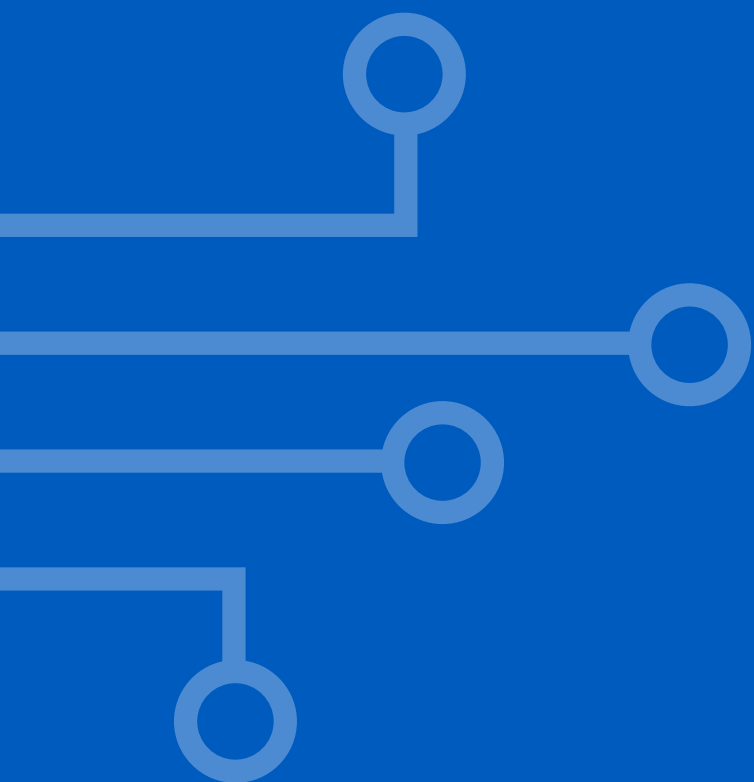




# Annex VII

# Transitiestrategie



# 1 Inleiding

Dit document bevat een Transitiestrategie, als overkoepelende en globale duiding van de manier waarop stap-voor-stap de beoogde situatie bereikt zou kunnen worden, vanuit de huidige situatie en de context van de organisatie en inrichting van de Aanbestedende dienst. Dit rekening houdend met de doelstellingen, risico's en beperkingen die daarbij relevant zijn.

## 1.1 Achtergrond

Deze Transitiestrategie hoort bij het Programma van Eisen. Het PVE beschrijft het 'wat' in termen van Diensten en functionaliteit, waar nodig aangevuld met (technische) specificaties als deze essentieel zijn voor het eindresultaat en de manier waarop diensten werken en worden afgenomen. De Transitiestrategie beschrijft in hoofdlijnen het 'hoe'.

## 1.2 Doelstelling

Het doel van deze Transitiestrategie is tweeledig:

- Gefaseerde, gecontroleerde overgang, waarbij de continuïteit van de bedrijfsvoering wordt gegarandeerd en risico's zoveel mogelijk beheerst worden
- Aansluiting bij / inbedding in ecosysteem van Diensten, werkzaamheden en verantwoordelijkheden van Aanbestedende dienst. Daarbij de toegevoegde waarde behouden en vergroten richting de afnemers van de Aanbestedende dienst.

Waar mogelijk en daar waar keuzes niet essentieel zijn voor het resultaat, wordt beoogd aan leveranciers vrijheid te geven bij de technische realisatie. Daarom wordt vanuit de Aanbestedende dienst geen invulling daaraan gegeven, maar wordt dit aan de eigenstandige verantwoordelijkheid van de leverancier overgelaten. De in dit document vastgelegde aanpak is bedoeld als voorstel, waarbij de positie van de Aanbestedende dienst verder concreet wordt gemaakt.

## 2 Fasering

Om grip te houden op de transitie stelt de Aanbestedende dienst voor om de overgang van Diensten van de on premises omgeving naar de Managed Private Cloud-omgeving uit te voeren in een aantal goed afgebakende stappen (fasen). Per fase is vastgelegd wat het beoogde resultaat is en wat de voorwaarden zijn om een begin te kunnen maken met een (op)volgende fase. Tevens is per fase op hoofdlijnen beschreven welke acties en werkzaamheden worden voorzien. Per activiteit is aangegeven wie (hoofd)verantwoordelijk is voor de uitvoering ervan.

### 2.1 Voorbereiding on premises

Momenteel beschikt de Aanbestedende dienst over twee datacenterlocaties: Soest en Doorn. In de huidige situatie is Soest de primaire locatie en Doorn de secundaire locatie (uitwijk). De inrichting van platformen en opslagvoorzieningen is grotendeels gelijk. Echter, op locatie Soest is beschikking over componenten voor aanvullende grafische rekenkracht (GPU's).

Het is de bedoeling dat na de transitie richting Managed Private Cloud op een van de locaties een beperkt aantal Diensten actief blijft. Hieronder zijn in ieder geval de diensten Interconnection gateway en Datadistributie, -inspectie en -filtering voor de veilige uitwisseling van dataverkeer met het internet en externe partijen. Dit geldt onder normale condities voor dataverkeer van en naar de kantoorlocaties van de organisaties die door de Aanbestedende dienst worden bediend en in geval van een uitwijksituatie voor alle verkeer van en naar internet en externe partijen.

Omdat de fysieke inrichting van de beschikbare ruimten in Doorn meer geschikt zijn, is het de wens om locatie Soest op te heffen en Doorn als colocation over te houden. Om de (extra) benodigde hardware tijdens de (volledige) transitieoperatie en daarna tot een minimum te beperken, is het de wens om apparatuur die (op termijn) vrijkomt uit Soest in te zetten op de locatie(s) van de Managed Private Cloudprovider. Daarvoor zijn verschillende opties, die bij de verdere uitwerking van de transitieplanning verder uitgewerkt moeten worden:

- Vrijmaken van apparatuur door redundante inrichting/configuraties enkelvoudig in te richten (*verantwoordelijkheid Aanbestedende dienst*).
- Vervangen van apparatuur op de op te heffen locatie door daar tijdelijk te huren apparatuur in te zetten (*verantwoordelijkheid Aanbestedende dienst*).

Resultaat van deze fase is het beschikbaar zijn van voldoende apparatuur/componenten voor de inrichting van het Kernplatform.

### 2.2 Inrichting virtualisatie-infrastructuur (landing zone)

Om er voor te zorgen dat de transitie van Diensten richting de Managed Private Cloud-omgeving verloopt zonder verstoringen voor de bedrijfsvoering is het van belang dat aan de volgende voorwaarden is voldaan:

- Connectiviteit vanuit de nieuwe Managed Private Cloud-omgeving met:
  - On premises datacenters
  - (Kantoor)locaties deelnemers Aanbestedende dienst
  - Het internet
  - Externe partijen (via GT Vaste Communicatie, DigiNetwerk)
- Mogelijkheid tot beveiliging van verkeersstromen van en naar de locatie(s) van de Managed Private Cloud-omgeving.
- Aanwezigheid van voorzieningen/componenten ten behoeve van Cyber Threat Intelligence-dienst (security monitoring).
- Platformen beschikbaar zijn voor het uitvoeren van Virtual Machines.
- Mogelijkheid om bestanden op te slaan.
- Voorzieningen beschikbaar zijn voor selfservicebeheer van de Aanbestedende dienst.

Voor het invullen van deze randvoorwaarden, dienen de volgende activiteiten uitgevoerd te worden:

- Opnemen van de locatie(s) van de Managed Private Cloud-omgeving in de glasvezelring van de Aanbestedende partij. De huidige (dark fiber)verbindingen worden geleverd door Eurofiber. Deze locatie(s) dient/dienen met (ten minste) twee bestaande locaties van de Aanbestedende dienst gekoppeld te worden, waarvan een de locatie Doorn betreft (*verantwoordelijkheid Inschrijver*).

- Inrichting colocatie op de locatie(s) van voor de plaatsing van apparatuur van de Aanbestedende dienst (*verantwoordelijkheid Inschrijver*).
- Plaatsing en configuratie apparatuur op colocatie (Lijst met apparatuur is op aanvraag verkrijgbaar). (*verantwoordelijkheid Aanbestedende dienst*).
- Uitbreiding van de netwerkkzones in de on premises datacenters (VLAN's) door configuratie streched VLAN's met behulp van VXLAN (*verantwoordelijkheid Aanbestedende dienst*).
- Realisatie van toegang tot internet en configuratie van BGP voor redundante toegang. Hierbij wordt gebruik gemaakt van het AS-nummer en de publieke IP-reeksen die Aanbestedende dienst ter beschikking heeft (*verantwoordelijkheid Aanbestedende dienst*).
- Inrichten hypervisorplatform(en) voor het uitvoeren van virtuele machines en het koppelen van de netwerkkzones aan de firewalls in de colocatie (*verantwoordelijkheid Inschrijver*).
- Inrichten voorzieningen voor bestandsopslag (*verantwoordelijkheid Inschrijver*).
- Inrichten Selfserviceportaal (*verantwoordelijkheid Inschrijver*).

Wanneer het kernplatform met bijbehorende voorzieningen en interconnectiviteit is gerealiseerd en getest, kan de volgende fase van de transitie worden ingegaan, de as-is-migratie.

De inrichting van het kernplatform raakt de volgende diensten, zoals vastgelegd in het PvE:

- Housing
- Datatransport (connectiviteit tussen IT-componenten, zoals applicaties, platformen et cetera).
- Datadistributie, -inspectie en -filtering (data-uitwisseling tussen netwerkkzones, beveiligd door inspectie en filtering)
- Interconnection gateway (koppelvlak voor verbindingen met externe netwerken/partijen)
- VM-Hosting (platform voor uitvoering van virtuele machines)
- Bestandsopslag (opslag van ongestructureerde data/bestanden)
- Selfserviceportaal (aanvraag/creatie virtuele platformen en andere componenten, rapportage)

## 2.3 As-is-migratie virtuele machines en bijbehorende data

Met de as-is-migratie worden alle virtuele machines uit de on premises-omgeving overgebracht naar de Managed Private Cloud-omgeving, waarbij de huidige inrichting voor Disaster Recovery middels een extra locatie wordt opgeheven en platformen worden geconsolideerd. De migratie wordt stapsgewijs uitgevoerd, waarbij rekening wordt gehouden met afhankelijkheden tussen workloads, zoals bij elkaar horende voorzieningen voor applicatiehosting en datamanagement (*verantwoordelijkheid Aanbestedende dienst*):

- Testsystemen Aanbestedende dienst
- Testsystemen deelnemers Aanbestedende dienst
- Applicaties en (ondersteunende) diensten van de Aanbestedende dienst
- Productieworkloads Aanbestedende dienst

Onderdeel van de as-is migratie is tevens de migratie van data die is opgeslagen op de centrale storageomgeving van de Aanbestedende Dienst in de vorm van netwerkshares (NAS / shared folders).

De migratie wordt stapsgewijs uitgevoerd, waarbij rekening wordt gehouden met:

- Migratie van bestanden inclusief mappenstructuur en metadata.
- Behoud van toegangsrechten (ACL's), inclusief gebruikers- en groepsrechten.
- Waarborgen van data-integriteit en volledigheid tijdens en na de migratie.
- Ondersteuning van incrementele synchronisatie (delta-migratie) om de uiteindelijke migratie-impact te beperken.
- Validatie en controle op juistheid en volledigheid van de gemigreerde data.

Bij de migratie wordt downtime van applicaties zoveel als mogelijk gereduceerd, onder andere door gebruik te maken van bestaande uitwijkmechanismes, indien passend en mogelijk.

Bij de migratie wordt de licentiestructuur herzien: Licenties voor besturingssystemen worden afgenomen van de Inschrijver op basis van de fysieke onderliggende infrastructuur die de virtuele machines uitvoert (*verantwoordelijkheid Inschrijver op basis van aanvragen Aanbestedende dienst*).

De migratie dient uiterlijk 1 juli 2027 afgerond te zijn, zodat alle (hardware)componenten in de on premises-omgeving buiten gebruik gesteld kunnen worden (in verband met aflopende supportcontracten).

De inrichting van de virtualisatie-infrastructuur raakt de volgende diensten, zoals vastgelegd in het PvE:

- VM-Hosting (platform voor uitvoering van virtuele machines)
- Datatransport (connectiviteit tussen IT-componenten, zoals applicaties, platformen, et cetera)
- Bestandopslag (opslag van ongestructureerde data/bestanden)
- Raw storage (bieden van volumes voor blokopslag of blobopslag)
- Data recovery (middelen voor dataherstel na incidenten/calamiteiten)
- Selfserviceportaal (aanvraag/creatie virtuele platformen en andere componenten, rapportage)
- Datatransport (connectiviteit tussen IT-componenten, zoals applicaties, platformen et cetera).
- Datadistributie, -inspectie en -filtering (datauitwisseling tussen netwerkzones, beveiligd door inspectie en filtering).

## 2.4 Transformatie

Wanneer de virtualisatie-infrastructuur is ingericht en de virtuele machines (in samenhang) succesvol gemigreerd zijn, is het mogelijk om een verdere herinrichting uit te voeren. Deze herinrichting richt zich op het meer en meer afnemen van Diensten van de Managed Private Cloud-leverancier. Het gaat onder andere om de volgende Diensten:

- Datamanagement (Oracle en SQL-databases als dienst)
- Workload Hosting (runtime-omgevingen op basis van volledig beheerde platformen)
- Service Access Control (beveiligde toegang tot back-end applicaties)

Er is geen vastomlijnd tijdspad of specifieke volgorde waarin de transformatie richting afname van Diensten ingevuld moet worden. Bij een transformatie richting een Dienst zijn wel een aantal randvoorwaarden:

- Diensten dienen te voldoen aan de eisen zoals gesteld in het Programma van Eisen.
- De uitrol en/of ingebruikname van instanties van Diensten dient geautomatiseerd plaats te vinden, inclusief registratie van instanties in de CMDB van de Aanbestedende dienst
- De (werking van een) Dienst dient ingebed te worden in servicemanagement- en beheerprocessen van de Aanbestedende dienst, inclusief het (zoveel mogelijk) geautomatiseerd afhandelen van meldingen, wijzigingen en rapportage, met gebruikmaking van de servicemanagementapplicatie van de Aanbestedende dienst.

De uitvoering van deze fase gebeurt in nauwe samenwerking tussen Aanbestedende dienst en Inschrijver.