** is kostbaar in aanleg vanwege twee volwaardige dc-locaties (Bonaire en Sint Eustatius of Saba), maar heeft minder structurele kosten dan drie afzonderlijke datacenters. Om de kosten te drukken kan voor op Bonaire in eerste instantie worden gekozen om de twee bestaande datacenters daar als één stretched datacenter in te richten.
- **Variant 10** neemt capaciteit af in bestaande overheidsdatacenters (ODC) in Europees Nederland en vereist slechts een fallbacklocatie op Bonaire, wat zorgt voor lagere TCO en betere kostenefficiëntie

ORGANISATIE & GOVERNANCE

- **Variant 1** vraagt van ieder OL dat zij zelfstandig een IT-organisatie opzet, waar het Rijk mogelijk ook gebruik van kan maken, wat organisatorisch zeer zwaar is. Of centrale aansturing en dienstverlening vanuit bijvoorbeeld SSO-CN is mogelijk.
- **Variant 2** brengt samenwerking tussen eilanden met zich mee, waardoor enige centrale ondersteuning mogelijk is. De organisatorische druk per eiland daalt. Saba en Sint Eustatius werken samen om het datacenter op de bovenwindse eilanden te operationaliseren.
- **Variant 10** maakt optimaal gebruik van centrale sturing en ondersteuning via het Rijk, door zich volledig te committeren aan de architectuur welke al in E-NL is toegepast. Overigens is dit een organisatorische inrichting waar ook in scenario 1 en 2 voor kan worden gekozen.

RISICO'S (CONTINUÏTEIT/SECURITY)

- **Variant 1** biedt per eiland lokale autonomie, maar is kwetsbaar voor fysieke verstoringen (storm, brand) zonder redundantie.
- **Variant 2** biedt enige failover binnen CN zelf, maar is kwetsbaar bij verbindingsproblemen tussen eilanden, met name tussen Saba en Sint Eustatius.
- **Variant 10** kent risico's bij verbindingsuitval, maar deze zijn grotendeels te mitigeren met fallbackmaatregelen op CN. Deze variant is kwetsbaar door fysieke afstanden en onderzeese kabels. Daarnaast is dit scenario zeer risicovol voor Saba en Sint Eustatius.

PRESTATIE (LATENCY/GEBRUIKERSERVARING)

- **Variant 1** scoort goed op lokale prestaties door directe fysieke nabijheid van systemen.
- **Variant 2** heeft goede prestaties mits de verbindingen binnen CN stabiel zijn.
- **Variant 10** heeft vergelijkbare prestaties, prestatie op de eilanden is afhankelijk van verbinding en buffering. Dit geldt met name voor Saba en Sint Eustatius.

FLEXIBILITEIT & SCHAALBAARHEID
- **Variant 1** is lokaal flexibel, maar beperkt schaalbaar en weinig toekomstbestendig, omdat elke uitbreiding een nieuwe lokale voorziening vergt.
- **Variant 2** biedt meer flexibiliteit binnen CN, maar blijft technisch begrensd. Deze variant is niet eenvoudig op te schalen in capaciteit of in type dienstverlening.
- **Variant 10** is zeer flexibel dankzij integratie met overheidsvoorzieningen, schaalbaarheid en aansluiting op landelijke ontwikkelingen.

ONTZORGING (BEHEERLAST)
- **Variant 1** vraagt maximale inzet van lokale organisaties, die alles zelf moeten regelen.
- **Variant 2** kan deels worden ondersteund via samenwerking en centrale backoffice, maar blijft deels lokaal afhankelijk. Eventueel opzetten van centrale platforms vanuit EN in CN.
- **Variant 10** biedt ontzorging door gebruik van centrale platforms (ODC Noord, Logius, DICTU), de mogelijkheid om terug te vallen op kennis, ervaring en ondersteuning vanuit EN en de standaardinrichting conform architectuur uit EN. Met lokale ondersteuning door bijvoorbeeld SSO-CN.

ARBEID/CAPACITEIT (BESCHIKBAARHEID SKILLS, LOKALE WERKGELEGENHEID)
- **Variant 1** vereist eigen technisch personeel op elk eiland, wat vrijwel onhaalbaar is gezien de arbeidsmarkt.
- **Variant 2** verdeelt arbeid over twee locaties, wat haalbaarder is maar nog steeds uitdagend.
- **Variant 10** legt technische taken bij centrale organisaties, en beperkt lokale inzet. Ondersteuning vanuit EN is actief.

CONTRACTEN/JURIDISCH
- **Variant 1** betekent per eiland aparte leveranciers en contracten – inefficiënt en foutgevoelig.
- **Variant 2** maakt gezamenlijke contracten mogelijk, mits governance op orde is.
- **Variant 10** eenvoudiger gebruik van bestaande overheidscontracten, met centrale SLA's en gestandaardiseerde afspraken.

SOCIAAL-MAATSCHAPPELIJK
- **Variant 1** sluit goed aan bij het gevoel van autonomie op de eilanden.
- **Variant 2** biedt een gedeeld gevoel van eigenaarschap binnen CN en versterkt samenwerking.
- **Variant 10** vereist vertrouwen in centrale sturing, maar sluit aan bij het werken als één overheid (NDS).

<24 UUR UITVAL (CONTINUÏTEITCRITERIUM)
- **Variant 1** garandeert lokale beschikbaarheid bij verbindingstoring, maar heeft geen uitwijk bij lokale rampen.
- **Variant 2** biedt betere continuïteit door failover tussen twee eilanden.
- **Variant 10** levert solide continuïteit mits fallback op CN is ingericht, en biedt uitwijk bij grootschalige verstoringen, met uitzondering voor de eilanden Saba en Sint Eustatius.

9.3 Resultaten en conclusie van de weging

Op basis van de inhoudelijke analyse, de strategische uitgangspunten en de kwalitatieve beoordeling van de drie resterende scenario's, valt **scenario 1** (lokale datacenters op Bonaire, Saba en Sint Eustatius) af als realistische optie voor de datacenterstrategie van Caribisch Nederland. De hoge kosten, lage schaalbaarheid, beperkte duurzaamheid, versnipperde governance en afhankelijkheid van schaarse lokale capaciteit maken deze variant kwetsbaar en niet toekomstbestendig. Hoewel dit scenario op het eerste gezicht aansluit bij het streven naar lokale autonomie en directe controle, weegt dit onvoldoende op tegen de nadelen en risico's. De fragmentatie en het ontbreken van coördinatie zijn fundamenteel in strijd met de richting die de Rijksoverheid en lokale stakeholders willen inslaan, namelijk: meer samenwerking, meer continuïteit en meer integratie met overheidsbrede digitale voorzieningen (NDS).

De strategie kiest voor een combinatie van scenario 2 en scenario 10, omdat deze samen de meest toekomstbestendige en veerkrachtige oplossing bieden. Scenario 2, een twin-datacenteropzet binnen Caribisch Nederland, kan op korte termijn worden gerealiseerd. De huidige datacenters op Bonaire (SSO-CN en Flamingo TV) functioneren al als twin-datacenter en kunnen verder worden ingericht als één stretched omgeving met logische redundantie, totdat een nieuwe locatie met meer capaciteit is gerealiseerd. Op termijn wordt Sint Eustatius of Saba de tweede twin-locatie naast Bonaire. Voor die tussenfase kan gebruik worden gemaakt van tijdelijke orkaanbestendige datacentercontainers op een beveiligde locatie, of een bestaand of nieuw gebouw. Dit vraagt om nauwe afstemming met lokale stakeholders en een gezamenlijke aanpak met duidelijke rolverdeling.

Tegelijkertijd wordt toegewerkt naar scenario 10: de koppeling van de Caribische datacenters aan een overheidsdatacenter (ODC) in Europees Nederland. Daarmee ontstaat een robuust model met failover en fallback over meerdere geografische zones, versterkt door centrale monitoring, security en compliance. Deze combinatie van scenario 2 (regionale redundantie binnen CN) en scenario 10 (uitwijk en ondersteuning vanuit EN) realiseert: lokale beschikbaarheid en veerkracht, gekoppeld aan centrale schaalvoordelen, strategische continuïteit en geopolitieke zekerheid.

De gekozen koers maakt het ook mogelijk om wederzijds voordeel te realiseren: Caribisch Nederland profiteert van centrale ondersteuning, terwijl Europees Nederland back-ups en uitwijk kan onderbrengen in CN. Dit vergroot de spreiding van dataopslag binnen het Nederlandse rechtsstelsel, wat van belang is in het licht van geopolitieke risico's.

Om deze gecombineerde strategie te laten slagen, moeten nu besluiten worden genomen over governance, financiering en connectiviteit. Deze afspraken moeten worden vastgelegd in heldere kaders en dienstverleningsovereenkomsten, zodat de belangen van zowel alle betrokken overheden geborgd zijn. Zo kan snel worden gestart met een realistische opzet (scenario 2) die doorontwikkelt naar een toekomstvaste structuur (scenario 2+10), waar zowel Caribisch als Europees Nederland bij gebaat is.
.

10 SAMENWERKINGSMOGELIJKHEDEN EN GOVERNANCE

Een goed besturingsmodel is voorwaardelijk voor de invoering van de gekozen variant. Dit hoofdstuk geeft antwoord op onderzoeksvraag 9: "Wat zijn de samenwerkings- en governancemogelijkheden tussen rijk, lokale overheden en uitvoeringsorganisaties?". Het hoofdstuk beschrijft hiertoe een passend governancemodel en de samenwerkingsopties die de datacenterstrategie moeten ondersteunen. Daarbij worden suggesties gedaan om rollen en verantwoordelijkheden van betrokken partijen nader uit te werken, waaronder de Rijksoverheid, de openbare lichamen, uitvoeringsorganisaties en marktpartijen. Er wordt specifiek aandacht besteed aan het behouden van flexibiliteit om in te kunnen spelen op toekomstige ontwikkelingen en behoeften. Het Nederlandse bestuurlijke afsprakenstelsel en het Huis van Thorbecke vormen het uitgangspunt voor een bestuurlijke inbedding die aansluit bij bestaande interbestuurlijke voorzieningen. Daarnaast wordt gekeken naar de rol die partijen als ODC-Noord, SSC-ICT, Rijkswaterstaat, Logius, DICTU, SSO-CN en mogelijk Defensie kunnen vervullen. Tot slot komen de juridische kaders en de impact op marktwerking binnen Caribisch Nederland aan bod.

10.1 Governance-model: centraal kader, lokale inbreng

Gezien de beperkte schaal van Caribisch Nederland en de technisch complexe aard van datacenterbeheer, ligt het voor de hand dat de centrale overheid, en in het bijzonder het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), de hoofdverantwoordelijkheid op zich neemt voor de inrichting en regie van de datacenterstrategie. Het is aan te bevelen dat BZK, via de directies Digitalisering en Koninkrijksrelaties – optreedt als opdrachtgever en regievoerder voor de ontwikkeling en realisatie van de datacenterstrategie. Deze rol sluit aan bij de bestaande verantwoordelijkheid van BZK voor zowel digitalisering als de Koninkrijksrelaties. Rapportagelijnen dienen te lopen naar de staatssecretaris van Digitalisering, die tevens Koninkrijksrelaties in portefeuille heeft, om bestuurlijke sturing en politieke verankering te waarborgen.

Het wordt aanbevolen om op strategisch niveau een interbestuurlijke sturingsgroep in te richten die fungeert als besluitvormend orgaan en zorg draagt voor voldoende bestuurlijk draagvlak. De samenstelling van deze groep, bij voorkeur met vertegenwoordigers van de relevante overheden en organisaties, vraagt om een nadere uitwerking in een vervolgtraject. Hierbij kan bijvoorbeeld gedacht worden aan de volgende samenstelling:

- BZK (voorzitter, opdrachtgever),
- De departementen (nader vast te stellen) met een direct belang,
- De openbare lichamen van Bonaire, Saba en Sint Eustatius (bij voorkeur de eilandsecretaris of directeuren bedrijfsvoering/ICT),
- Rijksdienst Caribisch Nederland (RCN), vertegenwoordigd door het hoofd van CIO-RCN,
- Een vertegenwoordiger van een centrale uitvoeringsorganisatie met operationele belangen in Caribisch Nederland.

Deze interbestuurlijke opzet sluit aan bij het Huis van Thorbecke en het Nederlandse afsprakenstelsel, waarin centrale en decentrale overheden gezamenlijk besluiten nemen binnen duidelijk vastgelegde kaders. Het verdient aanbeveling om de samenwerking te formaliseren in een ministeriele regeling (zoals het Besluit Sturing Digitale Overheid) of convenant, waarin verantwoordelijkheden, rolverdeling en financiering expliciet zijn vastgelegd.

Geadviseerd wordt om onder de sturingsgroep een projectorganisatie in te richten die verantwoordelijk is voor de uitvoering. Deze organisatie moet bestaan uit specialisten van operationele partijen zoals SSO-CN, SSC-ICT, ODC-Noord, Logius en DICTU, aangevuld met externe deskundigen en projectleiders voor domeinen als gebouwinrichting, IT-infrastructuur en migratie. Om de kwaliteit van dienstverlening structureel te borgen, verdient het aanbeveling om deze tijdelijke projectstructuur na de implementatie door te ontwikkelen tot een permanente beheer- en governance-organisatie. Daarbij is het cruciaal dat hier een duidelijke resultaatverplichting aan wordt gekoppeld, aangezien praktijkervaring laat zien dat kennisuitwisseling weliswaar mogelijk is, maar inzet van daadwerkelijke exploitatiecapaciteit vanuit ODC's in de praktijk vaak geen

prioriteit krijgt. Dit vereist dat de directeuren van de ODC's CN expliciet meenemen in hun rapportages en hierop sturen via concrete KPI's.

10.2 Inrichting beheerorganisatie

Op basis van gesprekken met stakeholders en het werkbezoek van Highberg aan Caribisch Nederland (CN) luidt het advies om SSO-CN te positioneren als beheerorganisatie voor het operationeel beheer van de datacenterlocaties in CN. Dit in nauwe samenwerking met een Nederlandse partner zoals SSC-ICT, Logius, Dictu en ODC-Noord. Deze inrichting maakt het mogelijk om lokaal het dagelijks beheer uit te voeren en een breder dienstenportfolio aan te bieden terwijl tegelijkertijd de tweede- en derdelijns ondersteuning wordt geborgd via de expertise, capaciteit en continuïteit van Europees Nederland.
Het is aan te bevelen om hierbij centrale ondersteuning te organiseren op het gebied van monitoring, incidentrespons en beveiliging via het Security Operations Center (SOC) van de Rijksoverheid. Daarnaast moeten beheertooling, logging, updates en back-upvoorzieningen worden afgestemd op de overheidsbrede infrastructuur, zodat bij calamiteiten snelle overdracht van beheer en fallback naar Europees Nederland mogelijk is.
Deze aanpak zorgt ervoor dat CN structureel onderdeel uitmaakt van de digitale rijksinfrastructuur en profiteert van schaalvoordelen en stabiliteit, zonder dat dit ten koste gaat van de lokale regie. De Openbare Lichamen behouden de zeggenschap over uitvoering en prioritering, terwijl het Rijk de randvoorwaarden voor robuuste dienstverlening garandeert.

10.3 Service Level agreements en Dossier Afspraken & Procedures (DAP)

Voor een betrouwbare en voorspelbare dienstverlening is het noodzakelijk om een set concrete Service Level Agreements (SLA's) vast te stellen. Enerzijds tussen diensten onderling en anderzijds naar gebruikers (stakeholders) van deze diensten door het SSO-CN. Denk aan eisen zoals 99,9% beschikbaarheid voor kritieke systemen, herstel binnen 24 uur bij calamiteiten en vastgelegde responstijden voor helpdesktickets.

Deze SLA's dienen bindend te zijn en moeten actief worden gemonitord door de regieorganisatie. Wanneer marktpartijen worden ingeschakeld voor dienstverlening, moeten zij contractueel worden verplicht tot naleving van gelijkwaardige servicelevels. Afwijkingen hierop zijn niet acceptabel gezien het belang van continuïteit, betrouwbaarheid en gelijke behandeling binnen de overheidsbrede infrastructuur.

Een DAP (Dossier Afspraken en Procedures) is een aanvulling op een SLA. Het legt vast hoe afspraken operationeel worden uitgevoerd, inclusief werkprocessen, escalaties, contactpunten en rapportage. Waar SLA "wat" bepaalt, beschrijft het DAP concreet "hoe".

10.4 Compliancy en auditing

Steeds meer wet- en regelgeving, zoals de Wet digitale overheid (Wdo) en de Gezamenlijke Elektronische Voorzieningen SUWI voor Suwinet stellen eisen aan compliancy en auditing van de overheidsdienstverlener. De overheidsdienstverlener zal veelal de IT-dienstverlening uitbesteed hebben aan een serviceorganisatie of datacenter. Bij de verplichte DigiD en Suwinet-audits van overheidsdienstverleners die DigiD gebruiken, kan de Register EDP-auditor (RE) van de overheidsdienstverlener steunen op uitgevoerde audits door een RE bij de serviceorganisatie/datacenter waar de overheidsdienstverleners aan uitbesteed is. Dit houdt in dat systemen of diensten die door serviceorganisaties worden beheerd (zoals cloudproviders of datacenters) niet rechtstreeks binnen de scope van de audit van de overheidsdienstverlener vallen. In plaats daarvan zal het vertrouwen in de serviceorganisatie/datacenter worden gebaseerd op het rapport van de DigiD audit die door een RE van de serviceorganisatie is uitgevoerd. Dit wordt ook wel een Third Party Memorandum (TPM) genoemd. In auditjargon wordt dit de 'carve-out methode' genoemd. Bij de verdere inrichting van de datacenterfaciliteiten in Caraïbisch Nederland is het aan te bevelen om de management- en beheerprocessen zo in te richten dat daar door een RE een 'TPM' over afgeven kan worden aan overheidsdienstverleners en toezichthouders die daar om vragen.

10.5 Organisatorische inbedding

Voor de organisatorische inbedding van de datacenterfaciliteiten in Caraïbisch Nederland zijn twee modellen denkbaar, elk met duidelijke voor- en nadelen.

De eerste mogelijkheid is om de faciliteiten onder te brengen bij een bestaande rijksdienst, zoals ODC-Noord, DICTU of SSC-ICT. Dit model sluit aan op bestaande juridische structuren binnen het Rijk en maakt het, afhankelijk van wie als opdrachtgever optreedt, mogelijk om werkzaamheden via inbesteding te laten verlopen conform de Aanbestedingswet. Deze route is juridisch houdbaar zolang de opdrachtgever een rijksdienst is. Zodra echter ook ZBO's of openbare lichamen (OL'en) gebruik willen maken van de dienstverlening, vereist dit nadere juridische borging, bijvoorbeeld via aanvullende afspraken of separate contractstructuren.

Een bijkomend voordeel van dit model is de mogelijkheid om personeel flexibel in te zetten via detachering of samenwerking met SSO-CN, met behoud van aansluiting op overheidsstandaarden. Tegelijkertijd kent deze variant ook een duidelijk risico: de aansturing ligt in Europees Nederland, wat kan betekenen dat Caribisch Nederland in de praktijk onvoldoende prioriteit krijgt binnen bredere Rijksprogramma's.

Een tweede optie is het opzetten van een nieuwe shared service-constructie onder gezamenlijke aansturing van BZK en de openbare lichamen. Dit vergroot de lokale betrokkenheid en biedt ruimte voor meer maatwerk, afgestemd op de specifieke behoeften van CN. Daar staat tegenover dat dit model organisatorisch zwaarder is en meer tijd en afstemming vraagt voor inrichting, aansturing en organisatorische borging.

Gezien de bestaande structuren binnen RCN en de rol van SSO-CN ligt het voor de hand om voort te bouwen op wat er al staat, en te kiezen voor een model waarbij SSO-CN als centrale beheerorganisatie fungeert binnen een bredere landelijke regiestructuur.

Welke organisatievorm ook wordt gekozen, essentieel is dat er één centrale beheerorganisatie verantwoordelijk is voor de volledige keten. Versnippering van verantwoordelijkheden over meerdere Openbare Lichamen of instanties moet worden voorkomen. SSO-CN kan hierin het lokale ankerpunt vormen. Wel moet bij de uiteindelijke inrichting nadrukkelijk worden geborgd dat alle betrokken partijen – rijksdiensten, ZBO's en OL'en – juridisch rechtmatig gebruik kunnen maken van de diensten van deze beheerorganisatie. Dit vereist óf een juridische structuur die aan de voorwaarden voor inbesteding voldoet, óf alternatieve contractuele afspraken die aanbestedingsrisico's uitsluiten.

10.6 Rollen van uitvoeringsorganisaties en departementen

Voor een succesvolle uitvoering van de datacenterstrategie is nauwe afstemming met rijksdiensten en betrokken uitvoeringsorganisaties en openbare lichamen belangrijk. Deze partijen zijn niet alleen eindgebruikers van de infrastructuur, maar spelen ook een rol in de vormgeving, implementatie en het beheer van de toekomstige voorzieningen. De onderstaande aanbevelingen beschrijven hoe deze samenwerking kan worden ingericht, geborgd en juridisch vormgegeven binnen het bestaande rijksdomein.

RIJKSORGANISATIES

Rijksorganisaties zoals de Belastingdienst, IND, OM en Politie zijn belangrijke eindgebruikers van de digitale infrastructuur in Caribisch Nederland. Het is aan te bevelen om deze partijen structureel te betrekken bij de verdere ontwikkeling en exploitatie van de datacenterstrategie, met name in de fase van eisenstelling en kwaliteitsborging. Het continueren en formaliseren van de gebruikersraad in CN wordt sterk aanbevolen. Deze raad bestaat uit lokale vertegenwoordigers van de voornaamste gebruikersorganisaties op de BES-eilanden, zoals CIO's of IT-coördinatoren. De gebruikersraad krijgt een structurele rol binnen de governance van de regieorganisatie onder BZK en vertegenwoordigt de belangen van de eindgebruikers. Zij signaleert actief operationele behoeften, schaalvragen en knelpunten, en levert input bij besluitvorming over infrastructuurontwikkeling. Zo wordt gewaarborgd dat de digitale infrastructuur blijvend aansluit op de praktijk en het gebruik in Caribisch Nederland.

UITVOERINGSORGANISATIES

Highberg adviseert om uitvoeringsorganisaties in de voorgestelde inrichting verantwoordelijk te laten blijven voor hun eigen applicatiebeheer, zodat geen extra coördinatielasten ontstaan. Zij nemen af op basis van de nieuwe infrastructuur, onder de voorwaarden zoals vastgelegd in de overeengekomen SLA's. Bestaande

voorzieningen, zoals eigen serverruimtes, kunnen waar nodig worden geïntegreerd in de centrale oplossing, mits dit past binnen de architectuur en beheersafspraken .

LOGIUS EN DICTU

Voor Logius en Dictu geldt dat betrokkenheid bij het ontwerp en de implementatie van de infrastructuur noodzakelijk is om aansluiting op generieke platformen en landelijke diensten zoals DigiD, MijnOverheid en DigiNetwerk mogelijk te maken. In de toekomstige inrichting dient verkeer vanuit CN naar Logius via beveiligde koppelingen te verlopen. Een technisch en organisatorisch koppelvlak kan worden ingericht in het datacenter op Bonaire of via een locatie in Europees Nederland. Het is aan te bevelen Logius en Dictu daarom in te passen in de governance en een adviserend en faciliterend aandeel te geven in de aansluiting van CN op de generieke voorzieningen.

RIJKSVASTGOEDBEDRIJF

Rijksvastgoedbedrijf (RVB) kan op twee manieren bijdragen. Enerzijds als adviseur bij het ontwerp van de fysieke datacenterinfrastructuur, waarbij ervaring met noodstroomvoorziening, gebouwveiligheid en robuustheid van toegevoegde waarde is. Anderzijds kan RVB worden betrokken als "klant" van het datacenter. Uit interviews blijkt dat het RVB structureel performance uitdagingen heeft bij het aanbieden van haar centrale ICT-diensten in het Caribisch gebied. Betrokkenheid van RVB wordt vooral aanbevolen in de rol van technisch specialist in de stuurgroep of projectstructuur.

SSC-ICT

SSC-ICT is een logische partij voor het leveren van beheer- en hostingdiensten ten aanzien van de digitale werkplek (DWR) binnen deze strategie. Het wordt aanbevolen om SSC-ICT verantwoordelijk te maken voor de tweede- en derdelijns ondersteuning van CN. In samenwerking met SSO-CN ontstaat een geïntegreerd beheermodel met gedeelde operationele processen en ketenverantwoordelijkheid. SSC-ICT beheert reeds IT-diensten voor meerdere ministeries en beschikt over de schaal en professionaliteit om dienstverlening richting CN te borgen. Prioriteitsstelling voor BES-organisaties dient te worden vastgelegd in een Dienstverleningsovereenkomst (DVO), onder sturing van BZK. Deze constructie blijft volledig binnen het overheidsdomein en valt onder inbesteding conform de Aanbestedingswet.

ODC-NOORD

ODC-Noord biedt een passende locatie voor een extra back-upcomponent binnen de twin-datacenterarchitectuur voor Caribisch Nederland. Het datacenter voldoet aan de vereiste overheidsnormen voor veiligheid, beschikbaarheid en schaalbaarheid en beschikt over voldoende fysieke capaciteit om uitbreiding te faciliteren. Door in ODC-Noord specifiek een eigen fysieke ruimte, bijvoorbeeld een afgesloten rack of cage, toe te wijzen voor Caribisch Nederland, kan een betrouwbare en structureel beheerde uitwijklocatie worden ingericht. Deze opzet creëert niet alleen een veilige uitwijkmogelijkheid vanuit de BES-eilanden richting Europees Nederland, (variant 10) maar maakt ook het omgekeerde mogelijk: het veiligstellen van data vanuit Europees Nederland in Caribisch Nederland, wat de wederzijdse veerkracht van de digitale infrastructuur versterkt.

Om deze samenwerking structureel te verankeren, wordt geadviseerd een dienstverleningsovereenkomst (DVO) te sluiten tussen BZK en DUO/OCW. Hierin moeten onder meer afspraken worden gemaakt over verantwoordelijkheden, serviceniveaus en escalatieprocedures. Een belangrijk aandachtspunt daarbij is de operationele prioritering: het is cruciaal de aan Caribisch Nederland gekoppelde systemen als vitaal worden aanmerkt, zodat bij storingen of calamiteiten wordt opgetreden volgens vooraf afgesproken responstijden en actielijnen. Alleen dan kan de twin-opzet daadwerkelijk de beoogde continuïteit en betrouwbaarheid leveren.

MINISTERIE VAN DEFENSIE

Betrokkenheid van het Ministerie van Defensie is op dit moment niet structureel voorzien. Toch wordt aanbevolen om in de uitwerkingsfase na te gaan of specifieke Defensielocaties of -voorzieningen kunnen worden benut, bijvoorbeeld bij beveiliging of fysieke huisvesting. Indien beschikbaar en geschikt kan een datacenterlocatie op of nabij een defensieterrein overwogen worden, mits afspraken worden vastgelegd in een interdepartementale overeenkomst. Defensie zou in dit geval geen uitvoerende partij worden, maar eerder een partner voor gedeeld gebruik van infrastructuur of beveiligingsmaatregelen.

BESTUURLIJKE AFSPRAKEN EN BORGING

Het is essentieel dat de samenwerking binnen het Rijk zorgvuldig juridisch wordt vormgegeven en geborgd. Het verdient aanbeveling om de rollen van BZK, SSO-CN, SSC-ICT, Logius, DICTU en RVB expliciet vast te leggen in een bestuurlijk akkoord en bijbehorende DVO's, met duidelijke afspraken over verantwoordelijkheid, dienstverlening, prioriteitstelling en rapportage. Dit waarborgt een stabiele, bestuurlijk gedragen en uitvoerbare inrichting van de datacenterstrategie voor Caribisch Nederland.

10.7 Betrokkenheid van marktpartijen en aanbestedingsaspecten

Het wordt geadviseerd om bij de inrichting en exploitatie van de datacenterfaciliteiten zoveel mogelijk gebruik te maken van bestaande interne rijksdiensten. Dit bevordert standaardisatie, borgt aansluiting op overheidsbrede voorzieningen en vereenvoudigt governance. Tegelijkertijd is inzet van marktpartijen op specifieke onderdelen noodzakelijk.
Voor de bouw van een nieuw datacentergebouw op Bonaire en de levering en installatie van hardware zoals servers, opslag en netwerkcomponenten, is inschakeling van externe leveranciers onvermijdelijk. Afnemers van datacenterdiensten moeten daarnaast de mogelijkheid behouden om het technisch beheer zelfstandig uit te voeren of hiervoor een derde partij te contracteren, binnen de geldende kaders voor beveiliging en regie.
De uitvoering van de bijbehorende inkooptrajecten ligt bij de Rijksdienst Caribisch Nederland (RCN), die daarbij de geldende inkoopregels toepast. Hoewel de Europese aanbestedingsrichtlijn formeel niet van toepassing is op Caribisch Nederland, wordt geadviseerd om de algemene aanbestedingsbeginselen, transparantie, gelijke behandeling en proportionaliteit, structureel toe te passen om zorgvuldigheid en rechtmatigheid te waarborgen.

IMPACT LOKALE ICT-MARKT

In een vervolgtraject is het noodzakelijk de positie van marktpartijen ten opzichte van de voorgenomen datacenteropzet helder uit te werken. Caribisch Nederland kent een kleinschalige ICT-markt met beperkte commerciële activiteit; momenteel is alleen Flamingo TV op Bonaire als commercieel datacenter actief, naast de faciliteiten van SSO-CN.

Een beproefd model, zoals in Europees Nederland, is het aanbesteden van een long lease-constructie waarbij een marktpartij eigenaar en exploitant van het datacenter is. De overheid huurt op lange termijn de benodigde capaciteit, terwijl de exploitant tegelijkertijd diensten kan leveren aan private partijen. Dit model versterkt de marktwerking, biedt schaalvoordelen en voorkomt dat de overheid zelf de volledige juridische en operationele complexiteit van exploitatie hoeft te dragen.

De introductie van zo'n voorziening heeft directe gevolgen voor de lokale markt. Het is daarom belangrijk de markteffecten zorgvuldig te beoordelen en een balans te vinden tussen publieke regie en ruimte voor commerciële dienstverlening. Tegelijkertijd biedt dit kansen voor versterking van de digitale kerninfrastructuur, bijvoorbeeld door co-locatie te faciliteren voor telecom- en IT-dienstverleners of door het opzetten van een regionale Internet Exchange (CN-IX) op Bonaire en mogelijk Sint Eustatius en Saba. Dit kan leiden tot betere prestaties, lagere kosten en meer concurrentie.

Juridische borging blijft nodig, maar wordt eenvoudiger wanneer de overheid uitsluitend capaciteit afneemt en de exploitatie bij de markt ligt. Daarbij moeten transparantie, kostendekkendheid en non-discriminatie worden geborgd om risico's op ongeoorloofde staatssteun te vermijden. In het vervolgtraject is afstemming met juridische experts nodig om de gekozen constructie duurzaam en rechtmatig te verankeren, met een heldere rolverdeling tussen overheid en markt.

UITBESTEDEN BEHEER

Als op termijn blijkt dat de beheercapaciteit binnen de overheid onvoldoende is, als zich een gekwalificeerde private aanbieder aandient of een instantie zelf het beheer wil uitvoeren of beleggen bij een derde, blijft het mogelijk een deel van het beheer uit te besteden. In dat geval moet een aanbestedingsprocedure worden gevolgd om alle geïnteresseerde marktpartijen een gelijke kans te geven. Voor de korte termijn verdient het echter de voorkeur om de exploitatie onder te brengen bij bestaande rijksdiensten, gelet op eisen rondom soevereiniteit, controle en beveiliging.

Voor alle externe inkooptrajecten is het essentieel om contracten af te sluiten waarin prestatie-eisen, beveiligingsstandaarden en servicelevels expliciet zijn opgenomen. Indien bijvoorbeeld netwerkdiensten worden afgenomen van een lokale telecomaanbieder zoals Telbo, Satel of Eutel dienen in de contracten redundantie, beschikbaarheid en hersteltermijnen contractueel te zijn vastgelegd, inclusief sanctiebepalingen bij niet-naleving. Er kan tevens worden overwogen gebruik te maken van innovatieve contractvormen, zoals Design-Build-Finance-Maintain (DBFM) constructies, bijvoorbeeld voor de aanleg en het beheer van nieuwe zeekabels. Het ministerie van EZ zou hierin een rol kunnen spelen.

10.8 Flexibiliteit in samenwerking

Gezien de snelle technologische ontwikkelingen en de veranderende organisatorische context is het van belang dat het gekozen samenwerkingsmodel voldoende flexibiliteit bevat om toekomstbestendig te zijn. Deze flexibiliteit kan op verschillende manieren worden geborgd binnen de governance- en samenwerkingsstructuur.

PRIVATE PARTIJEN

Samenwerking met private partijen dient modulair en doelgericht te worden ingericht. Voor specifieke deelterreinen kan gekozen worden om concurrentie toe te laten, mits dit de kern van de infrastructuur niet ondermijnt. Zo kan bijvoorbeeld het energiebeheer van het datacenter via een separate overeenkomst worden ondergebracht bij een gespecialiseerde partij, zoals een Energy Service Company (ESCo) voor duurzame stroomvoorziening. Dergelijke innovatieve samenwerkingsvormen zijn mogelijk zonder afbreuk te doen aan de soevereiniteit en beveiliging van de data-infrastructuur. Het afsprakenkader moet expliciet ruimte bieden voor dergelijke constructies onder duidelijke randvoorwaarden.

NIEUWE STAKEHOLDERS

Het model moet tevens voorbereid zijn op de incrementele aansluiting van nieuwe stakeholders. In de toekomst kan het wenselijk of noodzakelijk zijn om andere rijksdiensten of zelfs andere Koninkrijksdelen – zoals Aruba of Curaçao, toegang te bieden tot de infrastructuur. Door de regie bij BZK te beleggen, ontstaat bestuurlijke ruimte om deze uitbreiding op termijn te faciliteren. Het afsprakenstelsel kan dan worden uitgebreid met nieuwe deelnemers, mits daarover wederzijdse overeenstemming bestaat. De structuur moet dit organisatorisch kunnen ondersteunen.

EXITSCENARIO'S

Daarnaast is het noodzakelijk om mogelijke exitscenario's te voorzien De governance moet zodanig worden ingericht dat een ordentelijke overdracht mogelijk is. Mocht bijvoorbeeld SSC-ICT op enig moment haar rol niet langer kunnen vervullen, dan moet een andere rijksdienst, zoals DICTU, de ondersteuning kunnen overnemen. De technische en organisatorische inrichting dient overdraagbaar te zijn, met volledige documentatie en brede kennisborging om afhankelijkheid van specifieke personen of partijen te minimaliseren. Als scenario kan worden overwogen om bepaalde taken uit te besteden aan de markt.

10.9 Conclusie

De uitvoering van de datacenterstrategie kan alleen verantwoord starten wanneer er een robuuste en bestuurlijk geborgde governance- en samenwerkingsstructuur is ingericht. BZK dient hierin de regierol te nemen, in nauwe samenwerking met de openbare lichamen en de relevante uitvoeringsorganisaties. Deze afspraken moeten worden vastgelegd in een bestuurlijk akkoord en vertaald in concrete dienstverleningsovereenkomsten, waarin verantwoordelijkheden, financiering, serviceniveaus en prioriteiten ondubbelzinnig zijn vastgelegd. Bestuurlijke vrijblijvendheid is hier geen optie: zonder heldere afspraken blijft de uitvoering kwetsbaar en onvoldoende verantwoord.

De governance moet bovendien stevig ingebed zijn in bestaande interbestuurlijke structuren en voldoen aan de spelregels van het openbaar bestuur. Dit voorkomt dat de datacenterstrategie los komt te staan van bredere overheidsontwikkelingen en versterkt legitimiteit en continuïteit. Tegelijkertijd moet de structuur voldoende wendbaar zijn om toekomstige technologische of organisatorische ontwikkelingen te kunnen opvangen, zoals schaalvergroting, vervanging van leveranciers, toetreding van nieuwe partijen of herinrichting van verantwoordelijkheden. Dit vraagt om vooraf doordachte scenario's, bestuurlijke flexibiliteit en een solide juridische borging.

Zonder deze randvoorwaarden is iedere technische realisatie gebouwd op drijfzand. De governance-inrichting moet daarom de eerste stap zijn, vóórdat met implementatie wordt gestart. Alleen zo worden risico's beheersbaar, kan expertise doelgericht worden ingezet en wordt het beheer structureel en betrouwbaar ingericht.

In het volgende hoofdstuk wordt ingegaan op de manier waarop risicomanagement, benodigde expertise en beheerinrichting worden georganiseerd om de strategie duurzaam tot uitvoering te brengen.

11 RISICOMANAGEMENT, EXPERTISE EN BEHEER

Met de keuze voor een gefaseerde datacenterstrategie, van een twin-datacenter binnen Caribisch Nederland naar een model met uitwijk naar Europees Nederland, wordt een robuuste basis gelegd voor digitale continuïteit en betrouwbaarheid. Maar techniek alléén is niet voldoende. De slagingskans van deze strategie wordt in hoge mate bepaald door de manier waarop risico's worden beheerst, expertise wordt georganiseerd en beheer wordt ingericht. Dit hoofdstuk beschrijft de voorwaarden en aanbevelingen op deze drie belangrijke aspecten. Het biedt richting voor de inrichting van risicomanagement, het ontwikkelen van noodzakelijke capaciteit en het borgen van een beheerstructuur die past bij de geadviseerde koers.

11.1 Vooraf borgen, niet achteraf bijsturen

Advies is om het risicomanagement vanaf de start integraal onderdeel te maken van de uitvoering van de datacenterstrategie. Wellicht ten overvloede, maar de complexiteit van de gekozen opzet, een stapsgewijze realisatie van een twin-datacenter in Caribisch Nederland met uitbouw naar Europees Nederland, vereist een professionele benadering van risicobeheersing. Dit betekent niet reactief bijsturen na incidenten, maar proactief risico's voorzien, analyseren en inregelen in zowel ontwerp als beheer.

11.2 Structureel risicobeheer

Het verdient aanbeveling om risicomanagement te verankeren in de governance en uitvoering van de strategie, met heldere afspraken over eigenaarschap, rapportage en actualisatie. Niet alleen technische risico's zoals netwerkuitval, dataverlies of compliance-issues dienen in beeld te zijn, maar ook organisatorische risico's, zoals gebrek aan personele capaciteit, bestuurlijke stagnatie of onduidelijke taakverdeling. Zonder structureel risicobeheer dreigt de uitvoering te verzanden of onnodig kwetsbaar te worden voor voorspelbare verstoringen.

11.3 Benodigde expertise organiseren

De uitvoering vraagt om versterking van de technische en organisatorische expertise in Caribisch Nederland. Aanbevolen wordt om gericht te investeren in kennisopbouw bij SSO-CN, via opleidingen, kennisdeling en structurele ondersteuning vanuit Europese overheidspartijen zoals SSC-ICT, Logius, Dictu en ODC-Noord. Daarbij moet de inzet gericht zijn op het opbouwen van structurele capaciteit, niet op incidentele ondersteuning of ad-hoc detachering. Alleen dan kan lokaal eigenaarschap worden gerealiseerd zonder afhankelijkheid van derden. Tegelijkertijd moet in EN specifieke expertise worden ingezet voor inrichting, compliance, beveiliging en interoperabiliteit. De samenwerking tussen CN en EN vereist een gedeeld beeld van verantwoordelijkheden en specialistische ondersteuning die gericht is op de langetermijninstandhouding van de voorziening.

11.4 Professionele inrichting van beheer en exploitatie

Aanbevolen wordt om beheer en exploitatie niet te benaderen als een sluitstuk van het project, maar als integraal onderdeel van de strategische realisatie. Dit betekent dat verantwoordelijkheden voor beschikbaarheid, incidentmanagement, beveiliging- en crisismanagement, capacity planning en lifecyclebeheer vooraf moeten zijn belegd. Hiervoor is een professioneel ingerichte beheerorganisatie nodig, waarin lokale uitvoering en centrale ondersteuning elkaar aanvullen, met duidelijke overdrachtsmomenten, aanspreekpunten en prestatie-afspraken. Het verdient aanbeveling om beheersafspraken contractueel te verankeren in dienstverlenings-overeenkomsten en SLA's, met concrete prestatie-indicatoren en escalatie-procedures. Alleen dan ontstaat een voorspelbaar en bestuurbaar exploitatiemodel.

11.5 Financiële borging en risicobuffers

Een ander essentieel aandachtspunt is de financiële borging. Advies is om investerings- én exploitatiekosten meerjarig af te stemmen, inclusief ruimte voor risicobuffers en onvoorziene uitgaven. Bezuinigingen op beheer of onvoldoende structurele financiering leiden vrijwel zeker tot knelpunten op het gebied van continuïteit, beveiliging of innovatie. Juist vanwege de strategische functie van digitale infrastructuur in CN verdient deze borging expliciete aandacht op bestuurlijk niveau.

11.6 Conclusie risicobeheersing

De datacenterstrategie zoals in de voorgaande hoofdstukken uiteengezet, is alleen uitvoerbaar als risicomanagement, beheer en benodigde expertise vanaf de start goed worden ingericht. Technische architectuur, bestuurlijke samenwerking en organisatorische keuzes vallen of staan met de mate waarin deze randvoorwaarden professioneel en structureel worden ingevuld.
Het advies is om deze onderdelen op te nemen in de eerstvolgende fase van de realisatie, betrek hiervoor de juiste partijen tijdig, en borg ze contractueel en bestuurlijk. Daarmee wordt niet alleen uitvoering mogelijk gemaakt, maar ook de houdbaarheid, veiligheid en betrouwbaarheid van de gekozen strategie op de lange termijn zeker gesteld. In bijlage B is uitgewerkt hoe deze strategische randvoorwaarden vertaald worden naar een globaal implementatiepad.

12 CONCLUSIES EN VERDERE AANBEVELINGEN

De analyse van het huidige datacenterlandschap in Caribisch Nederland maakt duidelijk dat de bestaande situatie een belemmering vormt voor de verdere digitalisering van het gebied, zowel bestuurlijk als strategisch. Hoewel het SSO-CN samen met het CIO-office goede stappen heeft gezet om versnippering en gebrek aan centrale sturing terug te dringen, blijft het bereik beperkt. Het dienstenportfolio is smal en richt zich uitsluitend op rijksoverheden, terwijl andere publieke stakeholders buiten beeld blijven. Hierdoor blijft de schaal bij deze stakeholders te klein om te voldoen aan de noodzakelijke eisen voor digitale soevereiniteit, continuïteit en kwaliteitsborging. De infrastructuur van de Openbare Lichamen, ZBO's en overige partijen blijft kwetsbaar, met een dienstverlening die per eiland verschilt en sterk afhankelijk is van tijdelijke oplossingen en projectmatige financiering. Deze situatie is onverenigbaar met de overheidsbrede ambitie om publieke digitale diensten betrouwbaar, gelijkwaardig en toekomstbestendig beschikbaar te maken voor álle inwoners van Caribisch Nederland.

12.1 Gefaseerde strategie

Op basis van de strategische variantenanalyse wordt geadviseerd om scenario 2 (twin-datacenter binnen Caribisch Nederland) en scenario 10 (twin-datacenter tussen Caribisch en Europees Nederland) niet als afzonderlijke alternatieven te beschouwen, maar parallel te realiseren in één geïntegreerde strategie.

Variant 2 maakt een snelle en haalbare start mogelijk binnen de lokale context. Door op korte termijn een twin-datacenterstructuur op Bonaire en Sint Eustatius of Saba te realiseren, ontstaat directe winst in termen van redundantie, beschikbaarheid en schaalbaarheid. De bestaande infrastructuur op Bonaire, waaronder het datacenter van SSO-CN, kan hierbij dienen als basis. Voor de bovenwindse eilanden wordt aanbevolen een modulaire voorziening op Sint Eustatius of Saba te ontwikkelen, bijvoorbeeld met orkaanbestendige containerdatacenters op beveiligde locaties van KMAR of Politie. Als alternatief kan samenwerking met Eutel en Satel worden verkend.

Variant 10 maakt het groeipad naar structurele integratie in de landelijke digitale infrastructuur. Aansluiting op een overheidsdatacenter in Europees Nederland maakt structurele uitwijk, ondersteuning en volledige beleidsmatige en technische compliance mogelijk.

Het advies is daarom om nu te besluiten tot de realisatie van een gecombineerde aanpak op basis van variant 2 en 10. Deze gefaseerde benadering combineert snelle uitvoerbaarheid met waarde op lange termijn voor CN én EN.

12.2 Architectuur ten behoeve van de strategie

De doelarchitectuur (zie Bijlage A) ondersteunt deze strategie. De twin-opzet op Bonaire en Sint Eustatius of Saba voldoet aan actuele eisen op het gebied van betrouwbaarheid, schaalbaarheid, segmentatie en energie-efficiëntie. Door in te zetten op Tier III-inrichting, fysieke segmentering van vertrouwelijke data, en redundante stroom- en netwerkvoorzieningen, wordt een robuuste infrastructuur opgebouwd die bestand is tegen lokale verstoringen, cyberdreigingen en natuurlijke calamiteiten.
Belangrijk daarbij is dat beide datacenters onderling worden verbonden via een veilige, snelle en redundante glasvezelverbinding. Deze koppeling maakt failover, dagelijkse replicatie en synchronisatie mogelijk, waardoor beschikbaarheid en gegevensbeveiliging structureel geborgd zijn. Daarnaast biedt deze infrastructuur ruimte voor toekomstige uitbreiding, zoals aansluiting van Saba of koppeling met extra netwerken en diensten.

12.3 Cruciale rol van zeekabels

Geen datacenterstrategie voor Caribisch Nederland is houdbaar zonder strategische verbetering van de onderzeese kabelinfrastructuur. De huidige kabelroutes, zoals het SSCS-systeem, en de kabels tussen beneden- en bovenwinds lopen deels via buitenlandse netwerken en derde landen, wat leidt tot verhoogde risico's op afluisterbaarheid, vertraging en beperkte (en dure) bandbreedte. Een brief van onder andere het ministerie van Economische Zaken (Kamerstuk 86825581) en het rapport van TNO (Research into Data Subsea Cables)

bevestigen dat er sprake is van een fundamentele kwetsbaarheid en afhankelijkheid.

De aanleg van een rechtstreekse onderzeese verbinding tussen Bonaire, Sint Eustatius of Saba en Europees Nederland is geen wens maar een strategische noodzaak. Totdat die verbinding gerealiseerd is, kunnen bestaande, deels verouderde, routes worden benut, al brengen die hogere latency en veiligheidsrisico's met zich mee. Dat vraagt om bewuste keuzes over welke data worden gesynchroniseerd, hoe vaak en met welk niveau van versleuteling. Een nieuwe zeekabel biedt de grootste zekerheid voor continuïteit, digitale autonomie en beheer onder Nederlands recht, maar vergt aanzienlijke investeringen en een langere doorlooptijd. Het benutten van bestaande kabelsystemen met dedicated capaciteit, contractueel geborgd in meerjarige SLA's, is sneller en betaalbaarder, maar houdt afhankelijkheid van commerciële partijen en buitenlandse jurisdictie in stand. Daarom ligt een hybride aanpak voor de hand: bestaande infrastructuur optimaal benutten met harde afspraken voor de korte termijn, terwijl parallel wordt toegewerkt naar een eigen of gezamenlijk beheerde zeekabel als structurele oplossing.

Nieuwe verbindingen moeten vallen onder Nederlandse of Europese jurisdictie, directe routes volgen zonder tussenkomst van derde landen, en voldoen aan eisen op het gebied van latency, capaciteit, encryptie en netwerksegmentatie. Het voorstel om via deze nieuwe kabel een Internet Exchange (IX) op Bonaire te koppelen aan een IX op Sint Eustatius of Saba, verhoogt de performance van internetafhandeling binnen Caribisch Nederland en vergroot de regionale onafhankelijkheid van derde partijen/landen. Zonder deze verbinding is de strategie technisch onvolledig en politiek kwetsbaar. Als de rechtstreekse routes tussen beneden-, bovenwinds en Europees Nederland er niet komen of uitblijven, heeft dat serieuze gevolgen voor de ontwikkeling van de regio zoals beschreven in hoofdstuk 7 'Randvoorwaarden voor netwerkinfrastructuur'.

12.4 Governance en financiering zijn voorwaarden voor succes

De strategie kan alleen succesvol worden geïmplementeerd als deze is ingebed in een heldere governance-structuur met voldoende bestuurlijke slagkracht. Het advies is om regie vanuit het ministerie van BZK te voeren, in nauwe samenwerking met de openbare lichamen, SSO-CN, RCN, de CIO Rijk en relevante uitvoeringsorganisaties. De verantwoordelijkheden voor eigenaarschap, exploitatie en compliance moeten expliciet worden belegd in bestuurlijke akkoorden en dienstverleningsovereenkomsten. Hierbij hoort ook juridische borging van databeheer, zodat zowel autonomie als aansluiting op overheidsinfrastructuur goed geregeld is.

Daarnaast is structurele financiering een randvoorwaarde. Digitale infrastructuur is geen tijdelijk project, maar een blijvende publieke verantwoordelijkheid, zeker op de BES-eilanden waar marktwerking beperkt is en structurele personeelstekorten spelen. Het is dan ook raadzaam om digitale infrastructuur formeel te erkennen als een publieke nutsvoorziening die permanent beschikbaar, veilig en betrouwbaar moet functioneren. Eenmalige investeringen in infrastructuur, zeekabels en organisatie moeten worden gevolgd door structurele financiering voor exploitatie, beheer, innovatie en versterking van lokale expertise. Het hanteren van incidentele of projectmatige financiering vergroot het risico op stilstand, kwaliteitsverlies en onnodige vertraging.

12.5 Professioneel beheer en risicomanagement

De kwaliteit van beheer is bepalend voor het succes van deze strategie. De aanbeveling is om beheerprocessen professioneel en integraal in te richten, conform ITIL/BIO en met duidelijke afspraken over incidenten, onderhoud, wijzigingen en capaciteit. De beheerstructuur moet hybride zijn: lokaal waar mogelijk, centraal waar nodig. Dit betekent dat SSO-CN operationeel verantwoordelijk is (zij werken reeds met ITIL) maar ondersteund wordt door SSC-ICT, ODC Noord of andere rijksdiensten voor specialistische ondersteuning en escalatie. Daarnaast moet risicomanagement in Caribisch Nederland voor overheden vanaf dag één worden toegepast, niet als controle achteraf, maar als integraal onderdeel van ontwerp, inrichting en exploitatie. Denk hierbij aan risico's op het gebied van netwerken (zoals kabelbreuken, latency en single points of failure), energievoorziening, personele capaciteit en juridische compliance. De risicostrategie moet worden vastgelegd in een formeel risicoregister en periodiek worden geactualiseerd. Hier ligt een belangrijke taak voor CIO-RCN ten behoeve van advies en architectuur.

12.6 Lokale capaciteit en eigenaarschap versterken

Om de strategie duurzaam te laten landen, is versterking van lokale capaciteit noodzakelijk. Caribisch Nederland moet niet alleen afnemer, maar ook mede-eigenaar en medevormgever zijn van de digitale infrastructuur. Dit vereist opleidingstrajecten, kennisdeling, deelname aan ontwerp- en besluitvorming, en ruimte voor lokale regie in het dagelijkse beheer. RCN en SSO-CN spelen hierin een sleutelrol, maar de samenwerking met lokale overheden, scholen en (semi)publieke partners is essentieel. Alleen door het opbouwen van lokaal eigenaarschap (medezeggenschap door o.a. Openbare Lichamen) wordt de infrastructuur robuust, wendbaar en maatschappelijk gedragen.

12.7 Duurzaamheid en circulariteit

De maatregelen zoals vastgelegd in bijlage C maken duidelijk dat duurzaamheid geen bijzaak is, maar een randvoorwaarde. Nieuwe voorzieningen moeten energiezuinig, herbruikbaar en onderhoudsarm zijn, en aansluiten bij de principes van circulaire economie. Koeling, stroomvoorziening, locatiekeuzes en materiaalgebruik moeten voldoen aan PUE-normen, cradle-to-cradle-ontwerp en minimale milieubelasting. Deze keuzes zijn niet alleen verantwoord, maar ook kosteneffectief op de lange termijn.

12.8 Integraal verbinden met digitaliseringsbeleid

De datacenterstrategie moet niet geïsoleerd worden uitgevoerd, maar verbonden blijven met bredere digitaliseringsvraagstukken zoals digitale inclusie, cloudbeleid, basisregistraties en netwerkinfrastructuur. Aansluiting op Diginetwerk, GDI, basisadministraties en andere landelijke voorzieningen vereist een veilige en beheersbare infrastructuur. De aanbeveling is dan ook om de strategie in te bedden in een breder digitaliseringsprogramma voor Caribisch Nederland, met duidelijke doelen, afhankelijkheden en sturingsmechanismen.

12.9 Strategische keuze en vervolg

Dit rapport vormt de afronding van de verkenningsfase voor de datacenterstrategie in Caribisch Nederland. De logische vervolgstap is het maken van een expliciete bestuurlijke strategische keuze. Op basis van de uitgevoerde analyse luidt het advies om de gecombineerde koers van scenario 2 en scenario 10 vast te stellen als richtinggevend kompas voor de komende jaren. Deze keuze vormt de basis voor een voorbereidend programma waarin concrete projecten, financiering, aanbestedingen en samenwerking worden uitgewerkt. Bijlage B bevat hiervoor een globaal stappenplan. In dit programma moeten ook de aanleg van de nieuwe zeekabels, het ontwerp van het twin-datacenter en de juridische en governance-inrichting worden voorbereid.

Het programma moet dan worden geleid door een programmamanager met mandaat, ondersteund door een projectorganisatie waarin alle betrokken partijen zijn vertegenwoordigd. Tegelijkertijd moeten marktverkenningen, contractstrategieën en technische ontwerpen parallel worden opgestart, om geen tijd te verliezen. Alleen door nu door te pakken, wordt de ambitie echt vertaald naar resultaat.

BIJLAGEN

A Bijlage - Globale doelarchitectuur

Om digitale dienstverlening op de BES-eilanden structureel te verbeteren en toekomstbestendig te maken, is een robuuste en soevereine datacenterinfrastructuur noodzakelijk. In dit hoofdstuk wordt de globale doelarchitectuur voor variant 2 uitgewerkt: een twin-datacenteropzet op Bonaire, Saba of Sint Eustatius. In deze doelarchitectuur werken wij één opzet uit: een opzet op Bonaire en Sint Eustatius. Op papier is op Sint Eustatius meer infrastructuur (én elektriciteitsvoorzieningen) aanwezig. Een nadere kijk hierop zou doorslag kunnen geven, waarbij in het geval de keuze op Saba valt, in de doelarchitectuur ook Saba in plaats van Sint Eustatius gelezen kan worden. Deze opzet ondersteunt niet alleen de continuïteit en veiligheid van publieke dienstverlening, maar biedt ook een fundament voor bredere digitale samenwerking binnen Caribisch Nederland. De architectuur is gebaseerd op strategische uitgangspunten die zowel technische als organisatorische eisen integreren. Denk hierbij aan betrouwbaarheid, schaalbaarheid, energie-efficiëntie en juridische beheersbaarheid. De komende paragrafen beschrijven de fysieke inrichting, energievoorziening, netwerkkoppelingen, gebruiksmodellen en de regie op beheer.

VISIE EN STRATEGISCHE UITGANGSPUNTEN

De doelarchitectuur voor variant 2 richt zich op het opzetten van twee volwaardige datacenters binnen Caribisch Nederland, op Bonaire en op Sint Eustatius. Sint Eustatius lijkt momenteel een betere keuze voor de bovenwindse eilanden, omdat er o.a. een geschiktere infrastructuur met hogere capaciteit en populatie is. De beide datacenters vormen idealiter samen een twin-datacenterstructuur. Deze opzet biedt maximale beschikbaarheid en digitale soevereiniteit, met bescherming tegen lokale verstoringen door onderlinge failover en redundantie. Het concept sluit nauw aan bij de wens om publieke dienstverlening op de eilanden te versterken en futureproof te maken, met beheersbaarheid binnen het Nederlandse domein.

FYSIEKE INFRASTRUCTUUR EN LOCATIE-EISEN

Beide datacenters worden gebouwd of aangepast volgens de hedendaagse normen voor betrouwbaarheid en veiligheid (Minimaal Tier III) Elk centrum beschikt over redundante stroomvoorziening, UPS-systemen, dieselaggregaten, branddetectie- en blussystemen, fysieke toegangscontrole en inbraakbeveiliging. De locatie-inrichting is modulair en schaalbaar met verschillende ruimten, zodat gegevens met hogere geheimhoudingsclassificatie van het rijk separaat kunnen worden van de rest van het datacentrum. De gebouwen moeten bestand zijn tegen de extreme weersomstandigheden die in het Caribisch gebied voorkomen, in het bijzonder op de bovenwindse eilanden. Stormbestendige constructies, verhoogde vloerniveaus, windbestendige beplating en waterdichte toegangsvoorzieningen zijn hierbij essentieel. Op Sint Eustatius kan bij een gefaseerde aanpak worden gestart met containerdatacenters of andere modulaire bouwvormen om snel operationeel te zijn en ervaring op te bouwen. Op Bonaire kunnen de bestaande datacenters worden gebruikt, totdat daar een betere en schaalbaardere voorziening is voorzien.

KOELING EN KLIMAATBEHEER

Vanwege het warme en vochtige klimaat zijn energie-efficiënte koeloplossingen noodzakelijk. Er wordt gewerkt met in-row of close-coupled koeling, gecombineerd met passieve en smart-gestuurde systemen die inspelen op actuele belasting en weersomstandigheden. Waar mogelijk worden natuurlijke luchtstromen benut, en bij nieuwbouw wordt aandacht besteed aan gebouworiëntatie, isolatie en reflectie van zoninstraling. Dit alles draagt bij aan het beperken van energieverbruik en verhoging van betrouwbaarheid.

ENERGIEVOORZIENING EN DUURZAAMHEID

Beide locaties krijgen dubbele netaansluitingen, UPS-voorzieningen en dieselaggregaten met voldoende opslagcapaciteit voor langdurige uitval. Duurzaamheid wordt integraal meegenomen via slimme energiesturing, PUE-monitoring en waar mogelijk toepassing van zonne-energie. Ook de inzet van herbruikbare en onderhoudsarme infrastructuur wordt gestimuleerd volgens het cradle-to-cradleprincipe. (C2C) Materialen en componenten worden zodanig gekozen en toegepast dat ze na hun gebruik opnieuw kunnen worden ingezet of veilig kunnen worden gerecycled, waardoor het datacenter past binnen een circulaire economie. Dit principe bevordert duurzaamheid door onder meer modulair bouwen, veilige materiaalkeuzes en het minimaliseren van verspilling gedurende de hele levenscyclus van het gebouw en de infrastructuur.

NETWERKCONNECTIVITEIT EN ONDERLINGE KOPPELING

De twee datacenters worden onderling verbonden via een nieuwe onderzeese glasvezelverbinding, bij voorkeur met hoge bandbreedte en relatief lage latency, zodat dagelijkse replicatie, synchronisatie en failover effectief mogelijk zijn. Als alternatieve verbinding tussen Saba en Sint Eustatius kan gebruik worden gemaakt van bestaande, oudere onderzeekabels (via SCF, ECFS en PCCS over St. Kitts en -Barths), een draadloze (microwave) verbinding of, indien technisch en economisch haalbaar, een tweede zeekabel langs een alternatieve route. Deze verbinding fungeert als redundantie voor de SSCS en vermindert de afhankelijkheid van externe netwerken of derde landen in het geval van een storing in het primaire systeem. Een toekomstige nieuwe zeekabel tussen Bonaire, Sint Eustatius en Europees Nederland kan bovendien zodanig worden ontworpen dat deze via zowel Sint Eustatius en Saba loopt, waarmee dezelfde strategische robuustheid wordt bereikt in combinatie met de SSCS. Binnen elk datacenter zijn de interne netwerken logisch gescheiden in beheer-, productie- en replicatieverkeer, met beveiliging op basis van netwerksegmentatie, firewalls en end-to-end encryptie van datastromen.

Extern zijn beide locaties verbonden met lokale telecomproviders en, bij voorkeur, een lokale Internet Exchange (IX) op Bonaire, die idealiter ook doorgetrokken wordt over de nieuwe kabel naar Sint Eustatius. Ook wordt expliciet rekening gehouden met toekomstige aansluiting op nieuwe onderzeese kabelinitiatieven op zowel Bonaire als Sint Eustatius.

Daarnaast dienen beide datacenters te beschikken over veilige en redundante koppelingen met Nederlandse overheidsnetwerken, waaronder Diginetwerk, het Rijks Overheids Netwerk (RON), BelastingNet, en andere overheidsnetwerken die benodigd zijn voor het ontsluiten van landelijke voorzieningen. Dit is noodzakelijk om overheidsorganisaties op de eilanden toegang te geven tot generieke digitale diensten zoals DigiD, de Basisregistratie Personen (BRP), de Basisregistratie Adressen en Gebouwen (BAG), Kadasterdata, het Handelsregister (KvK), en ketenintegraties zoals met DUO, de RDW en CJIB.

Deze verbindingen moeten voldoen aan de eisen voor beschikbaarheid, integriteit en vertrouwelijkheid en dienen technisch te worden ingericht met redundantie, bandbreedtegaranties en netwerksegmentatie. Verkeer mag bij voorkeur niet via derde landen worden geleid, zoals Venezuela, Panama, de Verenigde Staten of de Dominicaanse Republiek, vanwege risico's op afluisteren, geopolitieke afhankelijkheden en verhoogde latency. De connectiviteit moet primair verlopen via soevereine, juridisch beheersbare routes onder Nederlandse of Europese controle.

INTEGRATIE EN TOEKOMSTVASTHEID

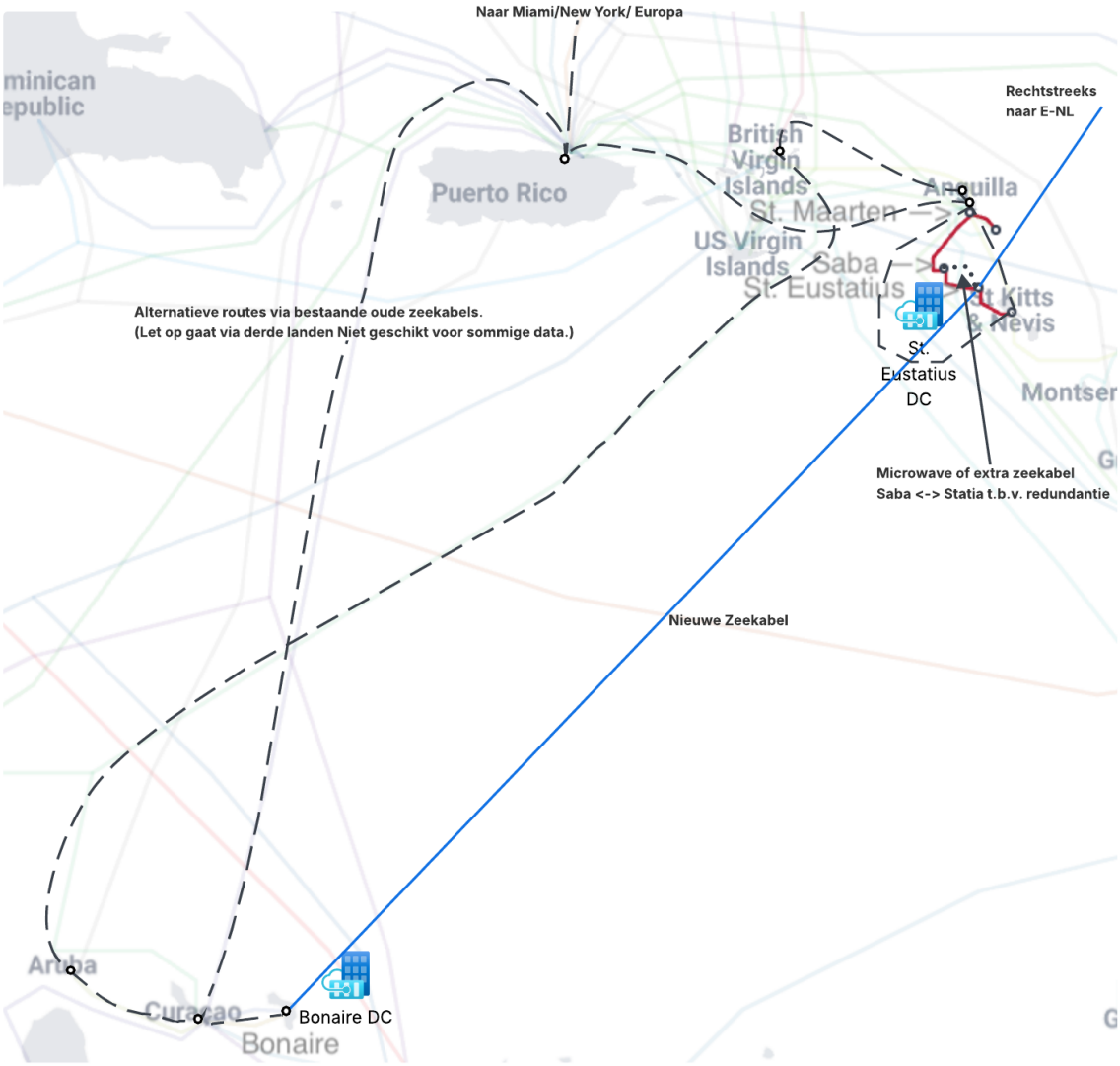
De twin-datacenterarchitectuur biedt de mogelijkheid om door te groeien naar een formeel Overheidsdatacenter Caribisch Nederland (ODC-CN). Het ontwerp is voorbereid op koppelingen met of maakt idealiter onderdeel uit van landelijke voorzieningen (zoals rijkscloud of centrale back-ups), maar blijft primair gericht op regionale zeggenschap en robuustheid. De strategie is alleen houdbaar als deze gepaard gaat met structurele investeringen in onderzeese infrastructuur en lokale capaciteitsversterking.

Randvoorwaarden (prerequisites)

Categorie	Voorwaarde
Fysieke infrastructuur	Twee geschikte locaties op Bonaire en Sint Eustatius. Gebouwen conform Tier III. Bestendigheid tegen orkanen, stormen en vocht. Optioneel: inzet van containerdatacenters voor gefaseerde start, of kleinschalige uitrol met name op Sint Eustatius. Fysieke segmentering in het datacenter om ook Rijksoverheidsdata van departementaal vertrouwelijk niveau of hoger te kunnen huisvesten separaat van de overige afnemers.

Energievoorziening	Redundante netaansluitingen, UPS-systemen, dieselaggregaten, brandstofopslag, smart energiemanagement.
Koeling	In-row en/of close-coupled koeling, passieve koeling, smart gestuurde systemen, gebouworiëntatie, isolatie.
Netwerk (intern)	Glasvezelverbinding(en) tussen beide locaties met hoge bandbreedte, lage latency, redundantie en scheiding van verkeer. DWDM voor inzet op alle glasvezels en zeekabels, dit om schaalbaarheid en scheiding van gegevens te garanderen.
Netwerk (extern)	Verbindingen naar lokale providers, IX op Bonaire, mogelijk doorgetrokken tot Sint Eustatius. Voorbereiding op nieuwe zeekabels. Vermijden van routes via derde landen, en de kortst mogelijke routes, om latency te verminderen. Aansluiting op Europees Nederlandse en Internationale netwerken op een slimme manier. (Optimale routes, bandbreedte reserveringen, separate kanalen en/of QoS) VPN als extra alternatief voor redundantie op (privé) zeekabels. Cloudconnectiviteit zoveel mogelijk privé routeren, vanwege veiligheid en kwaliteit van de verbindingen.
Beheer & exploitatie	Regie door RCN, het datacenter gepositioneerd als een onderdeel van een bestaande rijksdienst, zoals ODC-Noord of SSC-ICT. Operationeel beheer door SSO-CN of marktpartner. Eilanden kunnen zoveel mogelijk (binnen redelijkheid) autonoom (geïsoleerd) functioneren, in het geval van calamiteiten.
Compliance	Voldoen aan alle BIO, NIS2, AVG, Nederlandse wetgeving of afsprakenkaders met vergelijkbare borging. Juridische borging van beschikkingsmacht. Marktconforme tarieven. SLA's op hersteltijden van verbindingen, zodat een kabelbreuk snel verholpen wordt, of een werkende bypass opgeleverd wordt. Juridische inbedding van datacenterfaciliteiten als onderdeel bestaande rijksdienst, om inbesteding mogelijk te maken.

OVERZICHT DOELARCHITECTUUR



Figuur 15.2: Een kijk op de potentiële doelarchitectuur
In bovenstaand figuur is een mogelijke doelarchitectuur weergegeven voor de netwerkinfrastructuur tussen twee datacenters in Caribisch Nederland: één op Bonaire en één op Sint Eustatius.

De **blauwe lijn** stelt een nog aan te leggen onderzeese glasvezelverbinding voor. Deze zou Bonaire rechtstreeks verbinden met Sint Eustatius, en vervolgens kunnen worden doorgetrokken naar Europees Nederland – al dan niet via Saba. Het betreft een strategische verbinding die buiten derde landen om loopt, wat de kans op afluisteren en geopolitieke beïnvloeding aanzienlijk verkleint. Deze verbinding biedt ook voordelen in latency, capaciteit en beschikbaarheid.

De **rode lijn** toont de bestaande Saba Statia Cable System (SSCS), die in eigendom is van de Nederlandse Overheid. Deze verbinding loopt vanuit St. Kitts via Sint Eustatius en Saba door naar onder andere St. Maarten en St. Barths. Hoewel deze verbinding op dit moment operationeel is en eigendom van de Nederlandse overheid, loopt hij deels via buitenlandse grondgebieden en netwerken, wat enkele afhankelijkheden met zich meebrengt. Communicatie tussen Sint Eustatius en Saba kan rechtstreeks plaatsvinden.

Een **gestippelde lijn** tussen Sint Eustatius en Saba geeft een mogelijke additionele redundante verbinding aan. Deze zou gerealiseerd kunnen worden via een draadloze microwaveverbinding, of via een korte extra zeekabel. Dit pad dient als fallback bij storingen in het primaire traject, en vergroot de netwerkweerbaarheid binnen het twin-datacenterconcept.

De **onderbroken lijnen** representeren bestaande oudere zeekabels van commerciële derde partijen. Deze verbindingen lopen eveneens via derde landen en brengen verhoogde risico's met zich mee op het gebied van geopolitieke controle, afluisterbaarheid en technische kwetsbaarheid. Omwille van de leesbaarheid zijn in de figuur niet alle verbindingen weergegeven; het betreft hier een selectie van de meest relevante en gangbare routes.

B Bijlage - Stappenplan richting geprefereerde variant

Voor de implementatie van de datacenterstrategie in Caribisch Nederland is een gefaseerde aanpak aanbevolen, waarin bestuurlijke besluitvorming, technische voorbereiding, realisatie en ingebruikname logisch op elkaar aansluiten. De totale doorlooptijd is afhankelijk van beschikbare middelen, regie en samenwerking tussen betrokken partijen. Bij tijdige besluitvorming en adequate inzet van capaciteit is een stapsgewijze realisatie binnen een beheersbaar tijdsbestek goed uitvoerbaar.

FASE 1 – STRATEGISCH BESLUIT EN VOORBEREIDING

Het project begint met een voorbereidingsfase waarin bestuurlijk commitment, beleidskaders en financieringsafspraken worden vastgesteld. Dit vormt de formele start van het programma. Er wordt een stuurgroep en projectteam ingericht en budget gereserveerd voor de eerste uitvoeringsstappen. Tegelijkertijd worden de functionele en technische behoeften van overheden en semi-overheden geïnventariseerd, en wordt gestart met het informeren van stakeholders over de opzet en het belang van het project. Deze fase biedt tevens ruimte voor het inrichten van een heldere governance en projectstructuur onder regie van de Rijksdienst Caribisch Nederland (RCN).

FASE 2 – ONTWERP EN LOCATIEVERKENNING

Na het strategisch akkoord volgt de ontwerpfase, waarin een technische uitwerking van de doelarchitectuur centraal staat. In deze fase wordt een gedetailleerde inventarisatie uitgevoerd van bestaande systemen, gebruikersbehoeften en randvoorwaarden. Op basis daarvan worden een technisch ontwerp en een programma van eisen opgesteld voor de twin-datacenteropzet. Tegelijkertijd worden er locaties op Bonaire en Sint Eustatius of Saba beoordeeld op geschiktheid en haalbaarheid. De aansluiting op toekomstige onderzeese kabelprojecten wordt integraal meegenomen in de ontwerpkeuzes.

FASE 3 – AANBESTEDING, CONTRACTERING EN VOORBEREIDING

Vervolgens verschuift de aandacht naar aanbesteding, selectie en formele contractvorming. Dit betreft onder meer de bouw of plaatsing van de datacenters (waaronder de afweging tussen nieuwbouw of containeroplossingen op Sint Eustatius of Saba), de levering van hardware en software, en het afsluiten van dienstverleningsovereenkomsten met strategische partners zoals SSO-CN, SSC-ICT, Logius en mogelijk ODC Nederland. Tegelijkertijd worden connectiviteitscontracten voorbereid voor betrouwbare netwerkverbindingen op de eilanden en naar Europees Nederland. Deze fase vormt de laatste voorbereiding op de daadwerkelijke implementatie.

FASE 4 – REALISATIE VAN INFRASTRUCTUUR EN PLATFORM

De fysieke implementatie vindt plaats in opeenvolgende stappen. Op Bonaire wordt begonnen met de bouw of plaatsing van het datacenter, het aanleggen van de nutsvoorzieningen en voor de dienstverleners; het installeren van ICT-infrastructuur, waaronder servers, opslag, netwerkcomponenten en beveiligingssystemen. Gelijktijdig met de inrichting van het tweede datacenter op Sint Eustatius of Saba. In deze fase worden ook de onderlinge glasvezelverbindingen gerealiseerd, netwerksegmentatie ingericht, beveiligingsmaatregelen toegepast en koppelingen vanuit Europees Nederland gelegd met voorzieningen zoals Diginetwerk en BelastingNet. Na succesvolle testprocedures wordt toegewerkt naar een productierijpe twin-architectuur. Tegelijkertijd worden er koppelingen gelegd met de lokale telecombedrijven, en wordt met hun hulp eventueel een internet exchange opgebouwd. (Eventueel in stichting vorm)

FASE 5 – MIGRATIE, UITROL EN INGEBRUIKNAME

Zodra beide datacenters operationeel zijn, begint de gefaseerde migratie van overheidsdiensten. Diensten van rijksorganisaties, openbare lichamen en semi-publieke instellingen worden stap voor stap overgezet naar de nieuwe infrastructuur. Oude systemen worden gecontroleerd uitgefaseerd. Tegelijkertijd worden betrokken medewerkers opgeleid en worden gebruikers (indien nodig) begeleid in de overgang naar de nieuwe digitale omgeving. De officiële ingebruikname van het twin-datacenter markeert het einde van deze fase.

FASE 6 – NAZORG, OVERDRACHT EN OPTIMALISATIE

In de afrondende fase blijft het projectteam tijdelijk actief voor monitoring, ondersteuning en overdracht naar structurele beheerorganisaties. RCN draagt de exploitatie formeel over aan de gekozen beheerstructuur (zoals SSO-CN of een consortium). Er worden audits en compliance-checks uitgevoerd, en op basis van gebruikservaring worden optimalisaties doorgevoerd. De voorzieningen worden verankerd in reguliere plannings- en beheerprocessen. De realisatie van rechtstreekse onderzeese verbindingen met Europees Nederland krijgt in deze fase ook verder vorm, waarmee de afhankelijkheid van buitenlandse netwerkhops wordt afgebouwd.

TOT SLOT

Hoewel het stappenplan ambitieus is, wordt het als realistisch beschouwd. De digitale weerbaarheid en continuïteit van publieke dienstverlening op de BES-eilanden vragen om een toekomstbestendige infrastructuur. Iedere maand uitstel vergroot het risico op incidenten, vertraagt de aansluiting op rijksbrede voorzieningen en beperkt de uitvoeringskracht van het digitaliseringsbeleid. Tijdige uitvoering is dan ook essentieel voor zowel de betrouwbaarheid van de publieke dienstverlening als voor de digitale autonomie van Caribisch Nederland.

C Bijlage - Duurzaamheidsmaatregelen

De datacenterstrategie biedt kansen om de duurzaamheid te verbeteren, zowel op de eilanden zelf als in de algehele ICT-voetafdruk van de Rijksoverheid. In dit hoofdstuk wordt advies gegeven welke maatregelen genomen moeten worden om de duurzaamheid te bevorderen. Hierbij wordt gekeken naar energievoorziening, klimaatimpact, afval en circulaire economie en eventuele aanvullende groene initiatieven.

Energie-efficiëntie en groene stroom

Aangeraden wordt om gerichte maatregelen te nemen om het energieverbruik van het datacenter in CN te beperken, gezien de hoge elektriciteitskosten en het feit dat de energievoorziening grotendeels gebaseerd is op dieselgeneratoren. Hoewel het aandeel zonne- en windenergie via WEB toeneemt, blijft de ecologische belasting aanzienlijk. Door de ecologische voetafdruk te verkleinen en tegelijkertijd de exploitatiekosten te verlagen, kan een duurzame en kostenefficiënte exploitatie worden gerealiseerd. De volgende stappen dragen hier aantoonbaar aan bij.

ZONNE-ENERGIE INZET

Evenals op het huidige datacentergebouw op Bonaire dienen ook de nieuwe datacentervoorzieningen zonnepanelen op het dak te hebben. Berekeningen laten zien dat een dak van ca. 200 m² makkelijk 30-50 kWp aan panelen kan dragen, goed voor pakweg 50–80 MWh per jaar in de tropenzon. Dat dekt een significant deel van het jaarverbruik van de datacenters (afhankelijk van de belasting, geschat 100-150 MWh/jaar). Hiermee kan een datacenter overdag (wanneer de airco hard moet werken) een deel van de stroom zelf opwekken, wat de netbelasting verlaagt. Eventuele batterijen slaan exces opgewekte zonne-energie op en eventueel elders opgewekte zon- en windenergie op voor de avondpiek, maar door de 24x7 consumptie is netlevering 's nachts deels onvermijdelijk.

GROENE STROOM INKOPEN IN NL

Bij uitbreiding van variant 2 naar variant 2+10 geldt voor de back-up op de NL-locatie (ODC-Noord bijvoorbeeld) dat het Rijk al stuurt op 100% groene stroom inkoop. Dus stroom die het datacenter in Nederland verbruikt, is afkomstig van duurzame bronnen (wind, zon, etc.). Dit betekent dat de helft van de infrastructuur al klimaatneutraal kan draaien.

EFFICIËNTE KOELING

Het is aan te bevelen om te investeren in moderne, energie-efficiënte koelinstallaties voor een datacenter. Voor CN biedt de inzet van passieve nachtkoeling een kans om energieverbruik te reduceren; wanneer de buitentemperatuur 's nachts onder de 27°C daalt en de luchtvochtigheid dit toelaat, kan buitenlucht worden benut om de servers te koelen in plaats van traditionele compressor-gebaseerde systemen. Overdag is het raadzaam om gebruik te maken van precisie-airconditioning met hoog rendement. Daarnaast verdient koeling via waterverdamping aandacht als aanvullende maatregel, met de kanttekening dat schaarste van zoet water op Bonaire een beperkende factor vormt en zorgvuldig moet worden afgewogen. Het streven naar een Power Usage Effectiveness (PUE) van minder dan 1,5 op CN is realistisch en passend voor de schaal en geografische omstandigheden van het project.

SLIMME LOADVERDELING

Indien mogelijk kunnen wellicht op termijn workloads meer in NL draaien op momenten dat de energiemix daar groener of goedkoper is, en meer lokaal als bijvoorbeeld de zon volop schijnt. Dit is een geavanceerde maatregel voor de toekomst en vraagt realtime orkestratie. Het ligt nu niet direct voor de hand, maar is een gedachte voor de toekomst: dynamisch "eco-gebaseerd" schakelen tussen sites.

Klimaat en mileu-impact

Behalve energie zijn er andere milieuaspecten:

WARMTE-UITSTOOT NUTTIG AANWENDEN

Een datacenter genereert warmte. In plaats van die zomaar weg te koelen naar buitenlucht, is het aan te bevelen om de warmte opnieuw te gebruiken. Hoewel verwarming van gebouwen in het Caribisch gebied overbodig is, kan restwarmte uit een datacenter alsnog nuttig worden ingezet. Zo kan deze warmte worden gebruikt voor absorptiekoeling, waarbij warmte wordt omgezet in koude om gebouwen of apparatuur te koelen. Ook kan restwarmte van waarde zijn voor aquacultuur, door het water op een stabiele temperatuur te houden voor vis- of garnalenteelt. In gecontroleerde landbouwomgevingen zoals hydroponics of vertical farming kan de warmte bijdragen aan een constante groeiomgeving. Daarnaast zijn er toepassingen in industriële processen zoals thermische ontzilting of voorverwarming van proceswater, en kan de warmte worden benut voor droogprocessen van landbouwproducten of bij het versnellen van biovergisting en compostering. Zo biedt restwarmte zelfs in een warm klimaat kansen voor circulair en efficiënt hergebruik.

KOELMIDDELEN

Voor koelinstallaties dient gekozen te worden voor milieu-vriendelijke koelmiddelen (lage GWP – Global Warming Potential). Hiermee wordt voorkomen dat bij eventuele lekkage er sterke broeikasgassen vrijkomen.

LOKALE IMPACT

Datacenters dienen zodanig ontworpen te zijn dat hinder (geluid van generator of airco) minimaal is voor omwonenden. Bijvoorbeeld, plaatsing generator in geluidsdichte behuizing. Ook lichtvervuiling, 's nachts geen felle lampen onnodig aan om natuur (vogels, zeeleven) niet te storen. Dit sluit aan bij het belang dat de Openbare Lichamen, besturen en burgers op de eilanden waarde hechten aan natuur en milieu.

Circulaire economie en e-waste

ICT brengt e-waste met zich mee bij vernieuwing van apparatuur. Maatregelen om dit circulair te beheren zijn:

LEVENSDUURVERLENGING HARDWARE

Geadviseerd wordt om hoogwaardige apparatuur te kopen met verwachte levensduur 5-7 jaar. Daarnaast dient "onderbenutting" te worden voorkomen, liever iets ruim specificeren en langer gebruiken dan elke 3 jaar vervangen. Voor servers/storage zal een lifecycle planning gehanteerd moeten worden waarbij uitgefaseerde hardware bij voorkeur een tweede leven krijgt (bv. als testserver, of donatie aan lokale scholen indien geschikt).

TERUGNAME EN RECYCLING

In contracten met hardwareleveranciers zoveel mogelijk een terugnameclausule opnemen. Bijvoorbeeld, als na 6 jaar de servers vervangen worden, dient de leverancier de oude terug te nemen voor refurbishment of recycling. Zo belandt het niet op de lokale vuilstort. Ook is het van belang om toners, batterijen e.d. via de juiste kanalen af te voeren (RCN heeft daar waarschijnlijk al procedures voor). Zo wordt gewaarborgd dat Europese standaarden voor e-waste ook hier worden gehaald.

Verdere duurzame initiatieven

Naast energie-efficiëntie, klimaatimpact en circulair materiaalgebruik zijn er aanvullende duurzaamheidsmaatregelen denkbaar die specifiek inspelen op de lokale context van Caribisch Nederland. Deze paragraaf beschrijft een aantal van deze verdiepende initiatieven.

INNOVATIE VOOR WATERGEBRUIK

Datacenters gebruiken water (koeling, schoonmaak). In CN is zoet water kostbaar (komt uit zeewater via omgekeerde osmose). Het verdient de aanbeveling om te onderzoeken of grijswater of regenwater opgevangen kan worden een bijdrage kan leveren, bijvoorbeeld regenwateropslag om airco's te voeden of voor spoeling van filters. Dit reduceert de vraag naar drinkwater.

ALIGNEREN MET NATIONALE DOELEN

De Rijksoverheid heeft ambities uit de Klimaatwet en de Nederlandse Digitaliseringsstrategie om ICT duurzamer te maken. De realisatie van de datacenterstrategie kan input leveren aan het Jaarverslag

Bedrijfsvoering Rijk, specifiek de CO_2-footprint. Mogelijk is dit een voorbeeldproject van groene IT op een bijzondere locatie.

MONITORING DUURZAAMHEID

Het is aan te bevelen prestaties te meten. Als de metingen tegenvallen kan bijgestuurd worden (bv. extra panelen bijplaatsen of efficiëntere koeling inzetten).

Gezien de kwetsbare natuur op de eilanden is het aan te bevelen dat het ICT-project niet alleen gericht is op digitale weerbaarheid, maar ook expliciet bijdraagt aan milieuverantwoordelijkheid. Door in te zetten op lokale opwekking van groene energie en een doordacht ontwerp kan het gebruik van diesel en de bijbehorende uitstoot aanzienlijk worden verminderd. Deze benadering sluit aan bij de duurzaamheidsambities van de Openbare Lichamen en adresseert expliciet de zorgen van stakeholders, die het belang van duurzaamheid als randvoorwaarde voor het project hebben benadrukt.

D Overzicht housingvarianten t.o.v. criteria

	Kosten	Organisatie	Duurzaam	Governance	Risico's	Flexibel	Ontzorging	Arbeid	Contracten	Prestatie	Schaal	Sociaal	Continuïteit
1. Lokale DC's per eiland	--	--	--	--	-	-	--	--	--	++	--	+	++
2. Twin DC CN	-	≈	-	≈	+	≈	≈	+	≈	+	≈	++	+
3. Lokaal DC + edge + EU back-up	--	++	≈	+	++	≈	-	++	≈	++	-	++	+
4. Primair EU, lokaal noodplatform	≈	≈	+	≈	++	+	+	--	+	-	+	--	--
5. Volledig private cloud (NL Rijksoverheid)	+	+	++	+	--	+	++	--	+	--	+	--	--
6. Volledig public cloud (EER)	+	+	++	-	≈	++	+	-	+	--	++	-	--
7. Private EU-cloud (managed)	≈	+	+	+	≈	+	+	--	++	--	+	--	--
8. Lokale outsourcing CN	≈	+	-	≈	≈	≈	+	+	+	+	≈	+	≈
9. Hybride cloud (per workload)	≈	-	+	-	≈	+	≈	+	≈	+	+	+	-
10. Twin-datacenter CN / E-NL	+	++	++	++	--	++	-	+	+	≈	+	+	+

In bovenstaande tabel zijn de tien mogelijke varianten weergegeven, beoordeeld op de 12 vastgestelde criteria met een score van ++ (zeer positief), + (positief), ≈ (neutraal), - (negatief) of -- (zeer negatief)

E Bijlage - Bronnen

Omschrijving	Datum	Auteur / Bron
Documenten		
Het Rijk in de cloud, Donkere wolken pakken samen	2025	Algemene Rekenkamer
Onderzoeksrapport naar de oorzaken van de langdurigheid van de onvolkomenheid bij SSO CN	2023	Auditdienst Rijk
Problemen in de bedrijfsvoering van Rijksdienst Caribisch Nederland	2024	Algemene Rekenkamer
I-strategie Rijk 2021 - 2025	2021	Min. van BZK
Onderzoek uitrol Rijksbrede Werkplek in Caribisch Nederland	2018	Berenschot
Rijksbreed cloudbeleid 2022	2022	Min. van BZK
PDC ODC-Noord 2024 v1.1	2024	ODC Noord
Cloud-afwegingskader JenV	2019	Cloud-afwegingskader JenV
20231109 BZK-BES (Gegevens gebruik en -uitwisseling voor Kadaster)	2023	Kadaster
PDC 2025 definitief	2025	SSO CN
PDC2024	2024	SSO CN
20240320 Faseplan-Realisatie SOLL-1en2 v06 (project “Registraties & voorzieningen digitale overheid Caribisch Nederland”)	2024	Min. van BZK
20240501 Datacenters (sheets uit werkbezoek mei 2024)	2024	Min. van BZK
handreiking-risicobeheersing-toepassing-publieke-clouddiensten-2.0	2023	Min. van BZK
implementatiekader-risicoafweging-cloudgebruik-v11	2023	Min. van BZK
kamerbrief-over-rijksbreed-cloudbeleid-2022	2022	Min. van BZK
Het+Rijk+in+de+cloud (Het Rijk in de cloud, Donkere wolken pakken samen)	2025	Algemene Rekenkamer
info datacenter strategie (Documentatie van bestaande datacenters/Netwerkinfrastructuur)	2025	SSO CN
NoO netwerk tekening	2025	SSO CN
ICT-beleid rondom datacenter- en cloud-dienstverlening	2025	Openbaar Lichaam St. Eustatius
GDI-programmeringsplan 2025 - Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO)	2025	Min. van BZK
44223281 Bijlage 4 EBA - Digitale infrastructuur Caribisch Nederland	2023	Min. van EZK
86825581.Bijlage 2 Research into Data Subsea Cables Enabling Caribbean Netherlands digitally	2024	Min. van EZK
86825581.Kamerbrief voortgangsupdate onderzeese datakabels	2024	Min. van EZK
bijlage-2-landing-a-sea-cable-in-the-netherlands	2021	Min. van EZK
Kamerbrief-over-zeekabels	2021	Min. van EZK
DATACENTER strategy used by OLS	2025	Openbaar Lichaam Saba
Organogram met verbindingen RCN SSO CN NETWERK V08	2025	SSO CN
Potentiële SSO CN klanten	2025	SSO CN
Draaiboek crisisbeheersing SSO CN	2024	SSO CN
overzicht betrokken partijen	2025	SSO CN
processen en werkwijze	2025	SSO CN
Terugkoppeling uitkomsten IT-audit interimcontrole	2024	SSO CN

Omschrijving	Datum	Auteur / Bron
Projecthistorie en Evaluaties - MAP	2025	SSO CN
Algemene verordening gegevensbescherming (AVG) vanaf vandaag in werking	2018	Rijksdienst Caribisch Nederland
Telecommunication in the Dutch Caribbean	2016	Min. van BZK
Algemene kaders consolidatie datacenters Rijk	2012	Min. van BZK
Logius Standaard Platform (SP) Turn-key DevOps containerplatfrom in de Nederlandse Rijkscloud	2022	Logius (BZK)
Datacenter TIER tabel en verbeteringen nodig Tier 2 --> 3	2025	SSO CN
Handboek ICT Huisvesting en bekabeling	2022	Rijksvastgoedbedrijf
Submarine Cable Map	Actueel	Submarine Cable Map
De staat van de digitale infrastructuur, de ruggengraat van onze digitale economie	2024	Min. van EZK
Digitale Infrastructuur Caribisch Nederland	2023	Min. van EZK
EUTEL: A structured approach to empower Statia's digital Future	2023	EUTEL NV
The Caribbean Netherlands in numbers 2023: Has electricity production from renewable sources increased?	2023	CBS
BES Connectivity Comparison Explainer (Short and Long)	2025	Pioneer Consulting / Min. van EZ.
Aansluiting Bonaire op nieuwe onderzeese datakabel	2025	Rijksoverheid.nl

F Bijlage - Lijst met afkortingen en definities

Afkorting / Term	Omschrijving
Active Directory	Software binnen het Microsoft Windows-ecosysteem voor centrale authenticatie en beheer van gebruikers, apparaten en toegangsrechten in een netwerk.
Anycast	Anycast is een netwerkconfiguratie waarbij één IP-adres wordt gedeeld door meerdere servers op verschillende locaties. In de context van DNS zorgt dit ervoor dat gebruikers automatisch verbonden worden met de dichtstbijzijnde DNS-server, wat zorgt voor snellere respons en hogere beschikbaarheid.
AVG	Algemene Verordening Gegevensbescherming. Europese wet voor bescherming van persoonsgegevens.
BAG	Basisregistratie Adressen en Gebouwen. Bevat officiële gegevens over adressen en panden in Nederland.
Backbone	Het hoofdnetwerk met hoge capaciteit dat als ruggengraat fungeert voor dataverkeer tussen netwerken, locaties of systemen.
Backup	Kopie van gegevens of systemen die wordt opgeslagen op een aparte locatie om herstel mogelijk te maken bij verlies, beschadiging of uitval van het origineel.
BES eilanden	Bonaire, Sint Eustatius en Saba
Beveiligingchallenges	Vragen of acties die gebruikers moeten beantwoorden of uitvoeren om hun identiteit te verifiëren, zoals het invoeren van een two-factor authenticatiecode, ter bescherming tegen ongeautoriseerde toegang.
BIO	Baseline Informatiebeveiliging Overheid. Normenkader voor informatiebeveiliging binnen de Nederlandse overheid.
CAS eilanden	Curaçao, Aruba en Sint-Maarten
Cache (Caching)	Cache is tijdelijke opslag van vaak geraadpleegde gegevens, zoals DNS-antwoorden of webinhoud, om sneller toegang te bieden en netwerkbelasting te verminderen. Caching verhoogt efficiëntie en verlaagt latency.
CERT	Een **CERT** (Computer Emergency Response Team) is een gespecialiseerd team dat beveiligingsincidenten detecteert, analyseert en coördineert om IT-systemen te beschermen tegen cyberdreigingen.

Afkorting / Term	Omschrijving
CJIB	Centraal Justitieel Incassobureau. Verantwoordelijk voor inning van boetes en financiële sancties.
Close-coupled koeling	Koeltechniek in datacenters waarbij koeling dicht bij de warmtebron wordt toegepast, zoals bij in-row of in-rack units, om luchtstromen te optimaliseren en energieverliezen te minimaliseren.
Cloud	Cloud is een model voor het leveren van IT-diensten via het internet, waarbij opslag, rekenkracht en applicaties draaien op externe datacenters in plaats van op lokale systemen. Gebruikers betalen meestal naar gebruik en profiteren van schaalbaarheid, flexibiliteit en beheergemak. Grote aanbieders van cloudinfrastructuur zijn onder andere Amazon Web Services (AWS), Microsoft Azure en Google Cloud Platform (GCP), ook wel bekend als hyperscalers.
Cloud Exchange	Geconsolideerde netwerkhub waar organisaties directe, veilige en snelle verbindingen kunnen maken met meerdere cloudproviders, wat latency verlaagt en prestaties en controle verbetert ten opzichte van publieke internetverbindingen.
CN	Het Caribische Nederland, ook wel de BES eilanden
Colocatie	Dienst waarbij klanten eigen apparatuur fysiek plaatsen in een gedeeld datacenter, inclusief stroom, koeling en netwerkvoorzieningen.
DNS (resolvers)	Domain Name System is het systeem dat internetdomeinnamen vertaalt naar IP-adressen. DNS-resolvers zijn de servers die deze vertalingen uitvoeren wanneer een gebruiker een website of dienst opvraagt. Lokale resolvers verbeteren snelheid en beschikbaarheid.
DUO	Dienst Uitvoering Onderwijs. Regelt o.a. studiefinanciering en onderwijsdata.
DC	Datacenter
Design-Build-Finance-Maintain (DBFM)	Contractvorm waarbij één partij verantwoordelijk is voor het ontwerp, de bouw, financiering en het onderhoud van een infrastructuurproject, vaak gebruikt bij publiek-private samenwerking om risico's en verantwoordelijkheden te bundelen.
DigiD	Digitale Identiteit. Authenticatiesysteem waarmee burgers veilig kunnen inloggen bij overheidsdiensten.

Afkorting / Term	Omschrijving
Diginetwerk	Gesloten netwerk dat veilige digitale communicatie mogelijk maakt tussen overheden.
Digitrale weerbaarheid	Digitale weerbaarheid is het vermogen van een organisatie of infrastructuur om bij digitale dreigingen de kerninformatie- en dienstverleningsprocessen in stand te houden, snel te reageren op incidenten en het normale functioneren te herstellen.
DPIA	Een Data Protection Impact Assessment is een verplicht privacyonderzoek dat wordt uitgevoerd wanneer een gegevensverwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen. Het brengt de risico's in kaart en beschrijft maatregelen om deze te beperken, in lijn met de eisen van de Algemene Verordening Gegevensbescherming.
DWDM	Dense Wavelength Division Multiplexing is een techniek waarmee meerdere datastromen tegelijk over één glasvezel worden verzonden via afzonderlijke lichtgolflengtes, om zo de capaciteit sterk te vergroten.
ECFS	East Caribbean Fiber System is een onderzeese glasvezelkabel die meerdere eilanden in het oostelijk Caribisch gebied met elkaar verbindt. De kabel is eigendom van een consortium van telecombedrijven en wordt gebruikt voor regionale en internationale connectiviteit.
Edge computing	Edge computing is een IT-architectuur waarbij data en rekenkracht zo dicht mogelijk bij de bron of gebruiker worden geplaatst, in plaats van in een centraal datacenter. Dit verlaagt latency, verbetert prestaties en is nuttig bij toepassingen zoals IoT of real-time videobewaking.
Eiland(en)	Geografische locatie, inbegrepen de lokale besturen, organisaties, bedrijven en burgers.
EN, E-NL of NL	Het Europese Nederland
Failover	Het automatisch overschakelen naar een back-up systeem of locatie wanneer de primaire dienst uitvalt, om continuïteit te waarborgen.
Fallback	Reservepad of alternatieve infrastructuur in een datacenter- of netwerkopzet die wordt gebruikt wanneer de primaire verbinding of dienst uitvalt, om beschikbaarheid en continuïteit te behouden.

Afkorting / Term	Omschrijving
Governance	Governance is het geheel aan structuren, processen en afspraken waarmee sturing, verantwoording en toezicht binnen een organisatie of project wordt vormgegeven, vaak gericht op transparantie, consistentie en risicobeheersing.
Hosting	Dienst waarbij IT-infrastructuur of applicaties voor klanten worden beheerd en beschikbaar gesteld vanuit een datacenteromgeving.
Hops	Hops zijn de tussenliggende netwerkpunten — zoals routers of knooppunten — waar dataverkeer doorheen moet reizen tussen de bron en de eindbestemming. Elke hop kan vertraging, risico op storing of interceptie toevoegen, vooral wanneer deze via netwerken in derde landen loopt.
Housing	Een datacenter waarbij faciliteiten zoals stroomvoorziening, koeling, netwerkverbindingen, brandbeveiliging en fysieke beveiliging geleverd wordt door het datacenter, maar het beheer van de apparatuur blijft in handen van de klant zelf. In de context van Caribisch Nederland betekent dit bijvoorbeeld dat overheden of semi-overheden hun eigen IT-apparatuur in een gedeeld rijksdatacenter kunnen plaatsen, zonder persé verplicht gebruik te maken van centrale hostingdiensten. (wel de mogelijkheid) Housing biedt hiermee autonomie over de eigen systemen, terwijl men profiteert van de robuuste en veilige infrastructuur van het datacenter.
Hybrid(e) Cloud	Combinatie van private en public cloudomgevingen, vaak aangevuld met on-prem infrastructuur, waarbij data en toepassingen flexibel tussen deze omgevingen kunnen bewegen afhankelijk van behoefte, kosten of regelgeving.
Internet of Things (IoT)	Netwerk van fysieke apparaten zoals sensoren, voertuigen en huishoudelijke apparaten die via internet gegevens uitwisselen en op afstand kunnen worden beheerd, vaak zonder menselijke tussenkomst.
In-row koeling	Koeltechniek waarbij airconditioningunits tussen de serverracks worden geplaatst om warme lucht direct bij de bron af te voeren, wat zorgt voor efficiënte koeling en energiebesparing binnen datacenters.
IP Transit	IP Transit is een dienst waarbij een netwerk via een internetprovider toegang krijgt tot het wereldwijde internet. De provider transporteert IP-verkeer namens

Afkorting / Term	Omschrijving
	de klant naar andere netwerken, meestal tegen betaling op basis van datavolume of capaciteit.
IPsec (tunnel)	Beveiligingsprotocol dat IP-verkeer versleutelt en authenticeert op netwerklaag, vaak gebruikt voor het opzetten van veilige VPN-verbindingen tussen locaties over het publieke internet.
IX of IXP	Internet Exchange. Een fysieke locatie waar netwerken van internetproviders en contentaanbieders verkeer met elkaar uitwisselen.
KvK	Kamer van Koophandel. Houdt onder meer het Handelsregister bij.
Latency	Vertraging in gegevensoverdracht, gemeten in milliseconden. Belangrijk bij netwerkprestaties, vooral over lange afstanden.
Legacy	Verouderde systemen of technologieën die nog in gebruik zijn maar niet meer voldoen aan moderne standaarden, vaak moeilijk te integreren of onderhouden.
Lifecyclebeheer	Proces van het plannen, implementeren, onderhouden, vervangen en uitfaseren van IT-middelen gedurende hun volledige levensduur, met als doel efficiëntie, veiligheid en kostenbeheersing.
MACsec	Media Access Control Security. Versleutelingstechnologie op laag 2 van het OSI-model voor beveiligde netwerkcommunicatie.
MeetMeRoom	Een fysieke ruimte in een datacenter waar netwerkproviders en klanten hun verbindingen direct met elkaar koppelen voor snelle en efficiënte fysieke koppelingen.
Multi-cloud	Gebruik van clouddiensten van meerdere aanbieders tegelijk, om afhankelijkheid van één leverancier te beperken en flexibiliteit, prestaties of compliance te verbeteren.
ODC	Overheidsdatacenter. Gecertificeerd datacenter in beheer of onder controle van de Nederlandse rijksoverheid.
OL (Openbaar Lichaam)	De lokale overheid op één van de BES-eilanden, tevens vertegenwoordigen zij de lokale organisaties met een publieke taak, waar zij een aandeel in hebben. Zoals o.a. ziekenhuizen, havens (lucht en zee), Water- en energiebedrijven etc.
On-prem(ise)	IT-voorzieningen die fysiek op locatie van de organisatie worden beheerd en gehost, in tegenstelling tot cloudgebaseerde oplossingen.

Afkorting / Term	Omschrijving
Peering	Afspraak tussen netwerkaanbieders om direct dataverkeer met elkaar uit te wisselen zonder tussenkomst van een derde partij, met als doel kostenreductie, lagere latency en hogere betrouwbaarheid.
PCCS	Pacific Caribbean Cable System is een onderzeese glasvezelkabel van circa 6.000 km die Zuid-Amerika, het Caribisch gebied en de Verenigde Staten met elkaar verbindt. De kabel is eigendom van een consortium, waaronder Orange, SETAR en Telefónica.
Point of Presence (PoP)	Netwerklocatie waar een organisatie fysieke verbinding maakt met het internet of andere netwerken. Een PoP bevat doorgaans netwerkapparatuur zoals routers, switches en soms caching-servers, en fungeert als toegangspunt tot een bredere infrastructuur.
Proprietary	Technologie, software of specificatie die eigendom is van een bedrijf en niet vrij beschikbaar of gestandaardiseerd, waardoor gebruik, koppeling of aanpassing beperkt kan zijn tot toestemming of licentie van de eigenaar.
PUE	Power Usage Effectiveness. Indicator voor energie-efficiëntie van een datacenter.
QoS	Quality of Service is een techniek in netwerken waarmee dataverkeer wordt geprioriteerd om prestaties te garanderen, bijvoorbeeld voor toepassingen die gevoelig zijn voor vertraging zoals spraak- en videocommunicatie.
Ransomware	Ransomware is kwaadaardige software die bestanden of systemen versleutelt en pas na betaling van losgeld (ransom) weer toegang verleent. Het vormt een ernstig beveiligingsrisico voor organisaties en overheden.
RCN	Rijksdienst Caribisch Nederland. De centrale vertegenwoordiging van de rijksoverheid op Bonaire, Sint Eustatius en Saba.
RDW	Rijksdienst voor het Wegverkeer. Beheert voertuiginformatie en -registraties.
Recursive Resolver	Een type DNS-server die namens de gebruiker volledige DNS-opvragingen uitvoert. De resolver zoekt stap voor stap naar het juiste IP-adres van een domeinnaam, beginnend bij de rootservers, en levert het eindresultaat terug aan de gebruiker. (Zie ook DNS)
Redundantie	Inrichting waarbij kritieke onderdelen van een systeem dubbel of meervoudig aanwezig zijn om uitval op te

Afkorting / Term	Omschrijving
	vangen en continuïteit van dienstverlening te waarborgen.
RON	Rijks Overheids Netwerk. Een infrastructuur die veilige en betrouwbare netwerkverbindingen biedt voor rijksorganisaties.
SBIR	Stichting Beheer ICT Rechtshandhaving is een Curaçaose non-profitorganisatie die ICT-oplossingen levert voor rechtshandhaving in het Koninkrijk der Nederlanden, waaronder Aruba, Curaçao, Sint Maarten én Caribisch Nederland (Bonaire, Sint Eustatius en Saba). Zij ontwikkelt, beheert en ondersteunt systemen zoals voor politie, justitie, marechaussee en andere ketenpartners binnen openbare orde en veiligheid
SCF	Southern Caribbean Fiber is een onderzeese glasvezelkabel van ongeveer 3.000 km die 15 eilanden in het oostelijke Caribisch gebied met elkaar verbindt. De kabel is eigendom van Southern Caribbean Fiber, een volledig dochtermaatschappij van Digicel Group.
Shadow IT	Gebruik van IT-systemen, applicaties of diensten binnen een organisatie zonder goedkeuring of toezicht van de centrale IT-afdeling, wat risico's kan opleveren op het gebied van beveiliging, compliance en beheer.
SIEM/SOC	Security Information & Event Management / Security Operations Center. Beveiligingssystemen voor monitoring, analyse en incidentrespons.
SSCS	Statia Saba Cable System is een onderzeese glasvezelkabel in eigendom van het Rijk die Sint Eustatius en Saba via St. Kitts verbindt met het bredere regionale netwerk. De kabel sluit ook aan op andere eilanden zoals Sint-Maarten en Saint-Barthélemy en vormt daarmee een belangrijke route voor internationale connectiviteit van de bovenwindse BES-eilanden.
SSC-ICT	Shared Service Centrum ICT. Rijksdienst die ICT-diensten levert aan ministeries en uitvoeringsorganisaties.
SSO-CN	Shared Service Organisatie Caribisch Nederland. Levert generieke diensten (zoals ICT, HRM) aan RCN en rijksdiensten op de eilanden.
Statia	Afkorting voor Sint Eustatius
Stretched Datacenter	Eén virtuele datacenteromgeving verdeeld over twee of meer fysieke locaties, waarbij systemen en data actief

Afkorting / Term	Omschrijving
	gesynchroniseerd worden voor hoge beschikbaarheid, failover en minimale uitvaltijd bij verstoringen.
Telemedicine	Telemedicine is het op afstand leveren van medische zorg en consultaties via digitale middelen zoals videoverbindingen, apps of online platforms, wat vooral waardevol is in geografisch afgelegen gebieden zoals Caribisch Nederland.
Throughput	Hoeveelheid data die binnen een bepaalde tijd succesvol door een netwerk of systeem wordt verwerkt, meestal uitgedrukt in Megabits per seconde (Mbps); geeft de werkelijke prestaties aan.
Twin-Datacenter	Een infrastructuuroptie waarbij twee datacenters geografisch gescheiden functioneren in een gekoppeld dienstverleningsmodel voor continuïteit en redundantie.
UPS	Uninterruptible Power Supply. Noodstroomvoorziening die bij stroomuitval tijdelijk elektriciteit levert doormiddel van accus.
Wavelength(s)	Afzonderlijke lichtgolflengtes op een glasvezel, gebruikt bij technieken zoals Dense Wavelength Division Multiplexing (zie ook DWDM) om meerdere datastromen gelijktijdig over één vezel te verzenden.
Workloads	IT-taken of processen die door systemen worden uitgevoerd, zoals applicaties, databases of rekenintensieve analyses, vaak gebruikt om capaciteit, prestaties of migratiebehoeften in te schatten.