Cloud- en Datacenterdiensten

1 CLOUD- EN DATACENTERDIENSTEN 5

1.1 ALGEMENE OMSCHRIJVING 5
1.2 ALGEMENE KENMERKEN 8
1.3 ALGEMENE OMSCHRIJVING ONDERSTEUNENDE PROCESSEN VOOR DIT DIENSTENPAKKET 9

2 CLOUD 12

2.1 SPECIFIEKE OMSCHRIJVING 12
2.2 MEERWAARDE VOOR DE KLANTEN 12
2.3 GEVRAAGDE KENMERKEN 13
2.4 OMSCHRIJVING VERDERE CONCRETISERING VAN DE ONDERSTEUNENDE PROCESSEN VOOR CLOUD DIENSTEN 16
2.4.1 Minimaal beheer 16
2.4.2 CloudOps beheer 19
2.4.3 Traditioneel beheer 21
2.4.4 Overzicht types beheer 21
2.4.5 Algemene beschrijving van de ondersteunende processen 23
2.4.6 Beschrijving van de ondersteunende processen en tools specifiek voor Cloud diensten 27
2.4.7 Continu versiebeheer (CloudOps/traditioneel): 33
2.5 OVERZICHT VAN DE CLOUD 34
2.5.1 Exploitatie 34
2.5.2 Eenvoudige Werkaanvragen 41

3 MANAGED DATACENTER 43

3.1 SPECIFIEKE OMSCHRIJVING 43
3.2 MEERWAARDEN VOOR DE KLANTEN 44
3.3 GEVRAAGDE KENMERKEN 45
3.3.1 Het managed DC 45
3.3.2 De managed DC dienstverlening 53
3.3.3 Het bestaande Managed DC – VPC Mechelen 60
3.4 INTERFACES MET ANDERE DIENSTENPAKKETTEN 61
3.4.1 Applicaties 61
3.4.2 Netwerken 64
3.4.3 Service desk en SIEM 66
3.4.4 Werkplekken 66
3.4.5 Mainframe 66
3.5 OMSCHRIJVING VERDERE CONCRETISERING VAN DE ONDERSTEUNENDE PROCESSEN 66
3.5.1 Incident Management: 66
3.5.2 Problem Management: 67
3.5.3 Subcontractmanagement: 67
3.5.4 Event Management: 67
3.5.5 Capacity management: 67
3.5.6 Availability management: 67
3.5.7 Configuratiebeheer: 68
3.5.8 Beveiligingsbeheer: 68
3.5.9 Log management 69

3.5.10 Packaging en Delivery ... 69
3.5.11 Exploitatiedossier ... 70
3.5.12 Continu versiebeheer: ... 70
3.6 SLA EN PRIJSMECHANISME ... 70
3.6.1 De dienst wordt geconcretiseerd door ... 70
3.6.2 SLA ... 71
3.6.3 Prijsmechanisme ... 74
3.6.4 Eenvoudige Werkaanvragen ... 85

4 DATACENTER OUTSOURCING ... 96

4.1 OMSCHRIJVING ... 96
4.2 MEERWAARDEN VOOR DE KLANTEN ... 96
4.3 SPECIFIEKE KENMERKEN ... 97
4.4 OVERZICHT VAN DE DC OUTSOURCING ... 97
4.4.1 Exploitatie ... 97
4.4.2 Eenvoudige Werkaanvragen ... 100

5 COMPUTERZAAL FACILITEITEN (CZF) ... 101

5.1 OMSCHRIJVING ... 101
5.2 MEERWAARDEN VOOR DE KLANTEN ... 101
5.2.1 Het beheren van computerzaalcapaciteit CZF ... 102
5.2.2 Het beschikbaar stellen van professioneel beheerde computerzaalcapaciteit CZF (inclusief stroomverbruik en koeling) ... 103
5.3 OVERZICHT VAN DE CZF ... 105
5.3.1 Exploitatie beheer van computerzalen ... 105
5.3.2 Exploitatie ter beschikking stellen van professioneel beheerde computerzalen ... 106
5.3.3 Eenvoudige Werkaanvragen computerzaalfaciliteiten ... 108

6 ONDERSTEUNING IN REGIE M.B.T. CLOUD- EN DATACENTERDIENSTEN ... 110

6.1 SCOPE EN DOEL ... 110
6.2 GECONCRETISEERD DOOR ... 110
6.3 PRIJSMECHANISME ... 111
6.4 FACTURATIE ... 111
6.5 RAPPORTERING ... 111

7 INFRASTRUCTUURPROJECTEN M.B.T. CLOUD- EN DATACENTERDIENSTEN ... 112

7.1 SCOPE EN DOEL ... 112
7.2 GECONCRETISEERD DOOR ... 114
7.3 UITVOERING ... 115
7.3.1 Werkaanvraag voor opmaken van een Projectvoorstel ... 115
7.3.2 Werkaanvraag voor uitvoering van een Project of Projectfase ... 116
7.3.3 Werkaanvraag voor de bestelling van een projectwijziging ... 117
7.4 SLA ... 118
7.4.1 Tijdige uitvoering van Projecten ... 118
7.5 PRIJSMECHANISME ... 119
7.6 PRIJSCORRECTIE ... 121

7.7 FACTURATIE 121
7.8 RAPPORTERING 121

8 TRANSITIE 123

8.1 INITIËLE TRANSITIE 123
8.2 DEELTRANSITIE TIJDENS DE DUUR VAN DE OVEREENKOMST 125

9 EXIT 126

9.1 MAATREGELEN BIJ HET BEËINDIGEN VAN DE OVEREENKOMST 126
9.2 DEELEXIT TIJDENS DE DUUR VAN DE OVEREENKOMST 127

1 Cloud- en Datacenterdiensten

1.1 Algemene omschrijving

Dit dienstenpakket omvat applicatie- en systeem ondersteunende faciliteiten zoals Infrastructuurdiensten, platformdiensten, datacenter dienstverlening etc die de Klanten en/of de door de Klanten ingeschakelde applicatie-dienstverleners nodig hebben om het operationeel beheer (‘run’) van hun applicaties te kunnen uitvoeren.

De dienstverlening die dient te worden geleverd binnen dit dienstenpakket moet de Klant in staat stellen om basis IT-Infrastructuurdiensten af te nemen van een professionele organisatie die schaalvoordelen en goede praktijken kan aanwenden om op ieder moment tot een optimale prijs te komen en de ‘total cost of ownership’ (TCO) voor de Klant te reduceren.

Het doel is dat Klanten - door gebruik te maken van dit dienstenpakket - hun applicaties operationeel kunnen beheren of laten beheren door een applicatieve Dienstverlener. Daartoe dienen alle hiervoor vereiste onderliggende platformen, infrastructuur, computerzalen beschikbaar en toegankelijk gehouden te worden met het gepaste niveau van beschikbaarheid, performantie en veiligheid.

Deze dienstverlening bestaat uit traditionele housing, hosting en diensten (beheer van bestaande computerzalen/datacenters in de Vlaamse overheid) en ook cloud-based dienstverlening (brokering van cloud-based ICT-diensten, zowel infrastructuur als platformen en ondersteunende functionaliteiten.).

De gevraagde DC dienstverlening dient te kunnen worden aangeboden zowel vanuit een DC outsourcing/managed DC/CZF als via publieke cloud-providers op dusdanige wijze dat de cloud-first strategie van VO-Klanten kan gefaciliteerd en gerealiseerd worden en waarop de klanten kunnen beroep doen en ‘as a service’ kunnen afnemen in functie van hun noden.

HFB wenst via de Overeenkomst een breed aanbod van datacenterdiensten op te zetten dat bestaat uit:

1. **Cloud diensten** : deze vormen de primaire optie en genieten de voorkeur, in lijn met de VO cloud strategie die een ‘cloud first’ principe vooropstelt. Dit houdt in dat standaard aanvragen voor IAAS/ PAAS diensten ‘by default’ beantwoord worden met diensten vanuit hyperscale public cloud. De VO cloud strategie is geen ‘cloud-only’ strategie. Andere opties, zoals een “managed DC” of outsourced DC of ComputerZaal Faciliteiten (CZF) blijven ook mogelijk (na een gegronde evaluatie)
2. **Managed DC diensten**: vanuit een behoefte aan continuïteit zal in tweede prioriteit ook nog gebruik worden gemaakt van traditionele **managed DC diensten**; dit betreft een dienst van een externe partij welke onderliggend gebruik kan maken van shared infrastructuur met andere klanten. Binnen het managed DC worden twee types van diensten onderscheiden:
    a. IAAS / PAAS diensten in het bestaande datacenter VPC Mechelen van DXC – in functie van continuiteit van bestaande toepassingen – beperkt in de tijd;
    b. IAAS / PAAS diensten in het nieuwe DC van P3;
3. **Housing/CZF diensten**: Hier voorzien we twee vormen van dienstverlening
    a. Een colocatie dienst die bestaat uit een CZF faciliteit van de P3 leverancier. Deze omvat het gebouw, fysieke beveiliging, stroomvoorziening, koeling, kooi en evt ook racks, databekabeling en patching en “remote hands”, hands&eyes. Bij voorkeur op

basis van dezelfde computerzaal faciliteit die onderliggend is aan de managed DC dienst, zodat applicaties op beide diensten dezelfde DC-locatie delen, wat een aantal specifieke platformintegraties, alsook connectiviteit naar het netwerk van de VO mogelijk maakt.

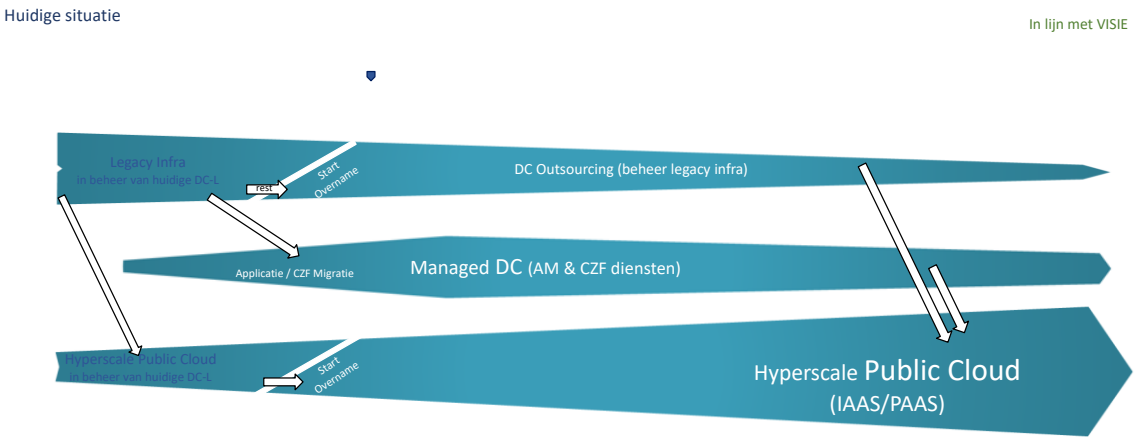
b. Een colocatie dienstverlening die steunt op een CZF faciliteit van de VO, buiten dit contract. Deze diensten omvatten “remote hands”, hands&eyes, contractbeheer, fysieke beveiliging enz…

c. Voor deze laatste categorie van DC’s is de visie om het aantal (voornamelijk) decentrale datacenters en computerzalen terug te schroeven vanuit het beleid om geen decentrale computerzalen in kantoorgebouwen te ondersteunen. Waar er een restcapaciteit aan eigen-computerzaal nodig blijft, wordt een gecentraliseerde externe CZF dienst gepromoot, die beantwoordt aan de vereisten rond duurzaamheid en connectiviteit met de VO netwerk backbone

4. **DC outsourcing diensten**: in derde prioriteit, en eveneens vanuit de behoefte aan continuïteit, kan ook nog gebruik worden gemaakt van VO-eigen DC’s. Het betreft hier klant-eigen DC infrastructuur, welke in beheer wordt genomen door de DC/Cloud dienstverlener..

Deze omgevingen moeten ten allen tijde veilig en GDPR (AVG) conform bruikbaar zijn. De verschillende types van DC dienen een implementatie te ondersteunen van alle vereisten van het VO veiligheidsbeleid, met inbegrip van de volledige netwerkbeveiliging, encryptie van Data at Rest (DAR) en encryptie van Data in Motion (DIM) met encryptiesleutels in beheer van HFB.

Het volgende schema geeft ‘eerder generiek’ de CMO – FMO roadmap weer waarbij de drie gevraagde types datacenter dienstverlening worden weergegeven (DC-outsourcing, managed DC en hyperscale public cloud). Hoe verder naar Future mode Of Operation (FMO) toe hoe verder DC outsourcing en Managed DC zullen kunnen worden afgebouwd ten gunste van groei in hyperscale public cloud.



Meer informatie aangaande de VO Datacenter visie rond continuïteit en de huidige (voornamelijk) gevirtualiseerde en X86-gebaseerde server infrastructuur kunnen teruggevonden worden in de referentie bibliotheek. Continuïteit zal op meerdere manieren kunnen gerealiseerd worden: door verder af te nemen van bestaande DC diensten of door migratie naar een managed DC of public cloud.

Continuïteit van de huidige (en voornamelijk dan 'legacy' ICT toepassingen) zal bovendien ondersteund worden, door het toepassen van een hybride DC/cloud architectuur. De DC/Cloud ICT-Dienstverlener zal een hybride omgeving beschikbaar stellen en houden waarop de Klanten kunnen beroep doen en 'as a service' kunnen afnemen in functie van hun noden.

Een hybride DC/cloud architectuur houdt in dat het volledige dienstenaanbod naast publieke cloud ook een "managed DC" dienst omvat en daarnaast ook diensten voor "DC outsourcing" en CZF voor realisatie van een VO-eigen DC omvat; daarnaast is er uiteraard ook de belangrijke en vaak eerste optie om SAAS applicaties toe te passen.

De integratie tussen de applicaties in de verschillende hosting locaties is hierbij een zeer belangrijk aandachtspunt, evenals de beheersaspecten op vlak van applicatie deployment, operationeel beheer, securitybeheer, enz… en andere aspecten zoals personeel en competenties, veranderingsbeheer, enz. Een entiteit zal hierbij de keuze maken die best aan zijn vereisten beantwoordt, rekening houdend met bovengenoemde aspecten.

De infrastructurele en platformdiensten worden maximaal as a service, tegen gekende voorwaarden en prijs, als managed service geleverd, dus ook met garanties van de nodige Service Levels zoals verder gevraagd in dit portfoliodocument.

Dit dienstenpakket moet kunnen worden aangewend in functie van de noden door de Klanten en de door de Klanten ingeschakelde Dienstverleners (applicatieve Dienstverleners). De applicatie Dienstverleners zullen verplicht worden om beroep te doen op de DC/Cloud dienstverlening mbt de benodigde infrastructuur- en platformen die nodig zijn om de applicatiesoftware te ontwikkelen en te draaien. Dit om informatieverspreiding en DC gerelateerde integratie en (security) governance binnen de perken te houden. De applicatie Dienstverleners zullen slechts zelf in bepaalde mate (uitzonderlijk) specifieke platform services of componenten inbouwen in de toepassing, een structureel aanbod van dergelijke services of bouwstenen dient dus steeds door de DC/cloud dienstverlener te worden voorzien.

Minstens voor de cloud-gebaseerde datacenterdiensten, maar waar mogelijk ook voor de traditionele datacenterdiensten, zullen interfaces aangeboden worden met het oog op o.a. "automated deploy" en "DevOps".

De datacenter dienstverlening houdt ook in:

- Adviesverstrekking obv knowhow en specialisatie in het domein, kennisdeling, informatieverstrekking, ondersteunen bij afhandeling van problemen of incidenten, …
- Regieprestaties op vraag van klanten, ter ondersteuning
- Projecten (infrastructuurgericht) voorbereiden en realiseren op vraag van klanten
- Brokering incl. contract management (afsluiten en beheren van contracten met onderaannemers of leveranciers van fysieke computerzaaldiensten, hard- en software voor zowel traditionele datacenterinfrastructuur als voor publieke cloudinfrastructuur (Iaas, PaaS en SaaS)
- Het beveiligingsbeheer m.b.t. de beheerde infrastructuur ifv het type dienst (fysieke computerzaal, servers, storage, netwerk- en beveiligingsinfrastructuur in het datacenter en in de publieke cloud, …) en de gekoppelde beveiligingsdiensten in lijn met de wettelijke en algemene ICT-veiligheidsrichtlijnen van de Vlaamse overheid. Dit kan o.m. bestaan uit volgende diensten:

- Bescherming tegen cybercriminaliteit via de uitbating en controle van veiligheidsbouwstenen
- Het voorzien van de nodige beveiligingsmaatregelen tegen aanvallen van buiten de organisatie, maakt deel uit van deze Diensten. Hieronder valt ook het beschermen tegen cybercriminaliteit en malware.
- De nauwe samenwerking met het Facilitair Bedrijf en de externe SIAM-dienstverlener (integratie) op het vlak van risico management & incident response (SOC, SIEM, ..)

De dienstverlening voorziet tevens een roadmap voor de toekomstige evolutie(s) op het vlak van de Cloud- en datacenter dienstverlening die jaarlijks ter beschikking zal gesteld worden, zodat alle betrokkenen er tijdig kunnen op inspelen.

De Cloud- en Datacenterdiensten omvatten niet alleen de infrastructuur- en platform diensten voor de “productie”-omgevingen; maar ook voor de non-productie omgevingen (ontwikkeling, test, integratie, proeftuin, opleiding …);

Het doel van proeftuinen, hiervan is om innovatie te versnellen of om toekomstige noden te capteren om innovatie uit te lokken, al dan niet via Sandbox Vlaanderen

De verschillende types van datacenters dienen toegankelijk te zijn zowel vanuit het internet als vanuit het private netwerk/backbone van de VO.

Het moet mogelijk zijn voor de Klantenteams om toegang te krijgen tot de eigen (virtuele) infrastructuur en platformen, hetzij voor eigen gebruik, hetzij om toe te laten aan derden om van op afstand bepaalde exploitatiehandelingen uit te voeren.

Het bestelproces (van aanvraag tot facturatie) voor de onboarding en aankoop van Datacenterdiensten dient snel, flexibel en transparant te zijn voor de Klant. Er wordt voor gezorgd dat de Klant via rapportering en via het centrale bestelportaal in Perceel 1 (service integrator), steeds een actueel en accuraat zicht heeft op de status van zijn bestellingen en op de kosten voor hosting en voor opzet van infrastructuur en platformen.

Alle types DC diensten dienen operationeel te zijn 24 uur per dag, 7 dagen per week, 52 weken per jaar (in het bijzonder voor computerzaaldiensten is er 24*7*52 werking zonder onderbreking).

1.2 Algemene kenmerken

De gevraagde kenmerken kunnen meer in detail teruggevonden worden in het DC/Cloud visie document (referentie bibliotheek). Deze worden als volgt samengevat:

- de voorgestelde oplossingen onderschrijven de VO Cloud visie en de te verwachten evolutie naar Cloud;
- ondersteuning van multi-tenancy met aandacht voor een aanvaardbare technische complexiteit en rekening houdend met eventuele beperkingen bv. opgelegd door voorwaarden van onderliggende Cloud providers;
- optimale toepassing van automatisering naargelang de mogelijkheden van het type DC dat wordt aangewend;
- werkbare dienstverlening in een multi-leveranciers context op basis van maximaal mogelijke automatisatie aangevuld met gestandaardiseerde service request (SIAM);

- werkbare dienstverlening met voldoende autonomie, modulariteit en segregatie per entiteit
- bevatten alle benodigde beveiligingsmaatregelen in lijn met het VO informatie classificatie raamwerk van toepassing op alle type DC diensten;
- beveiligde connectiviteit naar het Internet;
- connectiviteit naar het netwerk van de VO (Managed DC);
- mogelijkheid tot het gebruik van private VO IP adres-ruimten in Managed DC en Cloud DC's;
- aantrekkelijke instapdrempel (competitief prijsniveau) voor een geïnteresseerde Klant

1.3 Algemene omschrijving ondersteunende processen voor dit dienstenpakket

De algemene procesvereisten zijn opgenomen in het contractuele document “Vereisten ondersteunende processen en overlegfora”. Hieronder zijn meer gedetailleerde vereisten opgenomen specifiek voor het Dienstenpakket ‘Cloud- en Datacenterdiensten’.

De Cloud- en Datacenter ICT-Dienstverlener zal moeten afstemmen met de ICT-Dienstverlener die de integratiediensten levert in het kader van deze Overeenkomst. De Cloud- en Datacenter ICT-Dienstverlener zorgt samen met de ICT-Dienstverlener voor de Integratiediensten voor een vlotte samenwerking m.b.t. processen, procedures en tools (bv. Interfacing tussen de tools voor afhandelen van Incidenten en Problemen, het Klachtenbeheer, Communicatiebeheer, SLA rapportering, ...). Daarnaast dient de Cloud- en Datacenter ICT-Dienstverlener ook samen te werken met de ICT-Dienstverleners voor andere dienstenpakketten.

De nodige processen en procedures voor de nodige samenwerking en interactie met de integratie-diensten, inclusief servicedesk & overkoepelende security diensten moeten opgenomen worden in de Serviceorganisatie. Zo moeten vanuit dit dienstenpakket de nodige kennisartikelen en scripts aangeleverd worden aan de overkoepelende eerstelijns servicedesk zodat incidenten zo goed mogelijk in eerste lijn kunnen opgelost worden en indien dit niet mogelijk is, correct kunnen toegewezen worden aan de juiste tweede lijn.

De Vlaamse overheid zet in op duurzaamheid. De ICT-dienstverlener beschrijft in de serviceorganisatie hoe hij invulling geeft in de processen om een ICT-Dienstverlening te realiseren die rekening houdt met maatschappelijk en ethisch verantwoord en/of duurzaam ondernemen.

Vanuit dit dienstenpakket moeten afstemming gebeuren i.v.m. de nodige datastromen naar een overkoepelende 'Security Information and Event Management' (SIEM) die deel uitmaakt van de Integratiediensten.

Volgende aspecten behoren tot de scope van de Cloud- en Datacenter diensten:

- De tweede lijn Service Desk voor het oplossen van Incidenten en Problemen m.b.t. de Cloud- en Datacenter diensten (Incident management). De eerste lijn Service Desk zit bij de ICT-dienstverlener voor de Integratiediensten. De Cloud- en Datacenter ICT-Dienstverlener geeft de gepaste prioriteit aan de Incidenten die via de eerste lijn doorgegeven worden of die automatisch gegenereerd worden via alarmen uit de monitoring tools, om de voor de diensten beschreven SLA’s te realiseren. Dit omvat eveneens het voorzien van een wachtdienst voor het garanderen van de overeengekomen dienstverleningsniveaus.

- Het oplossen van Problemen in het kader van de Cloud- en Datacenter diensten d.m.v. “proactief probleembeheer” o.b.v. monitoring. Verder voert de Cloud- en datacenter ICT-dienstverlener een 'root cause analyse' (RCA) uit, voert de nodige Correctieve acties uit en legt Proactieve Verbetervoorstellen voor aan de Klant. (Problem management).
- Voorstellen doen en adviezen geven in het kader van het opstellen van een roadmap voor het dienstenpakket Cloud- en Datacenter diensten in het kader van Service Portfolio Management.
- De monitoring van de voor de Cloud- en Datacenter diensten onderliggende infrastructuurcomponenten.
- Het correct houden van de Configuratiedatabank m.b.t. de Cloud en Datacenter diensten
- Beheer van de configuratiecomponenten m.b.t. de licenties en contracten die gebruikt worden voor Cloud- en Datacenterdiensten. Het Configuratiebeheer m.b.t. softwarelicenties moet o.a. toelaten om na te gaan of het reële gebruik in overeenstemming is met de verworven licenties. Er dient steeds een overzicht beschikbaar te zijn over welke licenties men beschikt. Afhankelijk van het type licentie, moet de relatie met een gebruiker (voor gebruikersgebonden licenties), met een server of een CPU (voor server- of CPU-gebonden licenties), etc. bijgehouden worden.
- M.b.t. het proces “Beheer van sub-contracten en aankoop” : Het afsluiten (en tijdig verlengen/actualiseren) van de nodige (onderhouds-) contracten om de Cloud- en datacenter diensten te realiseren.
- Het proces “Beheer sub-contracten en aankoop” omvat onder meer ook het licentiebeheer dat de administratieve lasten voor de Klanten moet helpen verlagen door integraal dit beheer over te nemen, terwijl de DC-Dienstleverancier er ook over zal waken dat zowel het risico op ongeautoriseerd gebruik van software als de kost van suboptimaal gebruikte software tot een minimum worden herleid. Het licentiebeheer omvat verder ook
    - beheer van de licentiegegevens m.b.t. software zodat de Configuratiedatabank m.b.t. deze licentiegegevens steeds accuraat blijft. Afhankelijk van het type licentie wordt de gepaste informatie bijgehouden om o.a. de overeenstemming tussen verworven licenties en het gebruik ervan te kunnen aantonen. Zo zal bv. voor licenties die “gebruiker”-gebaseerd zijn, bijgehouden worden welke gebruikers over een licentie beschikken en zal voor licenties die “CPU”-gebaseerd zijn, bijgehouden worden voor welke CPU’s er een licentie is. De Cloud- en Datacenterdienstverlener dient de naleving van de licentievoorwaarden binnen de door hem geleverde Diensten te kunnen aantonen bij eventuele audits door de betrokken softwarefabrikanten en ondersteuning te bieden bij deze audits, zowel voor wat betreft licenties aangekocht door de DC-Dienstleverancier als voor wat betreft licenties die, in overleg met de Cloud- en Datacenterdienstverlener, aangekocht zijn door de Klant zelf
    - De nodige informatie en sturing te verschaffen aan de Klant met betrekking tot de lopende contracten, betalingen en hernieuwingen om zo een optimale compliance met de contractuele verplichtingen t.a.v. de licentiegevers te ondersteunen;
    - Monitoring van het eigenlijke gebruik van software onder licentie om bij onderconsumptie de toekomstige afname beter af te stemmen op dit gebruik;
    - Stelselmatig input verschaffen over mogelijke optimalisaties in de licentie portefeuille, waarbij het inruilen van een eigen licentie door de Klant voor een Licentie as a Service aangeboden door de DC-Dienstleverancier steeds mogelijk moet zijn
- De Cloud- en datacenterdienstverlener dient o.a. ten behoeve van de toepassingen een aantal onderliggende platformen (middleware zoals RDBzMS, webservers, applicatieservers, …) te

beheren samen met de bijhorende contracten, welke al dan niet VO-specifiek kunnen zijn. Deze platformen zijn in veel gevallen gemeenschappelijk voor meerdere toepassingen en klanten. De Cloud- en datacenterdienstverlener dient alle kosten (inclusief alle contractkosten waarbij eventuele kortingen toegepast worden) correct te versleutelen en te factureren aan de betrokken klanten

- Het bijwonen van operationele overlegfora met HFB om de processen, procedures en ICT-dienstverlening m.b.t. de Cloud- en datacenter diensten continu te optimaliseren.
- Facturatie van de applicatie ondersteunende infrastructuur, Cloud en/of DC diensten dient versleuteld te worden naar de klanten o.b.v. een correcte verdelingssleutel. Dit is een administratieve taak voor de Cloud en DC dienstenleverancier. Het is de Cloud en DC dienstenleverancier toegelaten om alternatieven voor te stellen die (kosten-)efficiënter zouden kunnen zijn voor de klanten, zolang de functionaliteiten van de alternatief tegemoetkomt aan de eisen van de klant en rekening houdt met business contiuniteit. De facturatie en versleuteling van de kosten moet rekening houden met eventuele kortingen en ook de kortingen moeten correct versleuteld worden per factuur naar de betrokken klant.

2 Cloud

2.1 Specifieke omschrijving

Hyperscale public Cloud diensten zijn voor de VO de aangewezen en realistische optie om de DC (IAAS en PAAS) diensten te bekomen die vereist zijn om te beantwoorden aan de business drivers en ICT vereisten, en om de applicaties te kunnen bouwen, in productie brengen en operationeel beheren zoals dit door de business zal vereist worden. Nieuwe applicaties die op maat gemaakt worden, zullen in eerste instantie als een Cloud-native toepassing ontwikkeld worden op basis van Cloud IAAS/PAAS diensten terwijl functionaliteit die breed in de markt toegepast wordt voornamelijk steunen op een aanbod van Cloud SAAS diensten.

Er zal een Multi-Cloud worden aangeboden zodat entiteiten individueel telkens de meest efficiënte en geoptimaliseerde keuze kunnen maken.

Multi-Cloud dient hier niet gezien te worden als een expliciete verplichting voor de ICT-Dienstverlener om te investeren in een overkoepelend framework van tools en diensten die agnostisch werken boven alle type datacenters heen (t.o.v. de native tooling, webconsole en API's van Cloud providers), zoals voor bv ontwikkeling en deployment van applicaties, voor het overkoepelend beheer ervan, het veiligheidsbeheer ervan, enz., De interfaces met de VO (SIAM) dienen echter wel gestandaardiseerd en gerespecteerd ongeacht het type datacenter wat erachter zit. Met overkoepelende diensten wordt bedoeld public Cloud agnostische orkestratie, Multi-Cloud management / brokering /cost-control /dashboarding / SSO, enz.…

De ICT-dienstverlener dient optimaal gebruik te maken van Clouddiensten welke uitstekend gestandaardiseerd zijn, aangeboden worden volgens een "pay-as-you-use" model, met inbegrip van een webinterface en APIs voor de bestelling en configuratie van alle DC infrastructuur en platformfuncties. Alle provisionering en aanpassing is voor 100% geautomatiseerd en wordt uitgevoerd in zeer korte tijd.

Het niveau van Business Continuity Management voor toepassingen dient door de klant bepaald te worden. Binnen één Cloud provider dient daarom de mogelijkheid geboden te worden om binnen één regio (binnen de EU) ten minste twee Availability Zones ter beschikking te hebben. Vanuit een DR-perspectief zal ook de mogelijkheid aangeboden worden om data te bewaren en toepassingen te runnen binnen een andere regio of cloud provider binnen de EU (cross-region backup).

2.2 Meerwaarde voor de Klanten

- Verlaging van de administratieve lasten voor het afnemen van public clouddiensten. Deze dienstverlening kan interessant zijn voor entiteiten met beperkte IT staf die willen focussen op kerntaken;
- De doorgans zeer hoge kwaliteit van public Cloud (beschikbaarheid, performantie, beveiliging) met hoge SLA's en penaliteiten.
- De doorgedreven standaardisatie, automatisatie en het enorme schaalvoordeel van public Cloud kunnen leiden tot een zeer hoge kostenefficiëntie
- Onbeperkte capaciteit en flexibele uitbreidingsmogelijkheden, modulaire afname mogelijk in functie van de noden

- Efficiënte behandeling van eventuele incidenten en problemen. Mogelijkheid tot inzicht en rapportering over gebruik van clouddiensten zowel technisch als financieel inclusief security checks, controle op de wettelijke compliance, etc.
- De facturatie, gekoppeld aan de VO financiële systemen, ondersteunende diensten voor cost control op afname, kostenoptimalisatie, technical support, etc.;
- De hyperscale public Cloud biedt enorme technologische en functionele mogelijkheden om de Vlaamse overheidsdiensten verder te verbeteren via een proces van digitale transformatie. Van de dienstverlener wordt verwacht dat hij de innovatie bij de Vlaamse overheid versterkt, door het actief en proactief aanbrengen van ideeën inzake technologische innovatie, door te inspireren en mee na te denken met de klant hoe deze kunnen toegepast worden in de bedrijfscontext van de klanten; Ook door ervaring en expertise mee te brengen uit andere bedrijfstakken en andere klanten;
- Duurzaamheid is een belangrijke na te streven meerwaarde in dit contract. Van de dienstverlener wordt verwacht dat hij aantoont dat duurzaamheid – in de brede betekenis – invulling krijgt binnen de geleverde diensten. Vooral worden ook concrete resultaten verwacht binnen de geleverde diensten, zoals inzake energie efficiëntie, recuperatie en afvalverwerking, herbruikbaarheid, enz.…
- Mechanismen voor samenwerking met andere diensten (service interfaces)
- Transparante prijsstructuur in functie van de afnames en de evolutie in de tijd.

2.3 Gevraagde kenmerken

De voorgestelde hyperscale Cloud oplossing houdt rekening met de volgende gevraagde karakteristieken:

- **SAAS boven PAAS boven IAAS** : de voorkeur gaat uit naar het gebruik van standaard PAAS of IAAS ‘building blocks’ van de hyperscale Cloud leverancier die de basis vereisten kunnen afdekken boven het introduceren van 3rd party elementen met niche functionaliteit:
    - sommige van deze 3th party elementen kunnen evenwel worden opgenomen in de service functionaliteit;
    - er kunnen gegronde redenen zijn om deze toe te passen; een voorbeeld is kostenreductie op vlak van data trafiekkosten, gezien de meeste Cloud leveranciers kosten aanrekenen op basis van transport data quota; deze zijn niet forfaitair of ‘bundle’ gebaseerd maar worden meestal per gigabyte aan effectief gepasseerd/verbruikt volume doorgerekend.
- **Standaardisatie en verschillende types van dienstverlening** gaande van minimaal beheer tot volledig beheer. Het volledig beheer kan traditioneel van aard zijn (cfr. Managed DC) of ingericht worden vanuit een CloudOps perspectief (volledig geautomatiseerd).
- **Multi-Cloud**: op het niveau van de individuele entiteit wordt idealiter gestandaardiseerd op de diensten van één enkele Cloud provider, gelet op efficiëntie, optimalisatie, integratieproblematiek en benodigde kennis binnen de beperkte schaal van één entiteit. Er is in de default dienstverlening geen streven naar portabiliteit over meerdere Cloud-leveranciers heen.

- **Schaalbaarheid**. Schaalbaarheid wordt gedefinieerd als een flexibele up- en downscaling in functie van de capaciteitsbehoeften op elk moment. Het is eigen aan Cloud IAAS/PAAS diensten dat dergelijke schaalbaarheid en dynamische schaling ondersteund wordt.

- **Autonomie**. Het spreekt voor zich dat VO entiteiten voor het gebruik van de DC diensten wensen te beschikken over een hoge graad van autonomie. Autonomie houdt in: eigen keuzes en beslissingen kunnen maken op vlak van architectuur, beveiliging, operationeel beheer, operationele dienstverlener, enz.…
    - de multi-tenancy die eigen is aan public Cloud diensten, vormt een uitstekende invulling van die autonomie (elke entiteit kan één of meerdere aparte tenants toepassen, wat hem isoleert van de andere gebruikers).
    - de HFB gemeenschappelijke diensten die in de public Cloud toegepast worden, ondersteunen maximaal de multi-tenancy; weliswaar houdt het gebruik van gemeenschappelijke diensten in, dat er geconformeerd wordt aan een aantal policies, standaarden en richtlijnen;
    - er wordt verder in de architectuur van de Cloud-gebaseerde systemen geen afhankelijkheid ingebouwd van on-prem gebaseerde systeemfuncties die deel uitmaken van het on-prem DC, dus storage, back-up, servers, netwerk, netwerk-security.

- **Compatibiliteit** met legacy VO-datacenters en toepassingen. Deze steunt enerzijds op het toepassen van X86-gebaseerde servers in de VO datacenters, en anderzijds op het vermijden van sterk verouderde platform software die niet meer ondersteund worden in een Cloud omgeving. Dit zijn keuzes die de Klant zelf kan maken. Merk op dat VPC Mechelen een (N-1) policy hanteert terwijl public Cloud diensten meestal ver gaan in het ondersteunen van oude platformen, vaak N-2 en zelfs N-3. Dit maakt het waarschijnlijk dat de as-is applicatie kan runnen in public Cloud zonder grote aanpassingen.
- **Beschikbaarheid**: het kunnen realiseren van zeer hoge beschikbaarheid van applicatiefuncties en data (> 99,95%), door het kunnen opvangen van meerdere fouten binnen HW en SW componenten, en door het aanbieden van meerdere AZ's en Regio's
    - binnen een Cloud provider zullen toepassingen met hoge beschikbaarheidsvereiste, binnen één regio over ten minste twee Availability Zones tworden ingericht; dat is sowieso mogelijk in public cloud diensten, zoals AWS, Azure, …
    - de beschikbaarheid van data in public Cloud voldoet aan uiterst hoge normen, beduidend hoger dan wat de VO vandaag hanteert, en ook hoger dan wat in VO-DC's, of doorgaans in Managed DC's wordt aangeboden
    - voor entiteiten die nog verder willen gaan, is er de mogelijkheid om – voornamelijk dan vanuit een DR-perspectief - voor zeer kritische data en toepassingen, data cross-region te bewaren en toepassingen te kunnen opspinnen binnen een andere regio op Europose bodem; bv regio's in Dublin, Frankfurt, Amsterdam, Parijs, enz.…
    - voor het uitwerken van een complete DR oplossing op basis van public Cloud, kan men beroep doen op bestaande referentie architecturen, documentatie en expertise.

- **Multi-Tenancy / dashboard** – het ondersteunen van de autonomie van de entiteit, door het aanbieden van volledig afgescheiden virtuele omgevingen en portalen
    - Een belangrijke vereiste behelst het kunnen scheiden van verschillende 'run' omgevingen van verschillende VO-entiteiten, Applicatie-Dienstleveranciers, ontwikkelingslandschappen, security classificaties etc.

- De nodige webportalen ten behoeve van de door de Klant aangeduide beheerder(s) die zowel op technisch als op financieel vlak een overzicht geeft van de bij de publieke Cloud-aanbieder afgenomen platform- en infrastructuurdiensten.
- Er wordt eveneens detailrapportering tot op het niveau van de apart gelabelde (“tags”) diensten opgeleverd.
- In de portaal kan de Klant alarmen configureren bij het bereiken van bepaalde financiële limieten m.b.t. het verbruik.
- Geconsolideerde maandelijkse facturatie, onderbouwd met detailrapportering van het gebruik van de diensten.
- Tenzij de klant hiervan afziet, zal de dienstenleverancier maandelijks een verbetervoorstel formuleren over hoe de klant zijn Cloud omgeving(en) kan optimaliseren vanuit het oogpunt van kosten efficiëntie, veiligheid, duurzaamheid en risicobeperking.
- Patchen in de Cloud, automatisering en CloudOps.

- **Connectiviteit** Teneinde de vooropgestelde hybrid architectuur te kunnen realiseren:
  - Zal private connectiviteit (cfr. Direct Connect / Expressroute /VPN/ …) – die de routering binnen de VO private address space (RFC1918) realiseert - onontbeerlijk blijven. Het gebruik van private punt-tot-punt verbindingen (lijnen), onderliggend aan deze connectiviteitsoplossingen, laat toe om harde garanties te leveren op vlak van beschikbaarheid, response tijden, packet loss en bandbreedtes.
  - Ook hier geldt de doelstelling om gemeenschappelijke platformen/lijnen te gebruiken in de context van de gekozen Cloud platformen om de kostprijs voor VO-entiteiten zo laag mogelijk te houden.
  - De doelstelling is om voor de meest gangbare hyperscale Cloud spelers (AWS, MS Azure) te beschikken over een VO POP (Point of Presence), die geleverd en uitgebaat wordt door de Netwerk leverancier op basis van performante, gegarandeerde en redundante punt-tot-punt verbindingen (lijnen) naar twee netwerk knooppunten die verbinding geven met andere VO datacenters en VO gebouwen.
- **Zero trust**
  - Het veiligheidsbeleid gaat uit van de zero-trust principes, cfr. NIST 800-207. Communicatie vanuit het VO netwerk, zoals de netwerkcontext van de werkplekken/ eindgebruikerstoestellen, of de netwerkcontext van andere VO- toepassingen of resources, binnen of buiten de Cloud-contexten, wordt beschouwd als communicatie vanuit een untrusted bron;
  - Er wordt een implementatie toegepast van de logische componenten van de zero-trust architectuur. Deze zijn: de Policy Engine (PE), de Policy administrator (PA), de Policy Enforcement Point (PEP);
  - Vanuit de architecturale en beveiligingsgoverance in de SIAM (SI), zal de implementatie van het zero-trust model aangestuurd en opgevolgd worden;
- **Security perimeters in de cloud**
  - Het is vanuit het veiligheidsbeleid geenszins de bedoeling om lokale security contexten zoals bijvoorbeeld die van werkplekken of andere security contexten of zones structureel te gaan doortrekken met open policies naar (extended) netwerkzones binnen verschillende Cloud omgevingen.
  - Toepassingen hebben hun eigen security context/perimeter/policies (PE, PA, PEP) en dienen door de datacenter leverancier ondergebracht te worden in verschillende toepassingszones conform hun dataclassificatie vereisten en bij voorkeur via webprotocollen te communiceren met de buitenwereld door gebruik te maken van open en

gestandaardiseerde webcommunicatie protocollen zoals HTTP/S webpublishing services, API REST/SOAP, SAML/OAUTH webauthenticatie, etc....

- **Toepassing van beste praktijken**
  - Bij de toepassing van de Cloud dienstverlening, worden de industrie beste praktijken toegepast, en daaronder vallen ook de aanbevolen architecturen en frameworks van de Cloud leveranciers. Bv: het AWS well architected framework.

2.4 Omschrijving verdere concretisering van de ondersteunende processen voor Cloud diensten

De algemene procesvereisten zijn opgenomen in het contractuele document “Vereisten ondersteunende processen en overlegfora”. Hieronder zijn meer gedetailleerde vereisten opgenomen specifiek voor de Cloud diensten in het Dienstenpakket “Cloud- en Datacenterdiensten”.

Voor de Exploitatie van de Cloud platformen zal de DC/Cloud ICT-Dienstverlener de onderliggende Cloud-aanbieder(s) en operationele betrokkenen aansturen om een kwalitatieve uitvoering te realiseren. Tevens zorgt hij ervoor dat alle achterliggende processen voor realisatie van deze Dienst voldoende zijn ingericht

Er dienen binnen Cloud diensten drie types van dienstverlening te kunnen worden aangeboden:

1. IAAS/PAAS – *minimaal beheer*, die een afgeslankte set van diensten omvat die als minimaal worden beschouwd indien het beheer zou gedaan worden door bijvoorbeeld de Applicatie leverancier.
2. CloudOps – *Cloud Operations beheer*, waarbij gebruikt wordt gemaakt van automatisering van de infrastructuur- en platformlaag benodigd voor Applicatiesystemen. De toepassing automatisering zorgt voor een herdefinitie/reductie van taken en diensten inzake infrastructuurbeheer;
3. IAAS/PAAS – *Traditioneel beheer*, dat zoals de naam aangeeft een traditionele waaier aan beheersdiensten omvat zoals service desk, monitoring, etc. zoals deze ook typisch in een traditioneel Managed DC zullen worden aangeboden

Voor wat betreft globale/gedeelde Cloud functionaliteiten (zoals bijvoorbeeld ‘root’ account/IAM management, gedeelde gateways, gedeelde interne koppelingen/verbindingen) dient de DC/Cloud ICT-Dienstverlener deze globale functies (proactief) te bewaken in termen van performantie (niet aanlopen tegen limieten), beschikbaarheid, beveiliging, kostevolutie, etc.).

2.4.1 Minimaal beheer

De P3 DC/Cloud dienstenleverancier levert

- Broker functie van public Cloud diensten
- Toegang tot het webportaal van de publieke Cloud leverancier, voor de configuratie van de Cloud IAAS/PAAS diensten; De DC/Cloud ICT-Dienstverlener stelt het volledige portfolio van de hyperscale IAAS/PAAS ter beschikking via de webportaal en API van de publieke Cloud-aanbieder, zonder toevoeging of filtering, en zonder dat men verplicht een bijkomend portaal van de DC/Cloud ICT-Dienstverlener dient te gebruiken (tenzij voor de hieronder vermelde portaal functies). De effectieve provisionering binnen public Cloud gebeurt door de Cloud-

aanbieder zelf, is volledig geautomatiseerd en dient middels het “pay-as-you-use”-model aangeboden. Er worden zowel productieomgevingen als omgevingen voor ontwikkeling en test aangeboden (non-productie-omgevingen).

- Exploitatiediensten:
    - bestelling;
    - tagging;
    - facturatie; gekoppeld aan de VO financiële systemen;
    - inzicht en rapportering over gebruik van clouddiensten door middel van dashboards zoals bijvoorbeeld het kunnen consulteren, bewaken/alarmeren van de (gecumuleerde) kosten, subscripties, security compliance etc. (zie verder).
    - een ondersteuning door een Technical Accountmanager (TAM), er wordt standaard geen lokale Nederlandstalige SDM-functie gevraagd. Op afspraak en in regie kan wel nog lokale Nederlandstalige SDM ondersteuning gevraagd worden.
    - een controle op de wettelijke compliance (AVG) van het Cloud aanbod inclusief de controle van de compliance rapportering (incl. audit rapporten) door de Cloud-aanbieder;
    - technische adviezen (extra betalende diensten)
    - ondersteuning inzake cost controle; (extra betalende diensten)
- Werkaanvragen/projecten en profielen die ingezet worden in regieprestaties
    - Bv i.h.k.v. de migratie en de target omgeving,
    - Bv projecten die specifieke tooling of expertise vereisen
- Een portaal voor de door de Klant als beheerder aangeduide personen, voor al zijn diensten, zowel die voor Cloud diensten, CloudOps, Cloud Traditioneel beheer, Managed DC diensten, enz.…
    - De voorkeur is dat de leverancier in Perceel 3 maximaal gebruik maakt van het overkoepelend bestelportaal & service cataloog bij de SI (perceel 1)
    - Het portaal dient voor:
        - het uitvoeren van de initiële bestelling
        - het melden van incidenten, vragen over het aanbod, het vragen van ondersteuning,
        - het bekijken van dashboards m.b.t. de afgenomen publieke Cloud diensten zoals bijvoorbeeld het kunnen consulteren, bewaken/alarmeren van de (gecumuleerde) kosten, subscripties, security compliance etc. (zie verder).
        - Merk op dat er geen standaard Service Desk is voor de Gebruikers;

Facturatie en financiële rapporten

De DC/Cloud dienstenleverancier (die hier dus een 'broker' rol heeft) levert gedetailleerde billing rapporten, waarvan het detail, en de frequentie van updates, in lijn is met de rapportering die de cloud provider levert.

- De toegang tot de billing rapporten gebeurt op een streng beveiligde manier; de billing rapporten kunnen geleverd worden aan de VO-entiteit zelf, zonder dat er inzage mogelijk is door andere VO-entiteiten, laat staan klanten-organisaties buiten de VO. De Broker zelf, en HFB hebben steeds inzage. De VO-entiteit kan het inzagerecht doorgeven aan derde partijen.
- Waar de Broker geen toegang kan leveren tot de gedetailleerde billing rapporten van de Cloud provider zelf, levert hij een alternatief dat dezelfde mate van detail, nauwkeurigheid en versheid van informatie levert; elke afwijking op deze regel dient voorafgaand door het bestuur te worden goedgekeurd. Als alternatief kan de broker zelf een webportaal aanleveren die de billing informatie op een gedetailleerde, maar ook overzichtelijke en grafische vorm voorstelt, op een manier die de VO-klant in staat stelt om zijn verbruik op te volgen, zowel dagelijks, als ook het actuele verbruik tijdens de dag zelf.
- Het webportaal levert een alarmfunctie die de VO-klant zelf kan instellen en dat de klant alarmeert indien het verbruik de ingestelde grenswaarden overschrijdt.

Accounts en Rechten

- De DC/Cloud dienstenleverancier levert aan de VO klant een Cloud user account met administratieve rechten op de webconsole van de Cloud provider. De klant kan deze Cloud user account zelf toepassen, of deze ter beschikking stellen van een door hem aangestelde dienstverlener welke onder de aansprakelijkheid van de klant werkt.
- De Broker behoudt de root rechten, maar zal de handelingen die root rechten vereisen en die een klant – of zijn aangestelde dienstverlener – vraagt, uitvoeren in het kader van support die hij levert in dienst van de klant. Analoog levert de Broker ook de nodige systeeminformatie zoals bv logs die ter beschikking gesteld worden, of geforward worden.

Ondersteuning

- De DC/Cloud ICT-Dienstverlener dient ervoor te zorgen dat de supportvragen van Klanten en Applicatie Dienstleveranciers zo efficiënt mogelijk worden gecapteerd en behandeld en dient in zijn offerte duidelijk toe te lichten hoe dit concreet kan worden gerealiseerd.
- De ondersteuning door een Technical Accountmanager (TAM) is in de dienst inbegrepen, maar is ook beperkt inzake de geleverde ondersteuning. Voor uitgebreide ondersteuningsvragen is een studieproject via werkaanvragen/project, of via regieprestaties steeds mogelijk.
- Hetzelfde geldt voor ondersteuning inzake cost controle; Adviezen inzake cost optimalisatie of vergelijkende studies zijn via werkaanvragen/project, of via regieprestaties mogelijk. Dit geldt ook voor projecten inzake migraties.

Operationele dienstverlening

- De DC/Cloud ICT-Dienstverlener dient bij 'minimaal beheer' geen backups, updates en upgrades van het OS of andere (applicatie) software die zal gebruikt worden (bijv. endpoint protection), uit te voeren.

Garanties

- De verantwoordelijkheid van de DC/Cloud dienstverlener wordt beperkt tot wat de achterliggende Cloud provider biedt (back-to-back).

2.4.2 CloudOps beheer

- Het CloudOps omvat het 'minimaal beheer', aangevuld met het configureren en beheren van de infrastructuur- en platformlaag van applicatiesystemen door gebruik te maken van automatisering (scripts). Het betreft "infrastructure as code" (IAC) waarbij de automatisering deel uitmaakt van een groter geheel van automatisering van het applicatiesysteem zelf: bv build en deploy van de applicatie. Het is dus cruciaal dat de ontwikkeling van automatisering van de onderste lagen gebeurt in nauwe samenwerking met de applicatieteams, volgens interfaces die onderling afgesproken worden (de applicatie is 'leading").
- De P3 DC/Cloud dienstenleverancier levert en configureert de onderliggende gestandaardiseerde infrastructuur- en platformdiensten, op vraag van, en volgens de specificaties van de VO-entiteit die klant is, of desgevallend de door hem aangestelde P5 AM dienstenleverancier. De P3 DC/Cloud dienstenleverancier zal dan ook als enige nog de public Cloud portaal gebruiken voor configuratie, en niet de P5 AM dienstenleverancier. Deze laatste kan wel gebruik maken van de automatiseringsbouwstenen die de P3 dienstenleverancier in zijn bestelportaal opneemt.
- De P3 DC/Cloud dienstenleverancier is verantwoordelijk voor de correcte uitvoering van de gevraagde diensten volgens specificatie, inclusief de **operationele beschikbaarheid** en de beveiliging van de infrastructuur of de platformdiensten zelf, en voor de correcte toepassing van de beveiligingsmaatregelen, voor het gevolg geven aan de events en changes vanuit de SI (SIEM en security beheer);
    - De P3 DC/Cloud dienstenleverancier is verantwoordelijk voor het "CloudOps" beheer van vServer instanties. Deze activiteiten omvatten de monitoring, up-to-date houden van het OS, alle ondersteunende processen, continu versiebeheer, enz… zoals beschreven in dit hoofdstuk;
    - Op Cloudops vServer instanties wordt standaard een antivirus, anti-malware oplossing toegepast. De ondersteunende tooling, software-licenties en processen daartoe zijn aanwezig en inbegrepen in de eenheidsprijs;
- Ingeval van **"Cloud ops"** diensten, neemt de P3 DC/Cloud dienstenleverancier ook de bijkomende verantwoordelijkheid voor de correcte ontwikkeling en uitvoering van de gevraagde automatiseringsdiensten, en het algehele integratie, operationele beschikbaarheid en beveiliging van de hele infrastructuur- en platformlaag die onderliggend is aan een applicatie;

- de P3 DC/Cloud dienstenleverancier zal bij “CloudOps” diensten instaan voor de beveiligingsarchitectuur van de onderliggende infrastructuur- en platformlaag, voor de correcte configuratie van de Cloud diensten, en de toepassing van aanvullende beveiligingsbouwstenen in de onderliggende infrastructuur- en platformlaag;
- ook zal de P3 DC/Cloud dienstenleverancier instaan voor het operationeel beheer van deze onderliggende infrastructuur- en platformlaag: incident- problem, change management; opvolging van security events en notificaties van de Cloud provider; opvolging van cost control;
- de P3 DC/Cloud dienstenleverancier kan ook instaan voor de opzet van tools en processen voor de samenwerking met de Service Integrator inzake het monitoren in de onderliggende infrastructuur- en platformlaag, het doorsturen van events, logs, .. naar de SIEM functie, enz.…
- de P3 DC/Cloud dienstenleverancier kan ook instaan voor het beheer van Kubernetes en de onderliggende server cluster;

Het infrastructuurbeheer en de CloudOps automatisering (IAC) dient zeer sterk geïntegreerd te zijn met het applicatie beheer en de automatisering van het applicatiesysteem waarvan de infrastructuur- en platformlagen een onderdeel zijn. Vanuit Dev/ops perspectief wordt de ontwikkeling en deployment van infrastructuur- automatisering aangestuurd door een gemengd devops team (P3 dienstenleverancier en Klantenteam), en ondersteund door een set van afspraken en tools.

- Bij de CloudOps dienst wordt een cataloog aangelegd van automatiseringsbouwstenen die een klantenteam kan bestellen via het bestelportaal;
- De automatiseringsbouwstenen zelf steunen op code, die in een VO-gedeelde software library (bv GitLab) zal worden beheerd, zodat er maximaal hergebruik kan gebeuren tussen alle percelen, leveranciers en klantenteams;
  - de P3 DC/Cloud dienstenleverancier zal instaan voor de opzet van deze VO-gedeelde software library (bv GitLab);
  - deze wordt toegankelijk gesteld (read/write) voor alle percelen, leveranciers en klantenteams binnen het ecosysteem;
- De verwachting is dat de P3 DC/Cloud dienstenleverancier de meeste code kan aanleveren vanuit corporate en externe bronnen. Hergebruik en overdraagbaarheid zijn essentiële karakteristieken.
- De ontwikkeling, test en deploymen van de CloudOps automatisering kan gebeuren op dezelfde Dev/Ops pipeline en tools die ook gebruikt wordt voor de applicatie ontwikkeling, door het gemengd DevOps team; De P3 DC/Cloud dienstenleverancier kan dergelijke DevOps toolkit en processen opzettten en beheren, als een klantenproject op vraag van de klant die een gemengd Devops Team wil opzetten.
- Bemerk dat indien de klant beroep doet op de diensten van P5 Application Management, deze laatste verwacht wordt om de DevOps toolkit en proces op te zetten en te beheren; In dit geval kan – indien de klant dit wenst – de P3 dienstenleverancier CloudOps automatisering ontwikkelen via deze tools & processen;

2.4.3 Traditioneel beheer

Het traditioneel beheer omvat het 'minimaal beheer', aangevuld met het beheren van de infrastructuur- en platformlaag van applicatiesystemen, cfr. alle standaard IAAS/PAAS processen (zoals opgelijst in hoofdstuk 2.5.5) en die ook gangbaar zijn in een traditioneel DC;

- De P3 DC/Cloud dienstenleverancier levert en configureert de onderliggende gestandaardiseerde infrastructuur- en platformdiensten, op vraag van, en volgens de specificaties van de VO-entiteit die klant is, of desgevallend de door hem aangestelde P5 AM dienstenleverancier; De P3 DC/Cloud dienstenleverancier zal dan ook als enige nog de public Cloud portaal gebruiken voor configuratie, en niet de P5 AM dienstenleverancier;
- De P3 DC/Cloud dienstenleverancier is verantwoordelijk voor de correcte uitvoering van de gevraagde diensten volgens specificatie, inclusief de **operationele beschikbaarheid** en de beveiliging van de infrastructuur of de platformdiensten zelf; De infrastructuur- en platformlaag staat in voor: incident- problem, change management; opvolging van security events en notificaties van de Cloud provider; opvolging van cost control;
- de P3 DC/Cloud dienstenleverancier kan ook instaan voor de opzet van tools en processen voor de samenwerking met de Service Integrator inzake het monitoren in de onderliggende infrastructuur- en platformlaag, het doorsturen van events, logs, .. naar de SIEM functie, enz....

2.4.4 Overzicht types beheer

De volgende tabel geeft het overzicht weer van de verschillende types van Cloud beheer:

	Minimaal beheer	CloudOps beheer	Traditioneel beheer
Toegang tot public Cloud provider			
Afsluiten (en tijdig verlengen/actualiseren) van de cloud contracten	SP	SP	SP
Toegang tot de webportaal public cloud provider (full admin)	Klant	SP	SP
Toegang tot de APIs voor configuratie (full admin)	Klant	SP	SP
Service requests			
Service provider biedt bestelportaal voor indienen/opvolgen van Service Requests	V	V	V
Service provider biedt support via TAM - binnen limieten van de dienst	V	V	V
Service provider staat in voor Opstarten/afsluiten van accounts	V	V	V
Logging, rapportering & facturatie			
DC/Cloud dienstverlener levert rapportering inzake verbruik, facturatie	V	V	V
DC/Cloud dienstverlener staat in voor centraal bijhouden van cloud Accounts, subscripties, Informatie betreffende contactpersonen klant, inclusief de aangestelde dienstverleners	V	V	V
DC/Cloud dienstverlener staat in voor centraal bijhouden van parameters inzake cloud gebruik (bv regio, max consumptie) en facturatiegegevens	V	V	V
DC/Cloud dienstverlener staat in voor centraal bijhouden informatieregisters inzake incident management, problem management, change management, die betrekking hebben op de geleverde dienst	beperkt tot technische ondersteuning	V	V
DC/Cloud dienstverlener levert op aanvraag van de klant de gedetailleerde billing rapporten van de cloud lev	indien beschikbaar	indien beschikbaar	indien beschikbaar
DC/Cloud dienstverlener levert logging informatie die enkel via de reseller kan geleverd worden	V	V	V
DC/Cloud dienstverlener meldt de notificaties, waarschuwingen, … afkomstig van public cloud provider	V	V	V
DC/Cloud dienstverlener biedt rapporten inzake verbruik en facturatie	V	V	V
DC/Cloud dienstverlener verzorgt de integratie met VO financiële toepassingen en processen (Orafin);	V	V	V
DC/Cloud dienstverlener houdt logs bij inzake de configuraties op de cloud, en kan die logs overhandigen aan de klant	V	V	V
Het doorsturen van relevante events en logs naar de SIEM van de Service Integrator	Klant	SP, mbt scripting & automatisering	SP, traditioneel
Technische ondersteuning			
DC/Cloud dienstverlener biedt toegang tot TAM (Technical Account Management) van de cloud provider	V	V	V
DC/Cloud dienstverlener biedt op vraag van Klant (betalende) support diensten door cloud specialisten, en adviezen inzake cloud kosten, architectuur enz…	V	V	V
Versiebeheer			
Uitvoeren van patches/hofixes , upgrades/packs (platform / OS specifiek)	Klant	SP, mbt scripting & automatisering	SP, traditioneel
het ontwikkelen en toepassen van automatiseringsscripts mbt versiebeheer op de onderliggende infrastructuur- en platformlagen (die kunnen getriggerd worden vanuit de applicatie)	Klant	SP	niet voorzien
Beschikbaarheidsbeheer			
DC/Cloud dienstverlener biedt beheer inzake beschikbaarheid , en voorziet dit ook in het exploitatiedossier	Beschikbaarheid beperkt tot wat de cloud leverancier aanbiedt	Voorzien voor de infra/platformlaag, maximaal geautomatiseerd	Voorzien voor de infra/platformlaag, traditioneel beheer
Voorzien van recovery en DR op de onderliggende infrastructuur- en platformlagen (op specificatie van klant)	Klant	SP	SP
Het nemen van de nodige back-up van de platformen en servers (OS/images). Backup van de 'data' zelf (bv database), is beperkt tot de backup/recovery van de backupfile van de database;	Klant	SP, mbt scripting & automatisering (geen backup van server images, wel recreëren)	SP
Het monitoren en desgewenst starten, stoppen en herstarten van de onderliggende infrastructuur- en platformlagen	Klant	Voorzien voor de infra/platformlaag, maximaal geautomatiseerd	Voorzien voor de infra/platformlaag, traditioneel beheer
Automatiseringsscripts mbt availability-management op de onderliggende infrastructuur- en platformlagen (die kunnen getriggerd worden vanuit de applicatie)	Klant	SP (geautomatiseerd)	niet voorzien
Configuratiebeheer			
Configuratie en asset beheer van de onderliggende infrastructuur- en platformlagen in de cloud; Bemerk dat voor dynamische cloud omgevingen, de CMDB enkel beperkte informatie bijhoudt;	Klant	SP	SP
Bijhouden van lijsten van IAAS/PAAS componenten in CMDB, ontsluiting naar het DDC-DWH; Bemerk dat voor dynamische cloud omgevingen, de CMDB enkel beperkte informatie bijhoudt;	Klant	SP	SP
Configuratiebeheer het onderhouden en actualiseren van de design artefacten die de onderliggende infrastructuur- en platformlagen documenteren	Klant	SP	SP
Beveiligingsbeheer			
DC/Cloud dienstverlener biedt cloud diensten cfr de AVG bepalingen	V	V	V
De configuratie van de IAAS/PAAS laag gebeurt cfr het VO security beleid (VO informatie klassificatie raamwerk)	Klant	SP	SP
De gegevens 'in rust' worden beveiligd door het toepassen van encryptiemaatregelen, cfr de minimale vereisten van het VO security beleid; Dit is in hoofdzaak een taak van de applicatiebouwer en exploitant;	Klant	Klant	Klant
De gegevens 'in motion' worden beveiligd door het toepassen van encryptiemaatregelen bij de configuratie van de onderliggende infrastructuur- en platformlaag	Klant	SP	SP
DC/Cloud dienstverlener biedt in de cloudomgeving betalende diensten aan inzake perimeterbeveiliging en beveiligde toegang tot het Internet	V	V	V
Op de onderliggende infrastructuur- en platformlaag zal de DC/Cloud dienstverlener de diensten inzake perimeterbeveiliging en beveiligd toegang tot het Internet) configureren.	op aanvraag (betalend aanbod)	inbegrepen	inbegrepen
Bewaken van de correcte werking van het toegangsbeheer (Accounts / IAM)	Klant	SP	SP
Uitvoeren van antivirusmaatregelen op de compute instance	Klant	SP	SP
Automatiseringsscripts mbt beveiliging op de onderliggende infrastructuur- en platformlaag (die kunnen getriggerd worden vanuit de applicatie)	Klant	inbegrepen	niet voorzien
Capaciteitsbeheer			
Opvolging/monitoring belangrijke parameters van individuele instanties van de onderliggende infrastructuur-	Klant	SP (geautomatiseerd)	SP
Capaciteitsbeheer van de onderliggende infrastructuur- en platformlaag; Automatisatie ervan vereist een gemengd devops team applicatie & infrastructuur	Klant	SP (geautomatiseerd)	SP
DC/Cloud dienstverlener stuurt notificaties indien ingestelde (overkoepelende) capaciteitsdrempels qua cloud consumptie worden overschreden	V	V	V
Notificaties indien componenten in de onderliggende infrastructuur- en platformlaag capaciteitsdrempels overschrijden	Klant	SP	SP
Beheer van incidenten, events en problemen			
Het monitoren van de infrastructuur- en platformlaag (IAAS/PAAS)	Klant	SP	SP
Het uitvoeren van incident- problem- en change management processen. Incidenten, gemeld via de Service desk of automatisch gegenereerd via alarmen uit de monitoring tools	Incident, problem, change mgmt beperkt tot wat de cloud leverancier aanbiedt	Voorzien voor de infra/platformlaag, maximaal geautomatiseerd	Voorzien voor de infra/platformlaag, traditioneel beheer
Proactief probleembeheer' en bij storingen een root cause analyse uitvoeren	niet voorzien	Voorzien voor de infra/platformlaag, maximaal geautomatiseerd	Voorzien voor de infra/platformlaag, traditioneel beheer

2.4.5 Algemene beschrijving van de ondersteunende processen

Onderstaande (ITIL) processen zijn van toepassing op de Cloud diensten; In het geval van “minimaal beheer” zijn deze processen minimaal ingevuld of afwezig. In geval van CloudOps zal het volledige beheer worden geautomatiseerd. Bij eventuele onduidelijkheid zal bovenstaande tabel steeds primeren.

Alle onderliggende processen hebben betrekking op, en zijn ook beperkt tot, de infrastructuur- en platformlaag onderliggend aan de applicatie.

2.4.5.1 Incident management:

- De DC/Cloud ICT-Dienstverlener geeft de gepaste prioriteit aan de Incidenten, gemeld via de Service desk of automatisch gegenereerd via alarmen uit de monitoring tools, om de als SLA opgenomen beschikbaarheid te realiseren. Dit omvat eveneens het voorzien van een wachtdienst voor het garanderen van de overeengekomen dienstverleningsniveaus met betrekking tot deze Dienst.
- M.b.t. CloudOps beheer kan de monitoring van het applicatiesysteem betrekking hebben op applicatie-services of componenten zelf, en ook op de onderliggende infrastructuur- en platformcomponenten, waarbij de eerste meer belang hebben dan de tweede. Het belang van OS-monitoring kan dus erg beperkt zijn, terwijl het belang van applicatie-monitoring en de correlatie van events stijgt.

2.4.5.2 Problem management:

- De DC/Cloud ICT-Dienstverlener voert het problem mgmnt proces uit, die betrekking heeft op de infrastructuur- en platformlaag onderliggend aan de applicatie die de dienstverlener ingeval van CloudOps of Traditioneel beheer uitvoert. Bij minimaal beheer gebeurt is het problem management proces beperkt tot de additionele netwerkbeveiligingsdiensten die aangeboden worden;
- De DC/Cloud ICT-Dienstverlener voert d.m.v. monitoring ook een “proactief probleembeheer” uit. Reactief voert de dienstverlener root cause analyses uit, en werkt daarvoor samen met andere dienstverleners in het ecosysteem;

2.4.5.3 Cloud en Subcontractmanagement:

- Dit houdt in het afsluiten (en tijdig verlengen/actualiseren) van de nodige contracten om de Cloud diensten te realiseren. Dit zijn de contracten met Cloud providers, en ook de bijkomende contracten inzake DC netwerk- en beveiligingsbouwstenen en alle ondersteunen infrastructuur en platformen om de diensten te realiseren;
- De dienstverlener ziet erop toe dat de contracten in lijn zijn met de AVG bepalingen, en controleert ook de audit rapporten die de Cloud provider voorlegt;

2.4.5.4 Monitoring en Event management:

- Dit betreft het monitoren van de infrastructuur- en platformlaag onderliggend aan de applicatie die de dienstverlener ingeval van CloudOps of Traditioneel beheer uitvoert. Bij minimaal beheer gebeurt die monitoring niet.

- Zowel performantie als beschikbaarheid dienen – al dan niet met automatisatie & scripting - te worden opgevolgd. Verder wordt het gebruik van de platform- en infrastructuur-componenten etc. opgevolgd zodat zowel abnormaal hoog gebruik of inbreuken op de veiligheid snel gedetecteerd worden. Vanuit een gecentraliseerd monitoring systeem worden alarmberichten uitgestuurd die automatisch Incidenten melden als bepaalde alarmdrempels worden overschreden.
- Het event management proces zorgt ook voor het doorsturen van relevante events naar de SI, voor distributie van de events naar andere'SP's in het ecosysteem, en naar de SIEM functie van de SI.

2.4.5.5 Capacity management:

- Het capaciteitsbeheer heeft betrekking op, en is ook beperkt tot, de infrastructuur- en platformlaag onderliggend aan de applicatie. Daarin zijn ook inbegrepen de bijkomende netwerk- en netwerkbeveiligingsbouwstenen die de dienstenleverancier aanbiedt.
- De belangrijke parameters i.v.m. deze laag worden opgevolgd, gemonitord en de Klant wordt ingelicht indien er afgesproken capaciteitsdrempels worden overschreden, en geadviseerd hoe de capaciteit kan aangepast worden.
- De klant kan advies vragen naar evaluatie of voorstellen om kostenoptimalisaties te realiseren.
- Cloud omgevingen bieden de mogelijkheid om dynamisch te schalen, en daar wordt rekening mee gehouden.
- Er zijn een aantal overkoepelende gebruikslimieten die door de dienstenleverancier worden beheerd.

2.4.5.6 Availability management (CloudOps/traditioneel):

- Het operationeel beheer van de infrastructuur- en platformlaag onderliggend aan de applicatie, om deze Diensten conform de gevraagde beschikbaarheidsniveaus te garanderen; (het bepalen van de beschikbaarheid zelf en vereist veiligheidsniveau zit op niveau applicatiebeheer of bij klant/opdrachtgever).
- De infrastructuur- en platformlaag onderliggend aan de applicatie, kan in grote mate resilient gebouwd zijn over meerdere instanties, availability zones en zelfs regio's, en waarbij het recovery proces ingeval van de CloudOps dienst, uitgevoerd wordt door een geautomatiseerd detection- en recovery systeem. De DC/Cloud ICT-Dienstverlener zorgt voor de nodige redundancy- en failover mogelijkheden om de gevraagde beschikbaarheid (bijv. over verschillende Availability Zones) te garanderen.
- Het beschikbaar houden – al dan niet met automatisatie & scripting – van de infrastructuur- en platformlaag onderliggend aan de applicatie, en alle processen die noodzakelijk zijn om de functionaliteit met betrekking tot de infrastructuur- en platformlaag onderliggend aan de applicatie te kunnen aanbieden.
- Het – al dan niet met automatisatie & scripting - opnemen in de operationele omgeving van bijkomende standaard platformen en servers via het proces "Beheer van de Service Portfolio en de Service catalogus " en nadat deze werden overgedragen vanuit projectwerking naar Exploitatie.
- Het nemen van de nodige back-up van de bestanden op de platformen en servers om te garanderen dat het verlies van data maximaal ingedekt is (inclusief het veilig bewaren van de

back-ups). Van de backup data files van databanken en van de bestanden in de beheerde servers wordt standaard minstens dagelijks een back-up genomen binnen de regio. De back-ups worden 30 dagen bewaard. De klant kan mits een betalend klantenproject (via werkaanvraag), de backup ook laten nemen in andere regio/ cloud provider / of daarbuiten.

- Bij traditioneel beheer: De DC/Cloud ICT-Dienstverlener neemt standaard een dagelijkse backup van de volledige server (image), en kan op aanvraag bijkomende backups nemen. De backup modaliteiten zijn als volgt te omschrijven:
    - de standaard retentie periode voor de backup is 30 dagen,
    - deze backup wordt op dezelfde regio gedurende deze periode bijgehouden.
    - De Klant is zelf verantwoordelijk om te bepalen wat geback-upt dient te worden en wat niet, rekening houdend met het feit dat in deze backup data ook het besturingssysteem geback-upt wordt (backup is immers een zaak van bescherming tegen logische fouten en dit valt binnen applicatiebeheer). Op die manier kan bij een restore van een volledige server de laatst werkende configuratie terug gezet worden.
    - De Klant moet zelf zorgen voor de back-up van eventuele databanken naar een backup bestand (en evt journal file) zodat dit vervolgens met de standaard systeem back-up kan meegenomen worden. De Klant kan aanpassingen vragen aan de beschreven standaard opzet : hij kan vragen om bepaalde gegevens niet te backuppen door middel van een project of in samenspraak met de SDM via regie prestaties.
- De DC/Cloud ICT-Dienstverlener voert – al dan niet met automatisatie & scripting - de nodige Updates en Upgrades uit van de software die wordt gebruikt met betrekking tot de platform- en serverdiensten.
- Al dan niet met automatisatie & scripting: het starten, stoppen en herstarten van servers.
- Al dan niet met automatisatie & scripting: installatie van service packs en hotfixes.
- Al dan niet met automatisatie & scripting: implementeren van antivirusmaatregelen.
- Al dan niet met automatisatie & scripting: tunen van de syteemcomponenten.

2.4.5.7 Configuratiebeheer en Asset management (CloudOps/traditioneel):

Alle informatie m.b.t. de actieve Cloud accounts (aantallen, kenmerken, klant) dient steeds actueel gehouden te worden De onderliggende platformen binnen hyperscale cloud omgevingen behoren tot de Cloud-aanbieder en behoeven geen Configuratiebeheer.

Binnen hyperscale Cloud omgevingen worden resources/assets meer en meer dynamisch gecreëerd, opgespind, gestopt en verwijderd wat indruist tegen de eerder statische logica van externe Configuratiedatabanken ter consolidatie van asset informatie en configuratie. Het al dan niet Up-to-date houden van een centrale Configuratiedatabank m.b.t. de inventariselementen voor Cloud IAAS/PAAS diensten - en ontsluiting naar het DDC-DWH zodat ze beschikbaar zijn voor de rapportering - zal alleen dienen te worden opgezet indien gevraagd (vb. in kader van traditioneel beheer). Indien mogelijk kan steeds gebruikt worden gemaakt van de standaard aangeboden configuratie en asset beheer via het portaal van de Cloud-aanbieder zelf.

Verder omvat het configuratiebeheer het onderhouden en actualiseren van de documentaire configuratiegegevens voornamelijk m.b.t. globale/gedeelde Cloud functionaliteiten en alleen waar gevraagd voor specifieke IAAS/PAAS platform- en serverdiensten.

2.4.5.8 Beveiligingsbeheer:

Het beveiligingsbeheer kan als volgt worden gedefinieerd:

- Het bepalen van het vereiste veiligheidsniveau, en de inrichting van de Cloud (security in the Cloud) zit op niveau applicatiebeheer (vereisten zelf bij klant/opdrachtgever).
- Bewaken van de correcte werking van het toegangsbeheer (Accounts / IAM) om ongeoorloofde toegang van personen of systemen tot de gegevens in de beheerde IAAS/PAAS dienst te vermijden (CloudOps/traditioneel). Hierbij gelden hogere eisen voor de toegang met uitgebreidere rechten (o.a. voor beheerdoel-einden) en voor toegang tot Persoonsgegevens. De toepasselijke organisatorische en technische maatregelen worden opgenomen in het exploitatiedossier van de server.
- Er dient voor Cloud omgevingen elk ogenblik een goede beschrijving beschikbaar te zijn van de platformen en/of opzet van de automatisatie die de DC/Cloud ICT-Dienstverlener inzet voor de server- en platformdiensten (traditioneel/CloudOps). Hierbij wordt ook aangegeven hoe deze platformen zijn gesegregeerd en geconnecteerd met de VO-WAN en het internet (netwerk- en beveiligings-componenten).
- Met betrekking tot de infrastructuur die onderliggend gebruikt wordt voor het bewaren en verwerken van persoonsgegevens is een verhoogd veiligheidsniveau van toepassing. Deze infrastructuur maakt mee het voorwerp uit van de controles m.b.t. de wet op de privacy. Een vereiste bovendien is dat deze infrastructuur uitsluitend binnen de Europese Unie mag geplaatst worden, wat impliceert dat enkel cloud regio's binnen de EU worden toegepast;
- Er dient gebruik te kunnen worden gemaakt van de door de publieke Cloud-aanbieder aangeboden platform (bv AWS KMS en Azure KMS) om zowel de data "in rust" als "in motion' te encrypteren. Deze zal worden toegepast op VO data, door de klant of zijn Applicatieleverancier i.h.k.v. een klantenproject.
- Op specifieke vraag (traditioneel/CloudOps), – al dan niet met automatisatie & scripting - voorzien van bescherming tegen malware op de beheerde platformen en servers (beveiligingspatches van endpoint protection, etc. indien niet voorzien door de Applicatie-Dienstleverancier).
- De onderliggende cloud aanbieder:
    - dient voor de publieke ontsluiting van de toepassingen te beschikken over eigen redundante Internet verbinding en perimeter beveiligingsdiensten zoals Internet border protection Next-gen Firewall (ngFW), aDDOS / IPS; en
    - dient voor alle instanties het principe van netwerksegregatie te respecteren: het opsplitsen in verschillende lagen en zones die logisch bij elkaar horen, eenzelfde risiconiveau hebben (cfr. VO dataclassificatie) of dezelfde security maatregelen vereisen.

Zie voor verdere beschrijving: 2.4.6.6 Beveiligingsbeheer, Compliance en Identity Management

2.4.6 Beschrijving van de ondersteunende processen en tools specifiek voor Cloud diensten

Inzake Cloud Management Processen en Tools, zijn er op een aantal vlakken specifieke vereisten:

2.4.6.1 Provisionering en Orchestratie

Voor de bestelling en de daarop volgende provisionering van public Cloud IAAS/PAAS diensten zijn volgende processen en tools noodzakelijk:

- Voor minimaal beheer wordt de bestelportaal van de public Cloud leverancier toegepast door de leverancier van Applicatiediensten (Perceel 5), of door het klanten-team.
- Voorafgaand aan de eerste bestelling van Cloud Minimaal Beheer, dient de VO-entiteit zich klant te maken van de Cloud diensten, door een bestelling uit te voeren in het bestelportaal van de leverancier in Perceel 3. Op die manier worden de master accounts aangemaakt, de bestelling en facturatie ingeregeld, parameters inzake regio en gebruikslimieten ingesteld, enz.…. Ook kan meteen een pakket 'Accounts', bv AWS accounts, klaargezet worden;
- De leverancier in Perceel 3 voorziet een bestelportaal voor al zijn diensten, zowel die voor Cloud diensten, CloudOps, Cloud Traditioneel beheer, Managed DC diensten, enz.…
    - De voorkeur is dat de leverancier in Perceel 3 maximaal gebruik maakt van het overkoepelend bestelportaal & service cataloog bij de SI (perceel 1),
- Bij de CloudOps dienst wordt een cataloog aangelegd van automatiseringsbouwstenen die een klantenteam kan bestellen via het bestelportaal.
- De automatiseringsbouwstenen zelf steunen op code, die in een VO-gedeelde software library (bv GitLab) worden beheerd, zodat er maximaal hergebruik kan gebeuren tussen alle percelen, leveranciers en klantenteams.
- Na bestelling of activatie van een CloudOps automatiseringsbouwsteen gebeurt een geautomatiseerde uitvoering ervan, en dus een orkestratie en provisionering van een geheel van Cloud IAAS/PAAS diensten; Bv een "landing zone";
    - De provisionering van public cloud diensten gebeurt op basis van de cloud-platform-native provisionering templates en diensten, en dus niet middels een bovenliggende Cloud orkestratie tool van een third party leverancier;
        - Dergelijke orkestratie tool kan uiteraard wel toegepast worden bij de provisionering in een Managed DC.
    - Er is geen vereiste naar (overkoepelende) tools en processen om Multi-Cloud orkestratie of hybrid Cloud orkestratie te ondersteunen.
    - Er wordt voorzien in een Task scheduler voor het schedulen van de provisionering zodat de uitvoering kan ingepland worden, bv tijdens daluren.
- CloudOps automatiseringsbouwstenen kunnen eveneens via een API aangesproken worden. Dat maakt het ook mogelijk om event-gebaseerde provisionering uit te voeren, bv om op te schalen, of om recovery uit te voeren.
- Het bestelportaal, de automatiseringsbouwstenen, de orkestratie, vinden we ook terug in een Managed DC als dit de vorm aanneemt van een "private Cloud". Het onderscheid is dat we bij public Cloud een 100% automatisering nastreven, en maximaal Cloud-native diensten en architecturen willen toepassen;

2.4.6.2 Cost Management en Resource Optimalisatie

Voor het beheer van de uitgaven voor public Cloud IAAS/PAAS diensten, en voor de optimalisatie ervan, zijn volgende processen en tools noodzakelijk:

- Een overkoepelende rapportering en facturatie over de verschillende public Cloud diensten, op periodieke basis;
    - Facturatie gebeurt met de facturatiesystemen en processen van de VO.
    - Klanten beschikken elke dag over actuele en accurate gebruiksrapporten.
    - Klanten (VO-entiteiten) hebben enkel inzage in de gebruiksrapporten van hun eigen entiteit, en niet van andere entiteiten.
- De leverancier geeft, op vraag van de VO-entiteit, ondersteuning inzake budgettering, dus het verwerken van gebruiksgebaseerde diensten (variabele kost) in een vastgelegd budget (vastlegging).
- De leverancier geeft, op vraag van de VO-entiteit, pro-actieve waarschuwingen (alerting) van de klant op basis van de grenswaarden (tresholds) inzake verbruik, die eerder met de entiteit afgesproken werden.
- De leverancier detecteert op vraag van de VO-entiteit, abnormaal gebruik, en geeft tijdige waarschuwingen (alerting) aan de entiteit om overspending te vermijden.
- De leverancier geeft, op vraag van de VO-entiteit, ondersteuning en pro-actief adviezen om de infrastructuur te 'rightsizen' en om de geschikte compute en andere diensten toe te passen in functie van het verwachte gebruik.
- De leverancier geeft pro-actief voorstellen om het cloud verbruik te beperken, door o.a.:
    - reserved instances uit de public Cloud cataloog toe te passen – wanneer dit de beste optie blijkt en na overleg en akkoord met de klant.
    - om serverless diensten toe te passen wanneer dit de betere optie is.
    - dynamische schaling, autoschaling enz.… toe te passen.
    - resources uit te schakelen of te verminderen in daluren.
    - gebruik te maken van platformdiensten.
    - enz.…
- De leverancier, op vraag van de VO-entiteit, berekent en vergelijkt de beste opties inzake het gebruik van IAAS/PAAS diensten.

2.4.6.3 Monitoring en Analytics

Voor het operationele beheer van de public Cloud dienst "traditioneel beheer" en "CloudOps" zijn volgende processen en tools noodzakelijk:

- Monitoring en event management processen, op basis van een monitoring tool, event processing platform, monitoring dashboard en monitoring Rapporten.
- Event interpretatie en alerting. Dit gebeurt zo mogelijk policy-gedreven.
- Het monitoring van de Cloud resource performantie.
- Log Collectie.
- De voorkeur gaat naar de inzet van Cloud native platformen waar mogelijk en beschikbaar.

2.4.6.4 Inventaris en Classificatie

Voor het operationele beheer van de public Cloud dienst “traditioneel beheer” en “CloudOps” zijn volgende processen en tools noodzakelijk:

- Een inventaris van alle gebruikte cloud resources;
  - Optioneel is een Cloud resource discovery service
- Het monitoren van wijzigingen in de Cloud resource configuratie .
- Het toepassen van Cloud-platform-native tagging.
- Bij het configureren van Cloud resources past men vooraf bepaalde regels toe, en ziet men toe op de toepassing ervan.
- Er gebeurt een detectie van untagged resources.

2.4.6.5 Cloud Backup en Disaster Recovery

Voor het operationele beheer van de public Cloud dienst “traditioneel beheer” en “CloudOps” zijn volgende processen en tools noodzakelijk:

- Het uitvoeren van backups van storage objecten op basis van object storage backup policies.
- Het uitvoeren van storage life cycle acties, op basis van storage life cycle policies;
  - Bv migratie van AWS S3 naar AWS Glacier.
- Het uitvoeren van backups van Block storage op basis van backup policies.
- Het uitvoeren van backups van compute instances (images, bv AWS EC2) op basis van backup policies.
- Het uitvoeren van restores van object storage point-in-time backups.
- Het uitvoeren van restores van Block storage point-in-time backups.
- Het uitvoeren van restores van compute instance point-in-time backups.

Alle backup processen en tools gebeuren in de regio waar de storage dienst afgenomen wordt (in een multi-AZ opzet). Indien de klant voor de backup een andere regio, of cloud provider kiest, dan wordt dit als een apart project, met aparte exploitatiekosten, verrekend. Merk op dat de regio’s bij start van het contract beperkt worden tot de regio’s die vandaag al worden toegepast;

2.4.6.6 Beveiligingsbeheer, Compliance en Identity Management

Voor het operationele beheer van de public Cloud dienst “traditioneel beheer” en “CloudOps” zijn volgende processen en tools noodzakelijk:

- Zie ook overzichtstabel in RefBib “security bouwstenen”
- Security event notificaties worden gerapporteerd, bij voorkeur overkoepelend over alle Cloud providers;
  - De Applicatieleverancier (Perceel 5), of klantenteam, en de Service Integrator, beschikken elke dag over actuele en accurate rapporten inzake security events.
  - Alle relevante informatie, zoals OS release, patching level, endpoint protection,.. gedetecteerde security events en logs (bijv. alerts van een bepaald niveau) dienen te

worden gecommuniceerd naar de globale SIEM van de VO (SIAM) voor interpretatie binnen de SIEM en de overkoepelende security monitoring.

- Raw data dient steeds ad-hoc toegankelijk te zijn voor het VO SOC team om redenen van investigation/ tracking /evidence /forensics.
- Klantenteams, applicatieleveranciers,… hebben enkel inzage in de event notificaties van hun eigen entiteit/applicatie en niet die van andere entiteiten/applicaties.

- De leverancier beheert de identiteiten en autorisaties van klantenteams, applicatieleveranciers,… op de verschillende rapporten en tools die hij ter beschikking stelt; Bij voorkeur kan hij daarvoor beroep doen op de WebIDM en VO-toegangsbeheer bouwstenen van HFB.
- Network flow monitoring. wordt voorzien
- De leverancier geeft, op vraag van de VO-entiteit, ondersteuning en pro-actief adviezen om de netwerk (segregatie) in te regelen conform de VO policies.;
- De DC leverancier past de beste praktijken inzake security architectuur toe, die de cloud provider voorziet. Hij past zoveel mogelijk ook de cloud native platformen toe die daartoe een bijdrage kunnen leveren, bv inzake fouten in de configuratie, threat- en anomalie detectie, IAM, security groups enz…
- De DC leverancier volgt de technologische evolutie van de cloud diensten op de voet, om de restris'co's verder te reduceren;
- De leverancier voorziet volgende bijkomende security bouwstenen in de context van public Cloud. De dienstenleverancier staat in voor: Service Design, Design Authority, Investering, commercieel contactpunt, Productbeheer, Exploitatie;
  - **aDDOS** levert bescherming tegen tegen DDoS aanvallen, zowel volumetrisch als applicatief. De bescherming maakt een onderscheid tussen het regulier (gebruikers en data) verkeer en herhaalde geautomatiseerde aanvragen (aanvallen) welke de (gecentraliseerde) ICT diensten kunnen overbelasten.
  - **Container security** (ingeval van CloudOps); Container security is een breed begrip dat de verschillende niveaus van beveiliging afdekt m.b.t. PAAS containers zoals docker (hardening image, toegang, account, netwerk,...); de realisatie ervan valt binnen de FMO, dus na transitie;
  - **Endpoint protection/ endpoint detection & response**: levert naast de traditionele signature-gebaseerde malware detectie ook meer intelligente, signatureloze methodes zoals ATP, gedragsmonitoring op applicaties / processen / memory / netwerk, machine learning, reputatie analyse etc. (multimethode beveiliding)
  - **Next-gen FW** (ngFW) voor de perimeter beveiliging, inclusief (minimale voorwaarden) IPS/IDS:IOC detectie, ATP, URL filtering, SSL decryption, Sandboxing, APP/User awareness, NAT, enz.…; de realisatie ervan valt binnen de FMO, dus na transitie;
    - Het betreft hier een maandelijkse eenheidsprijs die per virtueel systeem wordt verrekend aan de klant, volgens throughput/bandbreedte,
      - € per 200 Mbps virtueel systeem
      - € per 500 Mbps virtueel system
      - € per 1000 Mbps virtueel system

        - Er wordt per VIP een begrenzing voorzien op vlak van:
            - Bandbreedte:
            - aantal backend servers: 3
        - Bij hogere aantallen backend servers worden bijkomende VIPS aangerekend.
    - **Threat Intelligence (TI) en Threat hunting (TH).**
        - TI levert een breed scala aan informatie over bedreigingen incl. de mogelijkheid tot het groeperen en centraliseren van threats / IOCs afkomstig van diverse platformen en bronnen van en naar verschillende security platformen, incl. bedreigingen die gecapteerd worden in sandbox-gebaseerde analyses, CERT-EU/CERT-BE, enz.… Dit laat een gedetailleerde analyse toe van de globale en extern geleerde bedreigingen in de infrastructuur die de SP beheert (reactief).
        - Threat hunting levert een pro-actieve aanpak voor het opzoeken van sporen van malicious activity.
- Volgende security bouwstenen in de context van public Cloud worden geleverd door andere partijen die instaan voor: Service Design, Design Authority, Investering, commercieel contactpunt, Productbeheer, Exploitatie;
    - **SIEM**. De DC/Cloud dienstverlener is verantwoordelijk voor het doorsturen van informatie naar de SIEM – zie beschrijving in VOPO document;
    - Opmerkingen:
        - **Application Delivery Control (ADC)** steunt op de Cloud native platformen (bv AWS ELB en ALB); Eventuele bijkomende Reverse Proxies zijn te implementeren als een RP middleware (bv NGINX of Apache) die runt op een Cloud compute instance.
        - Voor split DNS (bv deels naar de VO DNS en deels naar Route53) is een split DNS service te implementeren als een DNS middleware die runt op een Cloud compute instance; De opzet van een split DNS gebeurt via een werkaanvraag;
        - De Forward Proxy functie zal geleverd worden door HFB en de Perceel 4 dienstverlener

Volgende tabel geeft een overzicht van de beveiligingsdiensten, en de rollen en verantwoordelijkheden:

2.4.6.7 Log Management

De Perceel 3 DC/Cloud dienstenleverancier staat in voor:

- Het loggen van alle operationele logs en organisatorische logs.
    - Het opslag en het beheer van de logs m.b.t. platformen en de onderliggende infrastructuur. Bestaande logs omvatten in eerste instantie operationele logs, en de

P3 DC/Cloud dienstenleverancier voorziet hiervoor de nodige opslag, tooling en beheersprocessen.

- Hierbij worden enkel Persoonsgegevens opgeslagen wanneer dit echt nodig is. De eventuele Persoonsgegevens in de logs worden na hoogstens één jaar verwijderd of geanonimiseerd, behoudens wanneer in goed gemotiveerde gevallen de DC/Cloud ICT-Dienstverlener met de betrokken Klant(en) afwijkende afspraken hebben gemaakt.
- Relevante logs worden doorgestuurd naar de Service Integrator (SI) in functie van de SIEM functie bij de SI;
    - Alle relevante informatie, zoals logs (bijv. alerts van een bepaald niveau) dienen te worden gecommuniceerd naar de globale SIEM van de VO (SIAM) voor interpretatie binnen de SIEM en de overkoepelende security monitoring.
    - Raw data zoals Logs dient steeds ad-hoc toegankelijk te zijn voor het VO SOC team om redenen van investigation/ tracking /evidence /forensics.
- De P3 DC/Cloud dienstenleverancier geeft antwoord op ad-hoc vragen inzake operationele logs, vanuit de SI of andere SPs.
- Voor nieuwe behoeften inzake organisatorische logging, zullen deze via klantenprojecten worden besteld. Voor deze behoeften kan hij beroep doen op de LOGaas dienst van HFB.
- De leverancier logt alle activiteiten (configuratie- en provisioneringsacties) op het Cloud platform, en stelt deze log ter beschikking van de betrokken entiteit.
- Bewaken van de logs m.b.t. gebruikte diensten. Hierbij worden enkel persoonsgegevens opgeslagen wanneer dit echt nodig is. De eventuele Persoonsgegevens in de logs worden na hoogstens één jaar verwijderd of geanonimiseerd, behoudens wanneer in goed gemotiveerde gevallen de DC/Cloud ICT-Dienstverlener met de betrokken Klant(en) afwijkende afspraken heeft gemaakt.

2.4.6.8 Packaging en Delivery, PAM

- Platform APIs van de Cloud management orkestratie toolset die toegepast wordt, worden beveiligd met Transport Layer Security (TLS).
- De administrator toegang tot de management tools die toegang verleent tot gebruikersinformatie klasse 3 of hoger van de VO (volgens het VO informatie classificatie raamwerk), voldoet aan de vereisten inzake Privileged Access Management:
    - sterke identificatie;
    - sterke authenticatie (MFA);
    - sterke autorisatie;
    - Logging en audit-trail van authenticatie en autorisatie acties;
    - Toegang wordt enkel verleend op een need-to-have basis; iinterventies zijn gekoppeld aan een change record in het change management systeem;

- Admin paswoorden worden bijgehouden in een beveiligde kluis, en zijn niet gekend noch visibel voor de administrators;
- en voor klasse 4 komt daarbij:
  - interventies worden goedgekeurd door een supervisor;
  - registratie van de uitgevoerde acties (camera functie);

- Bij voorkeur kan de P3 dienstverlener daarvoor beroep doen op de PAMaas, en de onderliggende WebIDM en VO-toegangsbeheer bouwstenen van HFB;
  - WebIDM biedt de nodige processen en beheersdplatformen aan voor het beheren van identiteiten, groepen en autorisaties, het delegeren en mandateren van rechten, enz.…
  - De kosten inzake gebruikerslicenties van CyberArk worden gedragen door HFB – binnen redelijke limieten –.
  - De kosten voor integratie met de HFB PAMaas (CyberArk gebaseerd) dienst, zijn op te nemen in de transitiekosten.

2.4.7 Continu versiebeheer (CloudOps/traditioneel):

Het al dan niet opzetten van continu versiebeheer dient steeds in overleg te gebeuren met de Klant of Applicatie-Dienstleverancier (dus enkel wanneer dit aangevraagd is). Desgevallend dienen upgrades en patches – al dan niet met automatisatie & scripting - zoveel mogelijk uitgevoerd worden in continue mode, waarbij updates kunnen worden gedeployed in een draaiend systeem zonder normale productiewerking te storen.

- Traditioneel: updates worden gedeployed op de omgeving. Er is slechts één omgeving op elk moment. Aanpassingen worden uitgevoerd op de bestaande instances van de IAAS/PAAS componenten.
- CloudOps: updates en patches van OS/Middleware worden verwerkt in een nieuwe release van de automatiseringsbouwsteen (IAC). Activatie van die IAC bouwsteen resulteert in één of meerdere nieuwe instanties van de IAAS/PAAS componenten met de nieuwe OS/middleware/Patch level versies. De nieuwe instances van de componenten staan naast de oude instances. Daarna gebeurt een overgang:
  - Rollend: Door geleidelijke overschakeling naar de nieuwe instances.
  - Blue/Green: Na de test van Green, worden alle sessies via de loadbalancer overgeschakeld van Blue naar Green. Hierbij delen Blue en Green dezelfde persistentielaag; Een roll-back naar Blue is steeds mogelijk.
  - Canary: Een beperkt aantal sessies worden overgeschakeld van Blue naar Green, zodat de nieuwe release in productie gaat met een minimaal risico (reductie van ‘blast area’). Als alles nog blijkt te werken wordt volledig overgeschakeld.
  - Wanneer de overschakeling volledig is, worden de oude instances gedeactiveerd en vernietigd.
  - Deze deployment aanpak kan ook gecombineerd worden met de applicatie-componenten, zodat de volledige stack dit deployment schema volgt.

2.5 Overzicht van de Cloud

2.5.1 Exploitatie

2.5.1.1 Scope en doel

Zie vorige paragrafen 2.4 Omschrijving verdere concretisering van de ondersteunende processen voor Cloud diensten en **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**;

2.5.1.2 Geconcretiseerd door

- Identificatiegegevens van de Klant die instaat voor betalingen met betrekking tot de betrokken Cloud diensten (Financieel Beheerder).
- Gevraagde dienst (Minimaal beheer / CloudOps / Traditioneel beheer).
- Beschrijving van de technische en organisatorische maatregelen voor de bescherming van de binnen het platform verwerkte Persoonsgegevens en van de verantwoordelijkheden van de Klant en de DC/Cloud ICT-Dienstverlener in dit verband. Minstens alle in artikel 30 punt 2 van de AVG opgesomde gegevens worden hierin opgenomen.
- Diensten omvatten het beheer van de beveiliging, en alle activiteiten die in VOPO document zijn opgesomd, en het toepassen van de Threat Intellegence en Threat Hunting tool.
- In geval van Traditioneel / CloudOps beheer:
    - Beschrijving van specifieke taken die uit te voeren zijn met betrekking tot de platformen, en dat kan ook automatisatie omvatten.
    - Beheerstools en de toepasselijke gebruiksmodaliteiten voor de Klant, die bij het platform horen en mee aangeboden worden, kan ook automatisatie omvatten. Incl. integratiemogelijkheden (bijv. DNS naam, te gebruiken API's, protocol en poort, …) i.f.v. een reële benutting van het platform.
    - Roadmap o.a. i.k.v. life cycle management.
    - beheer OS (patchmanagement, endpoint protection).
    - Backup van OS (traditioneel), recreëren van OS (CloudOps), backup Data .
    - Besturingssysteem (Unix/Linux), Windows).
    - Productie-, ontwikkel- of testserver.
    - Beschikbaarheidsvenster: OFWEL 24/24 7d/7d, OFWEL UKT (Uitgebreide Kantooruren).
    - Vereiste beschikbaarheid (AZ 1, 2, evt 3).
    - Vereist veiligheidsniveau.
    - Aantal gigabyte en type storage.
    - Aantal gigabyte /specifieke vereisten back-up.

- Vereiste netwerk ontsluitingen (Internet, intra-Cloud, Managed DC, Outsourced DC,..). DC/Cloud dienstenleverancier voorziet connectiviteit naar internet, de Netwerk leverancier voorziet de private ontsluitingen naar het VO netwerk.
- Netwerk dienstenleverancier (Perceel 4) levert aanvullende connectiviteit.
- Er is een exploitatiedossier voor Traditioneel / CloudOps beheer van Cloud infrastructuur- en platformen.

- Vereiste beveiligingsdiensten (ngFW, TI/TH tool,…).
- Vereiste netwerk beveiligingsparameters (virtuele netwerken, security groups, loadbalancing, DNS, ..).

2.5.1.3 SLA

2.5.1.4 Beschikbaarheid van de server- en platformdiensten

Voor de diensten CloudOPs en Cloud Traditioneel zijn dezelfde bepalingen als bij “managed DC” in paragraaf 3.6.2 SLA van toepassing;

2.5.1.4.1 Specifieke bepalingen voor cloud diensten

Voor het gedeelte dat door de DC/Cloud ICT-Dienstverlener in onderaanneming aan een publieke cloud-aanbieder wordt toevertrouwd, geldt de door die publieke cloud-aanbieder aangeboden SLA. De gevraagde beschikbaarheid dient minimaal gelijk te zijn aan de officieel gecommuniceerde beschikbaarheid van de cloud-aanbieder(s).

Voor de kostprijs die betrekking heeft op Cloud Deel 1a in het prijsmechanisme: bij het niet naleven dient een prijscorrectie van toepassing te zijn die minimaal gelijk dient te zijn aan de officieel gecommuniceerde penaliteiten van de cloud-aanbieder(s).

Voor cloudOps en Cloud Tradtioneel (Cloud Deel 2 en Cloud Deel 3 in het prijsmechanisme) geldt de beschikbaarheids-SLA zoals beschreven in “managed DC” in paragraaf 3.6.2 SLA wel ten volle, wanneer er gebruik gemaakt wordt van een multi-AZ en redundante infrastructuur- en platformlaag, onderliggend aan een applicatieservice; De SLA wordt in dat geval berekend op basis van de beschikbaarheid van het geheel van de infrastructuurcomponenten (de “laag”) die instaan voor de applicatieservice,

- bv een applicatie service runt op een “laag” die bestaat uit een set van 3 IAAS servers verspreid over 2 of meer AZ’s; Wanneer 1 IAAS server faalt, maar de andere 2 (in andere AZs) niet, en de applicatieservice kan verder runnen, dan wordt de SLA niet berekend op basis van de onbeschikbaarheid van de ene IAAS server, maar op de beschikbaarheid van het geheel van de 3 IAAS servers;

Voor platformen van een publieke cloudaanbieder dient het 24/24 7/7 beschikbaarheidsvenster steeds van toepassing te zijn;

Dat geldt ook voor de additionele beveiligingscomponenten die in de publieke cloud omgeving geplaatst worden; Voor deze beveiligingscomponenten gelden dezelfde bepalingen als bij “DC netwerk en beveiligingscomponenten” in “managed DC” in paragraaf 3.6.2 SLA;

2.5.1.4.2 Antwoordtijd voor het beantwoorden van support vragen

Voor het beantwoorden van support vragen dient het volgende te worden gerespecteerd:

- Beantwoorden van support vragen via mail.
- Telefonische ondersteuning op afspraak, met voldoende flexibiliteit voor het maken van afspraken (tijdens kantooruren).
- Minimaal de Engelse taal perfect beheersen.
- Antwoorden dienen kwalitatief afdoende te zijn, technisch gedetailleerd en onderbouwd met kennis van zaken
- Antwoordtijden volgens prioriteit:
    - P1 – businesss kritisch, antwoord binnen de 4 uur verwacht (kantooruren)
    - P2 – medium kritisch, antwoord binnen de 24 uur verwacht
    - P3 – niet kritisch, antwoord binnen de 48 uur verwacht

2.5.1.5 Prijsmechanisme

De prijs voor de Exploitatie op infrastructuur van een publieke cloud-aanbieder wordt opgebouwd op basis van :

- **Dienst Minimaal beheer: Cloud Deel 1**
- **Dienst CloudOps beheer: CloudDeel 1 + Cloud Deel 2**
- **Dienst Traditioneel beheer: Cloud Deel 1 + Cloud Deel 3**

Aanvullend worden ook kosten aangerekend voor de bijkomende beveiligingsdiensten in de cloud die de klant inzet, zoals de Next-Gen FW (ngFW)

- Het betreft hier maandelijkse eenheidsprijzen die per beveiligingsdienst en per eenheid worden verrekend aan de klant;
- Alle kosten inzake de hulpmiddelen voor het leveren van de cloud infrastructuurdiensten, en alle ondersteunende systemen zoals hardware, software licenties, operationeel beheer, monitoring, logging, opslag van logs,, doorsturen van logs, … zijn in de prijs van de diensten inbegrepen;
- De forfaitaire maandelijkse eenheidsprijs voor het ter beschikking stellen van een Next-Gen FW (ngFW) in de publieke cloud.
    - Het betreft hier een maandelijkse eenheidsprijs die per virtueel systeem wordt verrekend aan de klant, volgens throughput/bandbreedte,
        - € per 200 Mbps virtueel systeem
        - € per 500 Mbps virtueel system
        - € per 1000 Mbps virtueel system

Aanvullend worden ook kosten aangerekend voor de VO-specifieke contracten die nodig zijn voor de te beheren platform- en serverinstanties en die maandelijks verrekend worden;

- Het betreft hier de in de VO-specifieke contracten afgesproken Eenheidsprijzen die maandelijks of jaarlijks per eenheid worden verrekend aan de klant;
- Voor VO-specifieke contracten die gebruikt worden voor meerdere Klanten, wordt een zo correct mogelijke versleuteling gebruikt

Deel 1

Voor minimaal beheer en voor traditioneel beheer dienen prijzen op basis van minstens 2 publieke cloud-aanbieders te worden opgegeven;

Hierbij dient bij aanvang van het contract een continuïteit geleverd te worden van de bestaande diensten, waarbij publieke cloud-aanbieder 1 AWS is, en publieke cloud-aanbieder 2 Azure is; Hierbij geldt dat er geen migratiekosten geïntroduceerd kunnen worden voor de toepassingen die actueel al op publieke cloud diensten steunen.

In deze prijzen zijn alle prestaties en alle facilitaire en broker kosten van de DC/Cloud ICT-Dienstverlener en alle benodigde (beheers) en ondersteuningsprocessen en tools inbegrepen.

Alle kosten inzake de hulpmiddelen voor het leveren van de cloud infrastructuurdiensten, en ook alle ondersteunende systemen zoals hardware, software licenties, operationeel beheer, monitoring, logging, opslag van logs,, doorsturen van logs, … zijn in de prijs van de diensten inbegrepen;

De prijs voor Exploitatie op infrastructuur van de publieke Cloud Provider 1 en 2 (minimaal beheer) bestaat steeds uit :

- DEEL 1.A. De eenheidsprijs voor het beheer van platform- en infrastructuurdiensten van de cloud aanbieder. De structuur wordt in volgende paragraaf toegelicht.
  - De eenheidsprijs voor het beheer van platform- en infrastructuurdiensten van de Cloud Provider 1;
  - De eenheidsprijs voor het beheer van platform- en infrastructuurdiensten van de Cloud Provider 2;
- DEEL 1.B. Optionele vaste forfaitaire kost per maand per aparte VO-klant voor het beheer van platform- en infrastructuurdiensten van alle Cloud Providers samen;
  - Dit laat de leverancier toe om de kosten van het Cloud *minimale* beheer forfaitair aan te rekenen, i.p.v. als een marge op het gebruik; Vooral voor grote volumes is dat van belang.

Toelichting over Deel 1.A.

De structuur van de eenheidsprijs voor het beheer van platform- en infrastructuurdiensten van de cloud aanbieder bestaat uit:

- De eenheidsprijs (1 + X) is gedefinieerd als de listprijs van 1 € van de publieke cloud MINUS de eventuele servicecredits, en PLUS de eventuele marge; Bemerk dat de resulterende eenheidsprijs ook kleiner kan zijn dan 1,00

- Voorbeeld:
  - De eenheidsprijs is: 1,00 minus servicecredits plus marge;
    - Voorbeeld: eenheidsprijs is 1,00 – 0,05 + 0,09 = 1,04
  - In de financiële bijlage wordt het afgenomen volume van de cloud diensten volgens de listprijs, vermenigvuldigd met de eenheidsprijs om het aan de VO gefactureerde bedrag te bepalen:
    - Vb volume aan clouddiensten is 100.000 € per maand volgens de listprijs
      - Dan is het gefactureerde bedrag: 100.000 € x (1,04) = 104.000 € per maand

Cloud Deel 2.

Deel 2 bestaat uit een recurrente maandelijke prijs voor de exploitatie van de Cloud Provider diensten, die in grote mate steunt op een ontwikkelde automatisatie;

Alle kosten inzake de hulpmiddelen voor het leveren van de cloud infrastructuurdiensten, en ook alle ondersteunende systemen zoals hardware, software licenties, operationeel beheer, monitoring, logging, opslag van logs,, doorsturen van logs, … zijn in de prijs van de diensten inbegrepen;

Het prijsmodel is gebaseerd op drie elementen

- **DEEL 2.A.** De eenheidsprijs per maand voor het beschikbaar houden van CloudOps Vserver instanties, volgens OS-type, SLA (24/7 of Uitgebreide kantooruren). Deze eenheidsprijs omvat alle beheerstaken voor de exploitatie en beveiliging van de CloudOps Vserver;

  DEEL 2.B. De eenheidsprijs per maand voor het beschikbaar houden van middleware instanties. Deze prijzen zijn dezelfde aan de beheerskosten voor “Managed DC middleware” in het prijsmodel van het managed DC – zie 3.6.3 Prijsmechanisme . Deze omvat alle beheerstaken voor de explotatie en beveiliging van een middleware platformlaag instantie, zoals bv het up-and-running houden van een Web Server, Application Server, RDBMS-server, enz…

  DEEL 2.C. De exploitatiekosten die betrekking hebben op het beheer van de automatiseringsbouwstenen, en op de beheerstaken voor het geheel van de infrastructuur- en platformlaag die middels deze automatiseringsbouwstenen worden uitgevoerd; Deze kosten hebben betrekking op
  - het onderhoud en het beheer van de automatiseringsbouwstenen,
  - de beheerstaken die uitgevoerd worden door middel van deze automatiseringsbouwstenen en die betrekking hebben op geheel van de infrastructuur- en platformlaag die onderliggend is aan een applicatie, zoals beschreven in dit hoofdstuk en bovenstaande paragraaf 2.4.2 CloudOps beheer in het bijzonder;
  - Deze prijs zal bepaald worden in functie van de omvang en de complexiteit van de deze automatiseringsbouwstenen en de beheerstaken, en zal verschijnen als “beheerkost” in het projectvoorstel van de leverancier; De ontwikkeling van de deze automatiseringsbouwstenen waarop CloudOps beheer steunt, gebeurt via de uitvoering van een project; het projectvoorstel van de leverancier zal de eenmalige ontwikkelkost

én de maandelijkse exploitatiekost bepalen; Bij de bepaling van de eenmalige ontwikkelkost en beheerskost zal de leverancier de profielprijzen die in het DC/Cloud contract vastgelegd worden, toepassen;

In deze prijzen zijn alle prestaties en alle facilitaire en andere kosten van de DC/Cloud ICT-Dienstverlener en alle benodigde (beheers) en ondersteuningsprocessen en tools inbegrepen.

Cloud Deel 3.

De prijs voor Exploitatie (Traditioneel beheer) op infrastructuur van een publieke Cloud Provider bestaat uit:

- **DEEL 3.A** De eenheidsprijs per maand voor het beschikbaar houden van traditionele IAAS Vserver instanties. Deze prijzen zijn dezelfde aan de beheerskosten in het prijsmodel van het managed DC.
- **DEEL 3.B** De eenheidsprijs per maand voor het beschikbaar houden van traditionele middleware instanties. Deze prijzen zijn dezelfde aan de beheerskosten voor “Managed DC middleware” in het prijsmodel van het managed DC – zie 3.6.3 Prijsmechanisme

In deze prijzen zijn alle prestaties en alle facilitaire kosten van de DC/Cloud ICT-Dienstverlener en alle benodigde (beheers) en ondersteuningsprocessen en tools inbegrepen.

Alle kosten inzake de hulpmiddelen voor het leveren van de cloud infrastructuurdiensten, en ook alle ondersteunende systemen zoals hardware, software licenties, operationeel beheer, monitoring, logging, opslag van logs,, doorsturen van logs, … zijn in de prijs van de diensten inbegrepen;

Voor infrastructuur/platform componenten, andere dan IAAS Vservers, die niet vermeld worden in de financiële bijlage, en die later toegevoegd worden, geldt dat de prijs van het beheer van die toegevoegde infrastructuur componenten markconform dient te zijn;

indien de toegevoegde infrastructuurcomponenten vergelijkbaar zijn met de infrastructuur componenten in de lijst, dan dient de prijs voor het beheer ervan in lijn te zijn met de prijsopgave binnen deze lijst, waarbij een extrapolatie zal toegepast worden, bv op basis van verwerkingscapaciteit zoals rekenkracht (vCPU) en throughput, opslagcapaciteit, enz… of gelijkaardige beheertaken en nodige effort voor beheer van de component.

2.5.1.6 Facturatie

Maandelijks wordt de factuur overgemaakt aan de Klant die de bestelling heeft geplaatst. Deze factuur bevat per type dienst:

- CLOUD Deel 1
    - DEEL 1.A; Kosten voor publiek cloud diensten:
        - het afgenomen volume van de cloud diensten van Cloud Provider 1 volgens de listprijs, vermenigvuldigd met de eenheidsprijs voor Cloud Provider 1;
        - het afgenomen volume van de cloud diensten van Cloud Provider 2 volgens de listprijs, vermenigvuldigd met de eenheidsprijs voor Cloud Provider 2;
    - DEEL 1.B; De optionele vaste forfaitaire kost per maand per aparte VO-klant;
- CLOUD Deel 2
    - Deel 2.A. Kosten voor het beschikbaar houden van CloudOps IAAS Vserver instanties
    - Deel 2.B. Kosten voor het beschikbaar houden van CloudOps middleware instanties
    - Deel 2.C. De exploitatiekosten die betrekking hebben op het beheer van de automatiseringsbouwstenen, en op de beheerstaken voor het geheel van de infrastructuur- en platformlaag die middels deze automatiseringsbouwstenen worden uitgevoerd
- CLOUD Deel 3
    - Deel 3.A. Kosten voor het beschikbaar houden van CloudOps en Traditioneel IAAS Vserver instanties
    - Deel 3.B. Kosten voor het beschikbaar houden van CloudOps en Traditioneel middleware instanties
- CLOUD. Kosten voor de VO-specifieke contracten die nodig zijn voor de te beheren platform- en serverinstanties en die maandelijks verrekend worden;
- CLOUD Kosten voor bijkomende beveiligingsdiensten in de cloud;
- Indien de SLA m.b.t. de beschikbaarheid van de cloud-dienst(sn) niet gehaald wordt dan is een Prijscorrectie van toepassing die minimaal gelijk dient te zijn aan de officieel gecommuniceerde penaliteiten van de cloud-aanbieder(s).

2.5.1.7 Rapportering

Maandelijks wordt per Klant een overzicht gegeven van :

- De SLA-metrieken en gerelateerde penaliteiten
- Rapportering van de als onderbouwing van de facturen vereiste gegeven waaronder de hoeveelheden van alle verbruikte cloud-diensten in de voorbije periode

2.5.2 Eenvoudige Werkaanvragen

Het bestelproces voor het afnemen van Cloud diensten dient volledig geautomatiseerd te zijn.

Eenvoudige wijzigingen aan de platformen van de publieke cloud-aanbieder worden door de Klant zelf ingebracht via een hiervoor voorziene portaal of – indien specifiek gevraa–d - in regie door de DC-Dienstleverancier.

2.5.2.1 Aanvragen voor aanmaak cloud account

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een set van nieuwe cloud accounts aan te maken, te wijzigen of te wissen voor minimaal beheer. Het kan gaan om een enkele account, maar ook om een (set) aantal tot 10 accounts; De aanvraag maakt melding van het type account (‘minimaal’, ‘CloudOps’, ‘traditioneel’).

2.5.2.1.1 SLA voor aanmaak cloud account

2.5.2.1.1.1 Tijdige uitvoering van Eenvoudige Werkaanvragen i.k.v. cloud accounts

Beschrijving en definitie

Per Dienst zal gemeten worden of deze Dienst binnen de contractuele Service level (zie in onderstaande tabel opgenomen uitvoeringstermijnen) of de met de Klant afgesproken uitvoeringstermijn werd uitgevoerd.

De met de Klant afgesproken uitvoeringstermijn kan niet korter zijn dan de contractuele Service Level en dient gestaafd te kunnen worden door een akkoord van de betrokken Klant (bv. Een e-mail).

	Service Level (uitvoeringstermijn)
Aanmaken cloud account	8 uur

Service Level

100 %.

Randvoorwaarden, assumpties en uitzonderingen

De uitvoering van dit Dienstenpakket gebeurt tijdens de Kantooruren.

Meetelementen en -methode

Voor elke Werkaanvraag wordt op de Service desk het tijdstip van indiening van de Werkaanvraag en het tijdstip van afsluiten geregistreerd. Indien de Werkaanvraag uit verschillende Diensten bestaat worden dezelfde gegevens per Dienst geregistreerd.

De registratie bestaat uit:

- Datum en uur van indiening de Werkaanvraag;
- Datum en uur van het einde van de uitvoering van alle activiteiten m.b.t. de Dienst;
- Datum en uur goedkeuring door de Klant van de Dienst/Werkaanvraag;

Mislukt een eerste poging om de Dienst succesvol uit te voeren, dan volgt hiervoor niet de goedkeuring door de Klant, maar een terugmelding door de Klant naar de Service desk zodat dit geregistreerd en opgevolgd kan worden. De uitvoering van de Dienst wordt pas afgesloten na succesvolle afwerking ervan en na expliciete goedkeuring door de Klant en na aanpassing van de gegevens in de Configuratiedatabank. Ingeval een terugmelding gebeurt, omdat de Klant niet tevreden is over de uitvoering (zowel op niveau van de Werkaanvraag als op het niveau van de Dienst), wordt de registratie als volgt aangevuld:

- Datum en uur van deze terugmelding;
- Datum en uur van het einde van de nieuwe acties;
- Datum en uur goedkeuring door de Klant;

De registratie herhaalt zich tot het moment dat de Klant zijn goedkeuring geeft.

Na goedkeuring door de Klant van de Dienst:

- Datum en uur afsluiten van Dienst/Werkaanvraag;

De volledige uitvoeringstermijn voor een Dienst wordt berekend als volgt:

- De looptijd tussen het tijdstip waarop de Dienst toekomt bij de Service desk (=datum van indiening) of het tijdstip dat de uitvoering kan starten (in het geval een afhankelijke Dienst besteld binnen dezelfde Werkaanvraag is uitgevoerd) en het tijdstip van het einde van de uitvoering van alle activiteiten van de Dienst volgens de DC/Cloud ICT-Dienstverlener;
- Indien de interventie niet wordt goedgekeurd door de Klant en er bijgevolg een terugmelding gebeurt, wordt de uitvoeringstermijn vermeerderd met de tijd tussen begin- en eindtijd van elke bijkomende activiteit, totdat de Klant de Dienst heeft goedgekeurd.

Dit betekent dat de uitvoeringstermijn, die zal getoetst worden aan de Service Level, enkel de effectieve uitvoeringstermijn berekent tot de Dienst is afgesloten, en niet de tijd nodig voor goedkeuring door de Klant.

2.5.2.2 Aanvragen voor ‘traditioneel beheer’ IAAS/PAAS diensten

Deze aanvragen (en gerelateerde SLA’s) zijn identiek als die van het ‘managed DC (zie verder).

3 Managed Datacenter

3.1 Specifieke omschrijving

Het managed DC aanbod zal een antwoord bieden op de doelstelling om het aantal decentrale datacenters af te bouwen en de versnippering van het VO DC landschap te verminderen, en kan fungeren als een CZF buffercapaciteit om consolidaties van eigen-VO datacenters uit te voeren. Ook het IAAS/PAAS aanbod binnen het managed DC aanbod staat in functie van het verminderen van een verspreiding van de VO applicaties over tientallen datacenters (VO en extern), en dus een verbetering van de kostenefficiëntie (vermindering van de kosten op vlak van applicatie-integratie, applicatiebeheer, netwerken, netwerkbeveiliging, securitybeheer, enz… die hieruit voortvloeit) en verbetering van de duurzaamheid (energieverbruik, PUE en benuttingsgraad).

Het managed DC zal zorgen voor de continuïteit van de huidige (en voornamelijk dan ‘legacy’ ICT toepassingen) dewelke in een hybride DC/cloud constellatie dient opgezet te worden. Het Managed DC zal draaien op infrastructuur uitgebaat door de DC/Cloud ICT-Dienstverlener als een Private Cloud: het betreft infrastructuur en platformen d“e "as a serv”ce" worden afgenomen en draaien op private infrastructuur van de DC-Dienstverlener.

Voor de “managed DC” IAAS/PAAS diensten ligt de lat op vlak van automatisatie lager dan public cloud: hier zijn afwijkingen ten aanzien van volledige automatisatie mogelijk in functie van wat technisch en financieel haalbaar is, of waar het gevraagde afwijkt van een standaard aanbod. Wat niet afgedekt wordt door de webinterface/API/automatisatie wordt opgevangen via een change-request proces en deels manuele verwerking. Er zullen voor het managed DC geen minimum vereisten rond automatisatie worden opgelegd. De resultante is dat de dienstverlening en de werkingsprocessen van het managed DC de karakteristieken heeft van een ‘traditioneel DC’, wat natuurlijk zijn repercussies heeft op kostenefficiëntie, rendement en personeelsinzet.

Een structureel aanbod van IAAS/PAAS diensten van het ‘managed DC’ zal dus door de DC-Dienstverlener dienen te worden geleverd. De Applicatie-dienstverleners kunnen zelf alleen in bepaalde mate (eerder uitzonderlijk) specifieke platform services of infrastructuur componenten inbouwen in de toepassingslaag, indien niet aanwezig in het IAAS/PAAS aanbod, en dit verantwoord is. De beslissing hieromtrent dient ter regularisatie onderworpen te worden aan een governance/approval proces waarbij HFB de evaluatie maakt en de beslissing tot goedkeuring neemt (ttz ifv behoeften, kwaliteit van het aanbod, impact mbt integratie, meerkosten, oplijning met visie & architectuur, veiligheid, cataloogbeheer etc.).

De functionele en technologische breedte en diepte van het “managed DC” IAAS/PAAS aanbod, zal op de meeste domeinen heel wat beperkter zijn dan wat we terugvinden in het public cloud aanbod en zal zich beperken tot basis IAAS diensten en een aantal basis PAAS diensten zoals databases en basis van eerder traditionele middleware (standaard applicatie server, webserver). De voorgestelde tools dienen traditionele platform management mogelijkheden te kunnen bieden zoals provisioning, configuratie, tuning, tracking, versiebeheer en staging. Vereisten zijn ook het continu respecteren van de grenzen (en tracking hierover) tussen de verschillende gebruikers (tenants), en het beheer van een variabele toewijzing van resources.

Ter illustratie mbt containermanagement: binnen hyperscale cloud zijn er meerdere PAAS diensten voor container management. Voor Managed DC zijn die niet in dezelfde brede en toegankelijke vorm en zal ook niet verwacht worden dat de DC/Cloud ICT-Dienstverlener container management systemen in enige vorm levert.

Het technologisch up-to-date houden en het eventueel bijsturen van de capaciteit in functie van de noden, maken ook deel uit van deze dienstverlening. Dit omvat zowel het regelmatig monitoren, evalueren en waar nodig bijsturen of optimaliseren van de betrokken hard- en software- componenten (o.a. via patches, Updates, Upgrades) als het periodiek herzien (in een meerjarencontext) van de technologische keuzes, alsook de migratie naar de nieuwe platformen. Hierbij wordt maximaal gebruik gemaakt van open standaarden en worden open source alternatieven mee overwogen.

Bij een Managed DC is de DC/Cloud ICT-Dienstverlener 'Design Autoriteit' en dus integraal verantwoordelijk voor de architectuur.

3.2 Meerwaarden voor de Klanten

- Verlaging van de administratieve lasten voor het afnemen van 'managed' datacenterdiensten
- Schaalvoordelen op het vlak van prijs en kwaliteit en gebruik van beste praktijken voor de standaard datacenterdiensten
- Uitbesteding van licentiebeheer
- Garanties op beschikbaarheid ondersteund door afdwingbare Service Level eisen. Garanties op kwaliteit (beschikbaarheid, performantie, beveiliging) met mogelijkheid tot differentiatie (o.a. in SLA's)
- Voldoende capaciteit en flexibele uitbreidingsmogelijkheden
- Modulaire afname mogelijk in functie van de noden
- Transparante prijsstructuur (per vastgelegde eenheid) in functie van de afnames en de evolutie in de tijd. Voor wat betreft het 'Managed DC' zijn de aan te kopen items beperkt waarbij er wel een meetstaat met cataloog items met eenheidsprijzen kan worden opgemaakt
- Mechanismen voor samenwerking met andere diensten (service interfaces)
- Een performante monitoring van de beheerde omgevingen en een efficiënte behandeling van eventuele incidenten en problemen
- Het Facilitair Bedrijf wil het gebruik van compacte datacenters met een hoge energie-efficiëntie verder stimuleren zodat we meerwaarden kunnen realiseren op het vlak van kost en energie-efficiëntie

3.3 Gevraagde kenmerken

3.3.1 Het managed DC

3.3.1.1 Vereisten - algemeen

Er wordt een 'managed DC' IAAS/PAAS dienst voorzien die geleverd wordt door de DC-Dienstenleverancier. Dit aanbod staat in functie van continuïteit van de bestaande applicaties. Het managed DC IAAS/PAAS aanbod heeft de karakteristieken van een traditioneel DC. Een overzicht:

- Het managed DC beantwoordt aan de vereisten van hoge duurzaamheid door gebruik te maken van (next-gen) energie-efficiënte technologie van de laatste generatie voor hoge duurzaamheid (hoge energie-efficiëntie, PUE, hardware, etc.) en ook de benuttingsgraad is minstens 60%:
- Het managed DC IAAS/PAAS aanbod beantwoordt aan de vereisten van pay-as-you-use/grow OPEX pricing model.
- Het 'Managed DC' dient 100% te worden aangeboden aan de VO door de DC/Cloud ICT-Dienstverlener, maar de DC/Cloud ICT-Dienstverlener hoeft daarom niet zelf de eigenaar te zijn. Subcontracting is toegestaan.

Het managed DC omvat alle Diensten m.b.t. het ter beschikking stellen en houden van verwerkingscapaciteit (op fysieke en virtuele servers), opslagcapaciteit (met of zonder back-up), netwerkcomponenten, in combinatie met de onderliggende computerzaalfaciliteiten en het provisioneren en beheren van enkele meer gestandaardiseerde platformen (databankplatformen, webservers en applicatieservers), maw het provisioneren en beheren van Infrastructuur en platformen. Deze gestandaardiseerde platformen worden ook ter beschikking gesteld van ontwikkelteams, zowel interne als externe (vb. via het raamcontract voor ontwikkelingen), die op basis van deze platformen toepassingen kunnen ontwikkelen en deze op een soepele manier in productie zetten en ter beschikking stellen van Gebruikers.

Er worden zowel productieomgevingen als omgevingen voor ontwikkeling en test aangeboden (non-productie-omgevingen).

Mee in scope van infrastructuur "as a service" en platform "as a service" zijn de bijhorend aangeboden hulpmiddelen (beheers- en ontwikkelingstools) en interfaces die de Klant (beheerder aan Klantzijde) in staat moeten stellen de server verwerkingscapaciteit en/of het platform te benaderen en zo effectief mogelijk te benutten. Deze omvatten de nodige beheerstools (geïntegreerde selfservice management tools) die via webinterface ter beschikking gesteld worden. Deze omvatten self-service provisioning, configuratie, een vorm van monitoring en administratie, en andere functies (bv. gedeeltelijke self- service monitoring, beheermogelijkheden voor sommige capacity en performance parameters van de middleware diensten van de PaaS, een mogelijk beperkte vorm van versiebeheer....).

Tevens krijgt de Klant samen met de infrastructuur as a service en/of het platform de nodige gebruiksinstructies en (vooringestelde) integratie-parameters (voorbeeld te gebruiken DNS naam, poort, protocol, enz.. voor zowel beheer als gewoon gebruik).

De Diensten worden zoveel mogelijk onder de vorm van van “Infrastructure as a Service” en “Platform as a Service” met het “pay-as-you-use”-model aangeboden. Het betreft “all-in” diensten waarbij alle voor de diensten noodzakelijke componenten zijn inbegrepen (investering en beheer van onderliggende infrastructuur, computerzaal, contracten, licenties, interfaces…).

Tijdens de uitvoering van de overeenkomst zal er steeds een breed aanbod van PaaS diensten beschikbaar zijn dat de marktevolutie volgt.

3.3.1.2 Vereisten datacenter

- Het voorgestelde ‘managed DC’ is van het type twin-DC maar beide datarooms/datacenters mogen gelokaliseerd zijn op één fysieke campus zolang binnen het DC twee aparte fysiek gescheiden Availability Zones kunnen worden gerealiseerd op basis van aparte en volledig gescheiden CZF diensten; deze twin-DC opzet moet volledig operationeel zijn van dag 1, en zonder bijkomende kosten of vertragingen onmiddellijk kunnen toegepast worden, met exact dezelfde functionele en technische karakteristieken, connectiviteit, IAAS/PAAS dienstenaanbod enz… over de twee DC’s.
- Principe van shared hosting waarbij onderliggende compute/storage capaciteit de facto gedeeld wordt met andere organisaties, ook buiten de VO. De volledige capaciteit wordt zo over meerdere accounts verspreid, wat de benuttingsgraad, duurzaamheid en schaalvoordeel vergroot;
- CZF, bestaande uit de housing van beveiligde racks, met bijhorende rack- en cabling services.
- De onderliggende CZF van het ‘managed DC’ dient minstens van het ‘type III’ te zijn (normering TIA 942-A inzake elektriciteit, brandbeveiliging, water, koeling, bewaking & controle, etc.).
- **Beschikbaarheid**: het kunnen realiseren van zeer hoge beschikbaarheid van applicatiefuncties en data (> 99,95%), door
    - het kunnen opvangen van meerdere fouten binnen HW en SW componenten, zoals
        - redundantie binnen de server hardware, bv redundantie van de voeding;
        - redundantie binnen het storage hardware, bv redundantie van de voeding en kritische componenten; RAID,
        - redundantie dmv de server virtualisatie, bv Vmotion of herstarten van de Vserver image op de andere site;
        - redundantie over het twin-DC, door storage replicatie, en door een Active-Active server opstelling, of een Active-Passive server opstelling;
        - offsite backup van data;
    - door het aanbieden van twin-DC of twee Availability Zones;
- Mogelijkheid virtualisatie op basis van één of meerdere type hypervisors
- Het ‘managed DC’ dient zich te bevinden binnen de grenzen van de EU lidstaten op 31 dec 2022 met uitzondering van het VK.
- Het ‘managed DC’ kan een netwerk latency van max 30 ms roundtrip ondersteunen naar systemen in Brussel;
    - Uitzondering op deze regel is het aanbod van Managed SMB File Server diensten; Hier is de maximale netwerk latency van max 4 ms roundtrip van tel. Deze dienst mag gerealiseerd worden in een enkelvoudig DC dat apart staat van de rest van het ‘managed DC’ dienstenaanbod;

  - Evenwel dient de data backup van deze dienst te gebeuren op een andere CZF of DC, op minstens 5 KM afstand;
  - De onderliggende CZF van deze dienst, dient op de hoofdlocatie minstens van het 'type III' te zijn (normering TIA 942-A inzake elektriciteit, brandbeveiliging, water, koeling, bewaking & controle, etc.).

- Het managed DC volgt de technologische evolutie op vlak van DC-infrastructuur in de markt, en biedt OS en server-HW features aan binnen de 12 maanden dat deze GA zijn. Het managed DC kan op geen enkel moment steunen op "end of (service) life" componenten waarvan de ondersteuning bij de leverancier ofwel ontbreekt, ofwel verminderd is, ofwel waarbij er continuiteitsrisico's zijn.
- Het 'managed DC' zal verder:
  - gelegen zijn in een geografisch gebied met een laag risico; voldoende maatregelen zijn getroffen tegen overstroming (ifv het max. volume water gemeten per m2 in dit gebied de vorige 30 jaar);
  - bouwkundig voorzien zijn om schade in geval van aardbevingen te vermijden;
  - zich niet bevinden in een gebied met risico op afschakeling van elektriciteit: https://economie.fgov.be/nl/themas/energie/bevoorradingszekerheid/elektriciteitsschaarste/afschakelplan-voor;
  - zich niet bevinden in een risico zone of in de buurt van Seveso sites.
- Het managed DC dient een failover mogelijk te maken naar een DR locatie (waarbij dus ook verschillende DR-RPO en DR-RTO waarden van toepassing zullen zijn) en bijgevolg ook de noodzaak voor ondersteuning van een minimale set van active-active configuraties van oa storage op basis van (al dan niet synchrone) replicatie;
  - indien beide datarooms/datacenters van het twin-DC concept, voldoen aan minimum voorwaarden, kan het tweede DC ook als DR-DC gebruikt worden.
  - Deze minimum voorwaarden zijn:
    - OF aansluiting op een verschillend substation van het hoogspanningsnetwerk en een autonomie van de eigen stroomvoorziening van 12u
    - OF een autonomie van de eigen stroomvoorziening van 24u;
    - ver genoeg van elkaar verwijderd zijn (> 5km in vogelvlucht);

3.3.1.3 Vereisten netwerk connectiviteit

- DC/Cloud ICT-Dienstverlener zal verantwoordelijk zijn voor de connectiviteit 2 x 10 Gbit/s (redundant) naar de glasvezel backbone van de Vlaamse overheid (op twee verschillende VO POP's) en alle kosten hieromtrent op zich nemen. Meer informatie aangaande de locaties van de VO POP's kan teruggevonden op: https://overheid.vlaanderen.be/netwerkdiensten/oplossingen/datacenters

- Het managed DC laat het gebruik en integratie met VO-netwerk oplossingen toe, zoals het gebruik van VO private IP address space, routeringsoplossingen met VO interne netwerken, integratie met de DNS service van de VO;
- Ook binnen het managed DC, gebruik van VO-netwerk oplossingen toelaten zoals het gebruik van VO private IP address space & routeringsoplossingen met VO interne netwerken.
- Redundante en voldoende performante Internet toegang leveren op basis van 2 verschillende ISP's.

3.3.1.4 Vereisten IAAS diensten

- Het 'managed DC' dient voornamelijk basis IAAS aan te bieden (dus t.e.m. provisionering van het OS en optioneel ook OS beheerstaken zoals patching) en een aantal basis-PAAS diensten zoals bijv. een aantal specifieke database of web services die actueel nog van tel zijn. De AM Leveranciers zullen de hogerliggende middleware frameworks en container management functies voor hun rekening nemen gezien de complexiteit van de demarcatie in niet (volledig) geautomatiseerde omgevingen.
- Principe van shared hosting waarbij onderliggende compute/storage capaciteit de facto gedeeld wordt met andere organisaties, ook buiten de VO. De volledige capaciteit wordt zo over meerdere klanten gedeeld;
- Multi-Tenancy – het ondersteunen van de autonomie van de entiteit, door het aanbieden van volledig afgescheiden virtuele omgevingen (op alle vlakken: netwerk/subnet, netwerkbeveiliging, Vservers, storage volumes, etc) en het volledig vermijden van interferentie tussen 'tenants'. Een belangrijke vereiste behelst het kunnen scheiden van verschillende 'run' omgevingen van verschillende VO-entiteiten, Applicatie-Dienstleveranciers, ontwikkelingslandschappen, security classificaties etc.
- Een schaalbare server/compute/storage/backup infrastructuur aanbieden waarop Applicatie-Dienstleveranciers applicatieservers kunnen inrichten ;
- Op een robuuste wijze kritieke DC netwerk services aanbieden; performante connectiviteit (IP en/of fiber-gebaseerd waar relevant) aanbieden tussen server- en opslag infrastructuur enerzijds en de netwerking componenten anderzijds ;
- Een aanbod van fysieke servers en Vserver op gevirtualiseerde server-infrastructuur;
    - De volgende Fserver types worden voorzien:

IAAS server - Ter beschikking gestelde fysieke server Small 8 cores, 16 Threads, 32 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Small 10 cores, 20 Threads, 32 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Medium 8 cores, 16 Threads, 64 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Medium 10 cores, 20 Threads, 64 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Large 16 cores, 32 Threads, 384 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Large 20 cores, 40 Threads, 384 GB RAM
IAAS server - Ter beschikking gestelde fysieke server XLarge 32 cores, 64 Threads, 512 GB RAM
IAAS server - Ter beschikking gestelde fysieke server XLarge 40 cores, 80 Threads, 512 GB RAM

  - Bemerk dat de DC/Cloud dienstenleverancier een keuze kan maken om het aanbod te beperken tot één Fserver type Small, Medium, Large, XLarge, dus ofwel de CPU types met 8,16,32 cores ofwel de CPU types met 10,20,40 cores; De eenheidsprijzen hebben nog betrekking op alle types;

- De server infrastructuur volgt de technologische evolutie inzake server hardware en software, zoals inzake CPUs, geheugen, server-backplane, IO, bandbreedte op de servers, bandbreedte van het storage-netwerk tss servers en storage en tss storage en backup, bandbreedte en encryptie van de communicatie tussen servers en applicaties, ….
- Fysieke opslagcapaciteit aanbieden die schaalbaar en performant is, en die logisch zal worden aangeboden volgens een 'tiered' model.
  - **Storage Tier 1**: SSD, Storage zonder roterende media (SSD of flash of gelijkwaardig); I/O size 256 KB,latency-sensitive, transactional workloads (> 5000 IOPS/TB)
  - **Storage Tier 2**: HDD, Indien een harde schijf geen SSD schijf is, dient de vermelde rotatiesnelheid 15K RPM te zijn voor Tier 2; I/O size 1024 KB, frequently accessed, "sustained throughput" intensive workloads, 15K RPM (> 500 IOPS/TB)
  - **Storage Tier 3**: HDD, infrequently accessed workloads, archiving/NAS etc, minimal 10K RPM
- De storage oplossing bestaat uit
  - **Non-replicated storage**: enkel op één site, A of B
  - **Replicated** storage omvat 2 copieën, elk op site A en B, en de Storage replicatie;
- Storage technieken zoals snapshots, autotiering en deduplicatie dienen ondersteund te zijn, en op aanvraag ingericht te worden in kader van een project werkaanvraag.
  - Er is de mogelijkheid om voor specifieke volumes on-site snapshots te nemen op de storage, volgens het schema in functie van de klantenvereisten;
  - Er kan een restore uitgevoerd worden vanuit de snapshots;
  - De aanvraag voor een restore uit een snapshot kan opgestart ofwel na een incident (bv HW fout), ofwel op vraag van de klant (bv bij logische fout);
- Snapshots
  - Er worden on-site snapshots genomen op de door de klant gespecifieerde storage volumes en schema. Als voorbeeld: elke 2u tijdens kantooruren, daarna elke dag voor 7 dagen en dan 1 per week voor 4 weken; Er kan een restore uitgevoerd worden vanuit de snapshots, in dit voorbeeld met een RPO van 2 uur; De aanvraag voor een restore uit een snapshot wordt opgestart binnen 4 uur tijdens kantooruren, cfr een request voor "data restore voor …x files".
  - De back-up heeft volgende kenmerken:
    - Backup is voor geval van een disaster op de primaire site of voor gevallen waar snapshots niet kunnen toegepast worden;
    - Backup volumes zitten offsite bv op Site B, wanneer de File Server en Storage gesitueerd wordt in de primaire site A, en vice versa;

- Er wordt een RPO voorzien van maximaal 24 uur.
- Backup schema en policy start van huidige backup schema. Vb: backup 1 x per 24u, voor 7 dagen en dan 1 per week voor 4 weken;

3.3.1.5 Vereisten beveiliging

- Zie ook overzichtstabel in RefBib "security bouwstenen"
- Hoge graad van beveiliging bieden middels next generation firewalls en geavanceerde technieken om cyberattacks van de nieuwe generatie te kunnen bestrijden (ATP based security, realtime malware analysis, anti-DDOS,…);
- Ondersteuning te bieden van alle vereisten van het VO veiligheidsbeleid, met inbegrip van de volledige netwerkbeveiliging, encryptie van Data at Rest (DAR) en encryptie van data in Motion (DIM) met encryptiesleutels in beheer van HFB;
- Applicaties op een beveiligde manier ontsluiten zowel intern (VO MPLS) als extern en met in achtname van extra authenticatie, beveiliging, manipulaties, etc.

3.3.1.6 DR Vereisten

Er dient voor het 'managed DC' de mogelijkheid tot Disaster Recovery voorzien te worden door de DC Leverancier. Deze componenten in het secundaire DC kunnen zowel 'actief-actief' of 'actief-passief' toegepast worden:

a.) In geval van een Actief-Active opstelling:

- wordt een active-active server opstelling toegepast op de primaire site A en de secundaire DR site B, én een storage replicatie over de beide sites, waarbij alle server-infrastructuur, operating system, OS beheer, middleware licentie, middleware beheer dubbel uitgevoerd worden, én waarbij het mogelijk is dat de applicatie active-active runt, en niet of nauwelijks onderbroken wordt door de disaster op één van de sites; De RTO waarde ligt dan laag tot zeer laag;
- De overschakeling van de applicatie kan transparant en automatisch uitgevoerd worden, zonder interventie van de applicatie dienstverlener; Bv door een DNS-gebaseerde overschakeling;
- Voor sommige middelwares kan de middleware geclustered worden. Dergelijke oplossingen zijn voorwerp van een apart project en dit wordt expliciet opgenomen in het exploitatiedossier;

b.) In geval van een Actief-Passief opstelling:

- zullen deze componenten in het secundaire datacenter 'gereserveerd' dienen te worden zodat ze – al dan niet geautomatiseerd – opgestart kunnen worden in geval van calamiteit in het primaire datacenter; De resulterende RTO waarde is

daardoor heel wat hoger dan in bovenvermelde active-active opstelling – bv enkele uren;

- Er wordt een active-passive opstelling toegepast op de primaire site A en de secundaire DR site B, waarbij alle server-infrastructuur, operating system, OS beheer, middleware licentie, middleware beheer enkelvoudig is;
- De applicatie runt steeds maar op 1 site; De DC/Cloud dienstverlener zorgt voor het starten van de passieve Vserver node, terwijl de applicatie dienstverlener zorgt voor de data restore en heropstart van de applicatie op site B;
- Op niveau van de server hypervisor kunnen de volledige server images van de servers op Site A beheerd worden, en opgestart worden op Site B;
- Er kan een storage replicatie over de beide sites toegepast worden in functie van een lagere RTO en RPO waarde.
- In het andere geval (zonder storage replicatie) wordt door de applicatie dienstverlener de restore uitgevoerd van de database-backup file vanaf de backup, op de storage op site B;

3.3.1.7 Security bouwstenen vereisten

- De leverancier voorziet volgende security bouwstenen in de context van Managed DC:
  - **Basic Firewalling**
  - **WAF** (bescherming tegen aanvallen op webapplicaties); de realisatie ervan valt binnen de FMO, dus na transitie;
    - Het betreft een ‘standaard’ WAF dienstverlening die een generieke web bescherming biedt gebaseerd op OWASP/Mittre)
    - een gecustomiseerde WAF setup dient als een betalend klantenproject ingericht te worden; een prijs per rule(set) add/change zal gehanteerd worden;
    - Verrekening gebeurt per App/VIP en throughput (bandbreedte); Deze bandbreedte wordt voorzien per App; Richtwaarden zijn:
      - 25Mbps – startwaarde, kleine applicatie, of test applicatie
      - 200Mbps – volwaardige applicatie
    - Het volume wordt op de WAF begrensd per App/VIP (toepassing);
  - **Endpoint protection/ endpoint detection & response**: levert naast de traditionele signature-gebaseerde malware detectie ook meer intelligente, signatureloze methodes zoals ATP, gedragsmonitoring op applicaties / processen / memory / netwerk, machine learning, reputatie analyse etc (multimethode beveiliding)
  - **Next-gen FW** (ngFW) voor de perimeter beveiliging, inclusief (minimale voorwaarden) IPS/IDS:IOC detectie, ATP, URL filtering, SSL decryption, Sandboxing, APP/User awareness, NAT, enz.…; de realisatie ervan valt binnen de FMO, dus na transitie;

- Het betreft hier een maandelijkse eenheidsprijs die per virtueel systeem wordt verrekend aan de klant, volgens throughput/bandbreedte,
  - € per 200M virtueel systeem
  - € per 500M virtueel systeem
  - € per 1000M virtueel system
- Er wordt per VIP een begrenzing voorzien op vlak van:
  - Bandbreedte:
  - aantal backend servers: 3
- Bij hogere aantallen backend servers worden bijkomende VIPS aangerekend.

- **aDDOS** levert bescherming tegen tegen DDoS aanvallen, zowel volumetrisch als applicatief. De bescherming maakt een ondersheid tussen het regulier (gebruikers en data) verkeer en herhaalde geautomatiseerde aanvragen (aanvallen) welke de (gecentraliseerde) ICT diensten kunnen overbelasten
- **Reverse Proxy of** Application Delivery Control in de vorm van loadbalancer, reverse proxy, applicatie web portaal. met uiteenlopende parameters en volgens verschillende methodes voor het afhandelen en doorsturen van sessies. Load Balancing zal gebruikt worden om de werklast te verdelen en productie en niet-productie applicaties en resources ter beschikking te stellen
  - Verrekening gebeurt per VIP;
  - Er wordt per VIP een begrenzing voorzien op vlak van
    - Bandbreedte: 200 Mbps
    - aantal backend servers: 3
  - Bij hogere aantallen backend servers worden bijkomende VIPS aangerekend;
- **Threat Intelligence (TI) en Threat hunting**.
  - TI lever teen breed scala aan informatie over bedreigingen incl. de mogelijkheid tot het groeperen en centraliseren van threats / IOCs afkomstig van diverse platformen en bronnen van en naar verschillende security platformen, incl bedreigingen die gecapteerd worden in sandbox-gebaseerde analyses, CERT-EU/CERT-BE, enz… Dit laat een gedetailleerde analyse toe van de globale en extern geleerde bedreigingen in de infrastructuur die de SP beheert;
  - Threat hunting levert een pro-actieve aanpak voor het opzoeken van sporen van malicious activity;
- Opm:
  - De Forward Proxy/SWG functie zal geleverd worden door HFB en de Perceel 4 dienstverlener; (FMO)
- **Platformdiensten voor encryptie van Data at Rest (DAR)** en encryptie van data in Motion (DIM) met encryptiesleutels in beheer van HFB; de realisatie ervan valt binnen de CMO, dus binnen transitie;

3.3.2 De managed DC dienstverlening

De Managed DC omvat alle Diensten m.b.t. het ter beschikking stellen en houden van verwerkingscapaciteit (op fysieke en virtuele servers), opslagcapaciteit (met of zonder back-up), netwerkcomponenten, in combinatie met de onderliggende computerzaalfaciliteiten en het provisioneren en beheren van enkele meer gestandaardiseerde platformen (databankplatformen, webservers en applicatieservers), maw het provisioneren en beheren van Infrastructuur en platformen. Deze gestandaardiseerde platformen worden ook ter beschikking gesteld van ontwikkelteams, zowel interne als externe (vb. via het raamcontract voor ontwikkelingen), die op basis van deze platformen toepassingen kunnen ontwikkelen en deze op een soepele manier in productie zetten en ter beschikking stellen van Gebruikers.

Er worden zowel productieomgevingen als omgevingen voor ontwikkeling en test aangeboden (non-productie-omgevingen).

Mee in scope van infrastructuur “as a service” en platform “as a service” zijn de bijhorend aangeboden hulpmiddelen (beheers- en ontwikkelingstools) en interfaces die de Klant (beheerder aan Klantzijde) in staat moeten stellen de server verwerkingscapaciteit en/of het platform te benaderen en zo effectief mogelijk te benutten. Deze omvatten de nodige beheerstools (geïntegreerde selfservice management tools) die via webinterface ter beschikking gesteld worden. Deze omvatten self-service provisioning, configuratie, een vorm van monitoring en administratie, en andere functies (bv. gedeeltelijke self- service monitoring, beheermogelijkheden voor sommige capacity en performance parameters van de middleware diensten van de PaaS, een mogelijk beperkte vorm van versiebeheer....).

Tevens krijgt de Klant samen met de infrastructuur as a service en/of het platform de nodige gebruiksinstructies en (vooringestelde) integratie-parameters (voorbeeld te gebruiken DNS naam, poort, protocol, enz.. voor zowel beheer als gewoon gebruik).

De Diensten worden zoveel mogelijk onder de vorm van van “Infrastructure as a Service” en “Platform as a Service” met het “pay-as-you-use”-model aangeboden. Het betreft “all-in” diensten waarbij alle voor de diensten noodzakelijke componenten zijn inbegrepen (investering en beheer van onderliggende infrastructuur, computerzaal, contracten, licenties, interfaces…).

Beschrijving van de dienstverlening

- De bestelling van de Managed DC IAAS Fservers, Vservers, Storage, .. gebeurt via een bestelportaal, waarbij de klant de dienst bestelt en configureert via een aantal stappen. Zo zal de klant voor Vservers de verschillende onderdelen apart configureren:
    - De dimensie van de Vserver hardware: vCPU en vRAM, via selectie vaneen T-shirt size;
    - De keuze van Storage volume en Tier
    - De keuze van OS licentie
    - De keuze van OS-beheerdienst
    - De keuze van een middleware licentie
    - De keuze van een middleware beheer
- De effectieve provisionering binnen het managed DC gebeurt zo veel mogelijk geautomatiseerd via automatiseringsbouwstenen. Er worden zowel productieomgevingen als non-productie-omgevingen geprovisioneerd;
- Het aanbod omvat zowel Vservers als Fservers. IAAS Vserver kunnen besteld worden via T-shirt sizes die een aantal VCPU's en volume aan VRAM, resp cores en RAM omvatten. Deze T-shirt sizes omvatten minimaal volgende types:

Type IAAS	Type Server	Label	Aantal Cores	RAM (GB)	OS Storage (GB)	vCPU	vRAM (GB)
IAAS Server	Fysiek	S	8	32	>100	nvt	nvt
IAAS Server	Fysiek	M	8	64	>100	nvt	nvt
IAAS Server	Fysiek	L	16	384	>100	nvt	nvt
IAAS Server	Fysiek	XL	32	512	>100	nvt	nvt
IAAS Server	Virtueel	XS	nvt	nvt	nvt	1	2
IAAS Server	Virtueel	S	nvt	nvt	nvt	2	4
IAAS Server	Virtueel	M	nvt	nvt	nvt	4	8
IAAS Server	Virtueel	M2	nvt	nvt	nvt	4	16
IAAS Server	Virtueel	L	nvt	nvt	nvt	8	16
IAAS Server	Virtueel	L2	nvt	nvt	nvt	8	32
IAAS Server	Virtueel	XL	nvt	nvt	nvt	16	32
IAAS Server	Virtueel	XL2	nvt	nvt	nvt	16	64
IAAS Server	Virtueel	XXL	nvt	nvt	nvt	32	128

- De bestelling van fysieke servers (Fservers) kan betrekking hebben op een minimale termijn die de leverancier vastlegt. Deze is maximum 36 maanden. De prijsopgave is op basis van een termijn van 36 maanden.
- Voor middleware licenties die steunen op cores, wordt op gevirtualiseerde servers een oversubscription ratio genomen: 1 CORE komt overeen met 4 VCPUs;

- Exploitatiediensten omvatten
    - bestelling;
    - facturatie; gekoppeld aan de VO financiële systemen;
    - inzicht en rapportering over gebruik van managed DC diensten door middel van dashboards zoals bijvoorbeeld het kunnen consulteren, bewaken/alarmeren van de (gecumuleerde) kosten, subscriptions, security compliancy etc. (zie verder).
    - een ondersteuning door een Technical Accountmanager (TAM), er wordt standaard geen lokale Nederlandstalige SDM-functie gevraagd. Op afspraak en in regie kan wel nog lokale Nederlandstalige SDM ondersteuning gevraagd worden
    - een controle op de wettelijke compliance (AVG) van het managed DC aanbod inclusief de het rapporteren over de compliancy rapportering (incl. audit rapporten) naar de klant;
    - Er is een exploitatiedossier voor het beheer van managed DC infrastructuur- en platformen;
    - technische adviezen (extra betalende diensten via werkaanvraag/project)

- Werkaanvragen/projecten en profielen die ingezet worden in regieprestaties
    - Bv ihkv de migratie en de target omgeving,
    - Bv projecten die specifieke tooling of expertise vereisen
- een portaal voor de door de Klant als beheerder aangeduide personen, voor al zijn diensten, zowel die voor cloud diensten, CloudOps, Cloud Traditioneel beheer, managed DC diensten, enz…
    - De voorkeur is dat de leverancier in Perceel 3 maximaal gebruik maakt van het overkoepelend bestelportaal & service cataloog bij de SI (perceel 1),
    - Het portaal dient voor
        - het uitvoeren van de bestelling van de managed DC diensten; De bestelling van de IAAS/PAAS diensten gebeurt zo veel mogelijk via het overkoepelende bestelportaal van de SI, en daar wordt ook de status van de bestelling getoond naar de klant. Waar dit niet mogelijk is, gebeurt de bestelling via het bestelportaal dat de dienstenleverancier hiervoor zelf voorziet.
        - het melden van incidenten, vragen over het aanbod, het vragen van ondersteuning,
        - het bekijken van dashboards m.b.t. de afgenomen managed DC diensten zoals bijvoorbeeld het kunnen consulteren, bewaken/alarmeren van de (gecumuleerde) kosten, subscriptions, security compliancy etc. (zie verder).
        - Merk op dat er geen standaard Service Desk is voor de Gebruikers;

3.3.2.1 SMB File Server diensten

De DC/Cloud leverancier biedt een IAAS Storage - SMB File Server dienst aan.

- Deze dienst omvat alle hard- en software, en alle tools en platformen die nodig zijn om de dienst te leveren:
    - De licentie is op basis van de Windows Server licentie;
    - De storage is gebaseerd op Storage Tier 2 non-replicated;
    - Er wordt voorzien in een anti-virus, anti-malware bescherming op de bestanden op de File Server;
    - De File Server zelf is redundant uitgevoerd op 1 site; Er wordt een active-passive opstelling toegepast;
    - Er worden on-site snapshots genomen op de storage, elke 2u tijdens kantooruren, daarna elke dag voor 7 dagen en dan 1 per week voor 4 weken; Er kan een restore uitgevoerd worden vanuit de snapshots, met een RPO van 2 uur; De aanvraag voor een restore uit een snapshot wordt opgestart binnen 4 uur tijdens kantooruren, cfr een request voor “data restore voor …x files”.
    - De back-up heeft volgende kenmerken:
        - Backup is voor geval van een disaster op de primaire site of waar de snapshots ontoereikend zijn;
        - Backup volumes zitten offsite bv op Site B, wanneer de File Server en Storage gesitueerd wordt in de primaire site A, en vice versa;
        - Er wordt een RPO voorzien van maximaal 24 uur.
        - Backup schema en policy start van bestaande schema; Vb: 1 x per 24u, voor 7 dagen en dan 1 per week voor 4 weken;
    - Er wordt uitgegaan van dataclassificatie klasse 4, en alle beveiligingsmaatregelen van klasse 4 worden toegepast, incl encryptie voor data at rest, op basis van het encryptieplatform dat de DC/Cloud leverancier voorziet, waarbij het key beheer gebeurt door de VO.
    - Archivering of hierarchisch storage management wordt niet toegepast
    - Disaster Recovery is voozien via een Active-Passive server opstelling, en een restore van de backup data op de DR site. RTO is 48u; RPO is 24u;
    - De File Server is multi-tenant, en bedient dus meerdere VO-entiteiten die afgescheiden zijn van elkaar, maar wel dezelfde File Server en Storage infrastructuur delen;
    - De dienstverlener alloceert een storage volume op de File Server, met de omvang die de klant definieert; De klant betaalt voor het volledige gealloceerde volume;
    - De netwerk latency round-trip is maximaal 4 ms, gemeten vanaf de VO POP, zie ook bovenstaande paragraaf 3.3.1.2 Vereisten datacenter; Een latency van 2 ms is beter.
    - De File Server werkt in combinatie met de “shared Active Directory” van de VO. Op die directory zijn de gebruikersidentiteiten gedefinieerd, en de groepen van gebruikers van de VO-entiteit. Het beheer van active directory en het gebruikersbeheer op niveau van de VO-entiteit in die directory zijn buiten scope.

  - Het onderliggende datacenter en de computerzaal en de netwerkconnectiviteit van 2x10 Gbps naar de VO POPs; Ook de netwerkverbinding naar de shared Active Directory Domein Controllers;

- Deze dienst omvat alle beheerstaken op de onderliggende server, storage en backup platformen, encryptie, enz…. die nodig zijn om de dienst te leveren; Dit houdt ook in de toepassing van urgente security patches, en het tijdig detecteren en actie nemen bij aanvallen van ransomware;
- De dienst omvat de inrichting van de file server en storage na de aankoop van de hierboven vermelde componenten. Het configureren van de file share omgeving dient te verlopen via een project werkaanvraag. De klant kan op die manier de inrichting van zijn volumes, inrichting van de fileshare, opzetten van een folderstructuur aanvragen, alsook het inrichten van de nodige toegangen voor de beheerders (maximum 5) als de toegangen voor de eindgebruikers. De klant kan ook opteren om in deze werkaanvraag het logon script aan te laten passen. Dit laatste gebeurt via Perceel 2 Werkplekdiensten;
- Deze dienst omvat alle beheerstaken die betrekking hebben op de inrichting van de File Server, de volumes, het rechtenbeheer, snapshot- en backupbeheer, en de afhandeling van standaard vragen die de klanten stellen met uitzondering van de betalende requests:

data restore van maximum 50 aparte files of 5 directories (restorecapaciteit files beperkt tot 200GB/uur) per aanvraag met behoud van de oorspronkelijke locatie
data restore van een onbeperkt aantal files of directories met behoud van de oorspronkelijke locatie of voor een data restore uit de laatste backup naar een andere locatie dan de oorspronkelijke

- Deze dienst omvat niet de beheerstaken die de klant zelf uitvoert, met name:
  - De inrichting van de folders en directory structuur, het rechtenbeheer, … binnen een volume; Het toevoegen van gebruikers aan groepen, en het toekennen van rechten aan groepen van gebruikers. Er is hiervan een beschrijving in de refbib: “Beheer Op Active Directory Groepen BOAG t.b.v. Aanbod Fileshare (VA25)”;
  - Evenwel moet de oplossing voor beheer het risico mitigeren, waarbij gebruikers die instaan voor rechtenbeheer op de file server, die rechten beheren middels hun gewone gebruikersaccount; dat maakt het risico/ de impact van ransomware te groot;

3.3.2.2 Middleware ondersteuning en PAAS diensten

Tijdens de uitvoering van de overeenkomst zal er steeds een breed aanbod van middleware ondersteuning en PaaS diensten beschikbaar zijn dat de marktevolutie volgt.

De volgende tabel geeft aan welke middleware platformen bij de start van de overeenkomst ondersteund worden. We maken daarbij een onderscheid tussen

- Ondersteuning in de vorm van operationeel beheer, zowel in het Managed DC, als bij “CLoudOps”, of “Traditioneel beheer” in een publieke cloud;
- De leverancier voorziet ook de onderliggende licenties van sommige middleware producten, als onderdeel van de Managed DC PAAS dienst. (merk op: NIET in public cloud: daar koopt de klant

de “bring your own license”); Wanneer de klant op zijn initiatief zelf de licenties aankoopt, of gebruik maakt van bestaande licenties, dan vervalt deze verplichting;

- De leverancier voorziet operationeel beheer, enkel bij DC outsourcing, en niet als onderdeel van Managed DC, noch bij traditioneel beheer in public cloud;
- De taken en processen inzake licentiebeheer zijn inbegrepen. Die zijn beschreven in het VOPO document;

Zowel LINUX servers als Wintel servers dienen deel uit te maken van deze Diensten. Ook het beheer van virtualisatielaag (bv VMWARE, …) dient inbegrepen te zijn in deze Dienst.

M.b.t. het dienstverleningsniveau moeten verschillende varianten en opties aangeboden worden (24/7 en Uitgebreide kantooruren). De Klant kan dit per middleware instance bepalen.

Er zullen Eenheidsprijzen toegepast worden; deze prijzen gelden per middleware instance per maand;

Beheer van middleware ACTIVEMQ Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware Apache HTTP SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware TOMCAT Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware POSTGRES PLUS ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware .NET FRAMEWORK Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware INTERNET INFORMATION SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware SQL SERVER ENTERPRISE Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware SQL SERVER STANDARD Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware NGINX Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware INTERNET APPLICATION SERVER ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware JDK Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware MYSQL Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware ORACLE APPLICATION EXPRESS (APEX) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware ORACLE CONTAINER FOR JAVA EE (OC4J) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware ORACLE DATABASE ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware ORACLE DATABASE STANDARD EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware WEBLOGIC SERVER ENTERPRISE Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware WEBLOGIC SERVER STANDARD Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware POSTGRESQL Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware JBOSS APPLICATION SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware JBOSS ENTERPRISE APPLICATION PLATFORM (EAP) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS
Beheer van middleware Kubernetes en de onderliggende server cluster - Cloud Deel 2.B.	CloudOps

3.3.2.3 Facturatie en financiële rapporten

De P3 DC/Cloud dienstenleverancier levert gedetailleerde maandelijkse billing rapporten, waarvan het detail, zoveel mogelijk gelijke tred houdt met de rapportering van public cloud;

- De toegang tot de billing rapporten gebeurt op een streng beveiligde manier; de billing rapporten kunnen geleverd worden aan de VO-entiteit zelf, zonder dat er inzage mogelijk is door andere VO-entiteiten, laat staan klanten-organisaties buiten de VO. De P3 DC/Cloud dienstenleverancier en HFB hebben steeds inzage. De VO-entiteit kan het inzagerecht doorgeven aan derde partijen.
- De broker levert zelf een webportaal die de billing informatie op een gedetailleerde, maar ook overzichtelijke en grafische vorm voorstelt, op een manier die de VO-klant in staat stelt om zijn verbruik op te volgen.

3.3.2.4 Accounts en Rechten

- De DC/Cloud dienstenleverancier behoudt de root rechten, maar zal de handelingen die root rechten vereisen en die een klant – of zijn aangestelde dienstverlener – vraagt, uitvoeren in het kader van support die hij levert in dienst van de klant. Analoog levert de Broker ook de nodige systeeminformatie zoals bv logs die ter beschikking gesteld worden, of geforward worden

3.3.2.5 Ondersteuning

- De DC/Cloud ICT-Dienstverlener dient ervoor te zorgen dat de supportvragen van Klanten en Applicatie Dienstleveranciers zo efficiënt mogelijk worden gecapteerd en behandeld en dient in zijn offerte duidelijk toe te lichten hoe dit concreet kan worden gerealiseerd.
- De ondersteuning door een Technical Accountmanager (TAM) is in de dienst inbegrepen, maar is ook beperkt inzake de geleverde ondersteuning. Voor uitgebreide ondersteuningsvragen is een studieproject via werkaanvragen/project, of via regieprestaties steeds mogelijk;
- Hetzelfde geldt voor ondersteuning inzake cost controle; Adviezen inzake cost optimalisatie of vergelijkende studies zijn via werkaanvragen/project, of via regieprestaties mogelijk; Dit geldt ook voor projecten inzake migraties;

3.3.2.6 Operationele dienstverlening

- De DC/Cloud ICT-Dienstverlener neemt snapshots en backups, en voert updates en upgrades van het OS of andere (applicatie) software uit, cfr de dienstenbeschrijving.

3.3.3 Het bestaande Managed DC – VPC Mechelen

3.3.3.1 Operationele dienstverlening

- De bestaande managed DC dienstverlening inzake IAAS/PAAS wordt niet verdergezet; De transitie voorziet een migratie van deze infrastructuur naar het nieuwe managed DC aanbod (in bereik van transitie)
- De bestaande managed DC dienstverlening inzake Applicatiebeheer wordt verdergezet - maar omvat enkel het beheer van de infrastructuur- en platformlaag onderliggend aan de applicatie, en niet het beheer van de applicatie zelf. zie supporting contract in de Refbib: VPC continuiteit - dienstbeschrijving Applicatie Management (1); Deze dienstverlening wordt verdergezet, maar is ook begrensd in de tijd tot eind 2024.;
- De DC/Cloud ICT-Dienstverlener zorgt voor de integratie van de dienstverlening met de SIAM zoals op vlak van event, configuration, incident, problem, change, … management; beveiligingsbeheer; logging; SIEM; Rapportering; enz…
- Uitzondering hierop vormt het bestelproces en bestelportaal; Uit de continuïteitsdoelling volgt dat de klant normaliter geen of zeer beperkte uitbreidingen realiseert. Indien de klant een uitbreiding wenst, dan gebeurt dit op basis van werkaanvraag en projectvoorstel, en niet via het bestelportaal; In dat projectvoorstel worden de nieuwe exploitatiekosten aangeboden;
- Afwijkend is de facturatie:
    - De kosten van het supporting contract m.b.t. VPC Mechelen, worden door de DC/Cloud dienstenleverancier verdeeld en gefactureerd aan de klanten, volgens de gerapporteerde bedragen. Deze rapporten worden maandelijks door de subcontractor opgesteld, en vermelden het bedrag dat overeenkomt met de exploitatiekosten per applicatie en per klant;

3.4 Interfaces met andere dienstenpakketten

3.4.1 Applicaties

De scheidingslijn tussen de dienstverlening van Perceel 3 “Cloud en datacenter diensten” en de verantwoordelijke voor de applicatielaag (Perceel 5 “applicatie beheer” of klantenteam), volgt in grote lijnen de logica van het **shared responsibility model** van een public cloud provider:

De P5 AM dienstenleverancier, of het klantenteam indien de VO-entiteit dit niet uitbesteedt

- De P5 AM dienstenleverancier beheert de applicatiecomponenten, en vraagt aan P3 de nodige onderliggende standaard infrastructuur en platformdiensten te voorzien en te configureren volgens zijn specificatie;
- De P3 DC/Cloud dienstenleverancier levert en configureert de onderliggende gestandaardiseerde infrastructuur- en platformdiensten, op vraag van, en volgens de specificaties van de VO-entiteit die klant is, of desgevallend de door hem aangestelde P5 AM dienstenleverancier; De P3 DC/Cloud dienstenleverancier zal de Managed DC portaal gebruiken voor configuratie, en niet de P5 AM dienstenleverancier; Deze laatste kan wel gebruik maken van de automatiseringsbouwstenen die de P3 DC/Cloud dienstenleverancier in zijn bestelportaal opneemt;
- De P3 DC/Cloud dienstenleverancier zal instaan voor het OS-beheer, de monitoring en het up-to-date houden van het OS; De P3 DC/Cloud dienstenleverancier zal instaan voor monitoring tools op vlak van infrastructuur, en de middlewares die deel uit maken van de onderliggende gestandaardiseerde infrastructuur- en platformdiensten,
- De P3 DC/Cloud dienstenleverancier zal instaan voor de installatie van monitoring tools op de applicatielaag; De klant en/of P5 AM dienstenleverancier zorgt voor de nodige licenties en toolselectie, en houdt hierbij rekening met de randvoorwaarden die de P3 DC/Cloud dienstenleverancier op dit vlak hanteert;
- De P3 DC/Cloud dienstenleverancier is verantwoordelijk voor de correcte uitvoering van de gevraagde diensten volgens specificatie, inclusief de **operationele beschikbaarheid** en de beveiliging van de infrastructuur of de platformdiensten zelf;
- Ingeval gekozen wordt voor een niet-standaard middleware platform, dat runt bovenop de IAAS diensten, dan komt dit platform in beheer bij de P5 AM dienstenleverancier .
- Deze regel geldt voor alle ‘niet standaard’ middlewares/platformsoftware die de P5 AM dienstenleverancier toepast, en waarvan de diensten niet geleverd worden door de P3 DC/Cloud dienstenleverancier. (we noemen deze: ‘niet standaard’);
- Voor de middlewares die niet in het standaard PAAS aanbod van de P3 DC/Cloud dienstenleverancier voorzien worden, kan de klant bij de P3 DC/Cloud dienstenleverancier de licenties aankopen en de installatie laten uitvoeren. De installatie ervan gebeurt op basis van een werkaanvraag;
- De P5 AM dienstenleverancier is eindverantwoordelijk voor het geheel van de architectuur en de integratie, de configuratie van alle applicatie- platform en infrastructuur componenten binnen de applicatie, alsook voor het eindresultaat. Dat geldt ook voor de resulterende beveiliging van het geheel van de applicatie, conform het model van “the security *in* the cloud”); De P5 AM dienstenleverancier staat in voor de risico analyse, voor de beveiligingsarchitectuur van de toepassing, voor de correcte toepassing van de beveiligingsmaatregelen, de toepassing van aanvullende beveiligingsbouwstenen, enz…

  - maar hij zal voor de onderliggende infrastructuur- en platformlaag wel beroep doen op de P3 DC/Cloud dienstenleverancier die kan instaan voor de (beveiligings)architectuur van de onderliggende infrastructuur- en platformlaag, voor de correcte configuratie van de managed DC diensten, voor de correcte toepassing van de beveiligingsmaatregelen, de toepassing van aanvullende beveiligingsbouwstenen in de onderliggende infrastructuur- en platformlaag;
  - En voor de uitvoering van operationele taken die betrekking hebben op die laag;
- De P5 AM dienstenleverancier staat ook in voor de planning en uitvoering van applicatie migraties; Hij kan daarbij beroep doen op de diensten van de P3 DC/Cloud dienstenleverancier;
- Backup/restore werkzaamheden volgens tabel onder hoofstuk **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**;

De P3 DC/Cloud dienstenleverancier

- Provisioneert – op basis van de configuratie in het bestelportaal - op een – zoveel mogelijk geautomatiseerde manier - de standaard infrastructuur en platformdiensten in het managed DC.
- De P3 DC/Cloud dienstenleverancier levert en configureert de onderliggende gestandaardiseerde infrastructuur- en platformdiensten van het managed DC, op vraag van, en volgens de specificaties van de klant of zijn aangestelde applicatie dienstverlener;
- De P3 DC/Cloud dienstenleverancier is verantwoordelijk voor de correcte uitvoering van de gevraagde diensten volgens specificatie,;
- De P3 DC/Cloud dienstenleverancier is verantwoordelijk voor het leveren van exploitatiediensten: bestelling; facturatie; technische ondersteuning; en vooral zal de P3 DC/Cloud dienstenleverancier instaan voor het operationeel beheer van deze onderliggende infrastructuur- en platformlaag: incident- problem, change management; opvolging van security events en notificaties; opvolging van cost control; rapportering over beveiliging & compliance, en de **operationele beschikbaarheid** en de beveiliging van de infrastructuur of de platformdiensten zelf …;
- De P3 DC/Cloud dienstenleverancier neemt de verantwoordelijkheid voor de correcte uitvoering en de algehele integratie, operationele beschikbaarheid en beveiliging van de hele infrastructuur- en platformlaag die onderliggend is aan een applicatie;
- de P3 DC/Cloud dienstenleverancier zal ook instaan voor de beveiliging van de managed DC diensten zelf, conform het model van “the security *of* the cloud”); Hij staat in voor de beveiligingsarchitectuur van de onderliggende infrastructuur- en platformlaag, voor de correcte configuratie van de IAAS/PAAS diensten, voor de correcte toepassing van de beveiligingsmaatregelen, en de toepassing van aanvullende beveiligingsbouwstenen in de onderliggende infrastructuur- en platformlaag;
- de P3 DC/Cloud dienstenleverancier kan ook instaan voor de opzet van tools en processen voor de samenwerking met de Service Integrator inzake het monitoren in de onderliggende infrastructuur- en platformlaag, het doorsturen van events naar de SIAM functie, het doorsturen van logs naar de SIEM functie, enz…

- De P3 DC/Cloud dienstenleverancier levert de diensten die nodig zijn voor de migratie en de target omgeving, onder meer expertise d.m.v. de aangeboden profielen die ingezet worden in regieprestaties of projecten; het uitvoeren van projecten; Het leveren van specifieke tooling of expertise;

	KLANT	DC leverancier
IAAS/PAAS diensten en Marketplace, van Hyperscale public cloud	bestellen en configureren via de webportaal van de DC leverancier voor de initiële bestelling	Leveren van Managed DC diensten. Leveren van de exploitatiediensten;
Applicatie componenten, pakketsofware	Installatie, configuratie en beheer	
Basis IAAS en PAAS diensten op Managed DC dienst	Specificaties van de onderliggende infrastructuur/platformen bepalen en bestellen;	Provisionering van de hele infrastructuur- en platformlaag die onderliggend is aan een applicatie
Middelwares bovenop de IAAS diensten van de managed DC dienst		De configuratie van managed DC PAAS, en ook aanvullende middlewares buiten het cloud aanbod;
OS beheer, patching van OS, admin rechten;		OS beheer, uitvoeren van patching of IPS van patched OS image, admin rechten;
Beveiliging	Overkoepelende verantwoordeljikheid (risico analyse, architectuur, uitvoering, exploitatie); Security in the cloud	Security of the cloud; Verantwoordeljikheid (risico analyse, architectuur, uitvoering, exploitatie) van de onderliggende infrastructuur- en platformlaag;
Onderliggende infrastructuur- en platformlaag		Architecturaal ontwerp, configuratie, operationeel beheer, beveiliging
Backup	Backupfile maken van database. (ifv recovery op logische fouten);	Traditioneel: Backup van server image (incl middleware en platform software); Backup en restore diensten van storage volumes en ,objecten, backupfiles en journal files van databases, …
Migratie (van de applicatie), ingeval een wijziging van de DC (bv stopzetting VPC,) .	Offerte, planning, uitvoering van applicatie migraties	Op vraag van klant: Leveren van de DC diensten die nodig zijn voor de migratie en de target omgeving

3.4.2 Netwerken

De P3 DC/Cloud dienstenleverancier, voor het managed DC, staat in voor:

- Ontwerp van de (beveiligings)architectuur van het DC netwerk, en de netwerkbeveiliging in het DC; De uitvoering van het DC netwerk, en de netwerkbeveiliging;
- Het realiseren van de netwerkverbinding met de VO netwerken; Mbt het managed DC zal de DC/Cloud ICT-Dienstverlener verantwoordelijk zijn voor de connectiviteit 2 x 10 Gbit/s (redundant) naar de glasvezel backbone van de Vlaamse overheid (op twee verschillende VO POP's) en laat het gebruik en integratie met VO-netwerk oplossingen toe, zoals het gebruik van VO private IP address space, routeringsoplossingen met VO interne netwerken, integratie met de DNS service van de VO, etc.
    - De integratie met het VO netwerk dient aangevraagd en afgesproken te worden bij de Netwerk leverancier van Perceel 4, en is voor Perceel 3 buiten scope;
- Versturen van service requests inzake routering, tunnel VPN info, Forward Proxy naar de P4 netwerkdienstenleverancier die deze zal uitvoeren;
- Versturen van service requests inzake VO private IP address space blokken (RFC1918) aan HFB, door het definiëren, documenteren en onderbouwen van de vereisten;
- Aanvragen van DNS wijzigingen (via webportaal van HFB)
- Het voorzien van de security bouwstenen in de context van Managed DC – zie voor een overzicht: 3.3.1 Het managed DC

De P3 DC/Cloud dienstenleverancier, staat in via de subcontractor DXC voor het bestaande VPC-Mechelen

Voor de "internet zones" wordt gebruik gemaakt van netwerk- en netwerkbeveiligingsdiensten van subcontractor DXC:

- Internet verbinding
- ADC (Load Balancer, Reverse Proxy)
- Internet connectie, aDDOS
- Connectiviteit met VO netwerk
- Er wordt gebruik gemaakt van de VO-DNS;

Voor de VPC overgangszone wordt gebruik gemaakt van de internet verbinding en netwerkbeveiligingsdiensten van HFB, uitgebaat door de P4 netwerk dienstverlener; Deze worden door P4 beheerd en gefactureerd aan HFB.

- netwerkbeveiliging (DC FW);
- Next-gen FW voor de perimeter beveiliging, incl IPS/IDS:IOC detectie, ATP, URL filtering, SSL decryption, Sandboxing, APP/User awareness, NAT, enz… op internet- en partner links;
- Forward Proxy naar Internet, met geavanceerde security mogelijkheden incl IPS/IDS, ATP, URL filtering, SSL decryption, Sandboxing, … voor het ontsluiten van platformen en toepassingen naar het internet;

Het nieuwe Managed DC aanbod van de DC/Cloud dienstenleverancier, kan niet langer gebruik maken van de netwerkbeveiligingsdiensten, internet-verbindingen, enz… van HFB.

De P4 netwerkdienstenleverancier staat in voor:

- De integratie van de managed DC connectiviteit binnen het VO netwerk, zoals het gebruik van VO private IP address space, routeringsoplossingen met VO interne netwerken, integratie met de DNS service van de VO, etc. De integratie met het VO netwerk wordt door Perceel 3 aangevraagd, en is buiten scope van P3, en binnen scope van P4.
- Het uitvoeren van requests en operationeel beheren van de beschikbare netwerkbouwstenen, zoals onder meer de routering naar het VO netwerk en VOnet;.
- Het uitvoeren van requests inzake de aanvullende beveiligingsbouwstenen die HFB bijkomend voorziet in de cloud;
- Het uitvoeren van requests inzake bijkomende site-to-site VPN verbindingen met het VO netwerk;
- Het voorzien van volgende security bouwstenen:
    - Cloud gebaseerde Forward Proxy met geavanceerde security mogelijkheden incl IPS/IDS, ATP, URL filtering, SSL decryption, Sandboxing, … voor het ontsluiten van platformen en toepassingen naar het internet; (FMO)
- Het operationeel beheer van de HFB netwerksecurity bouwstenen voor de “overgangszone” binnen het bestaande VPC-Mechelen;

HFB staat in voor:

- Voor alle netwerkdiensten en bouwstenen die vermeld zijn bij “P4 netwerkdienstenleverancier”, en ook de HFB netwerk security diensten – voor VPC overgangszone (in afbouw)
        - netwerkbeveiliging (DC FW)
        - Next-gen FW voor de perimeter beveiliging, incl IPS/IDS:IOC detectie, ATP, URL filtering, SSL decryption, Sandboxing, APP/User awareness, NAT, enz… op internet- en partner links
        - Forward Proxy naar Internet, met geavanceerde security mogelijkheden incl IPS/IDS, ATP, URL filtering, SSL decryption, Sandboxing, … voor het ontsluiten van platformen en toepassingen naar het internet
    - HFB staat in voor de processen van Strategy to Porfolio, Requirement to Deploy, product management, product/service design, de design autoriteit van de onderliggende infrastructuur, dienstenleverancier en klantzijde t.a.v. de P4 dienstenleverancier;
    - de P4 dienstenleverancier staat in voor de operationele invulling in de processen van Request to Fullfill, Detect to Correct;

- HFB levert ook eigen diensten:
    - De WS-Security Gateway bouwsteen (op basis van IBM DataPower), voor verwerking van SOAP/XML service requestes met een WS-Security gebaseerde beveiliging
    - De APIGEE API Gateway bouwsteen op basis van Google/Apigee on-prem en SAAS;

- De PKI/DCB bouwsteen voor machine/device/applicatie certificaten
- De ACM “VO-toegangsbeheer” bouwsteen voor gebruikers identificatie en SSO (SAML/O-AUTH/OIDC) en voor server/applicatie identificatie (O-AUTH)
- De Key Management bouwsteen voor private key beheer, in combinatie met cloud KMS oplossingen zoals bv AWS KMS en Azure KMS;
- De PAMaas bouwsteen voor privileged access management;

3.4.3 Service desk en SIEM

Analoog aan **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**

3.4.4 Werkplekken

Analoog aan **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**

3.4.5 Mainframe

Mainframediensten maken deel uit van een ander dienstenpakket, maar mogelijk kan er datacenter dienstverlening nodig zijn in het kader van integratie met mainframetoepassingen.

3.5 Omschrijving verdere concretisering van de ondersteunende processen

De algemene procesvereisten zijn opgenomen in het contractuele document “Vereisten ondersteunende processen en overlegfora”. Hieronder zijn meer gedetailleerde vereisten opgenomen specifiek voor managed datacenter diensten in het Dienstenpakket “Cloud- en Datacenterdiensten”.

Voor de Exploitatie van de servers en platformen zal de DC/Cloud ICT-Dienstverlenerde verschillende operationele betrokkenen aansturen om een kwalitatieve uitvoering te realiseren. Tevens zorgt hij ervoor dat alle achterliggende processen voor realisatie van deze Dienst voldoende zijn ingericht. De concrete beschrijving van het bereik van de dienst wordt per klant beschreven in een exploitatiedossier.

De achterliggende processen voor realisatie van deze Dienst betreffen o.a.:

3.5.1 Incident Management:

- De DC/Cloud ICT-Dienstverlener geeft de gepaste prioriteit aan de Incidenten, gemeld via de Service desk of automatisch gegenereerd via alarmen uit de monitoring tools, om de als SLA opgenomen beschikbaarheid te realiseren. Dit omvat eveneens het voorzien van een wachtdienst voor het garanderen van de overeengekomen dienstverleningsniveaus met betrekking tot deze Dienst.

3.5.2 Problem Management:

- Oplossen van Problemen.
- D.m.v. monitoring “proactief probleembeheer”.
- Bij storingen een root cause analyse uitvoeren.

3.5.3 Subcontractmanagement:

- Subcontractmanagement: Afsluiten (en tijdig verlengen/actualiseren) van de nodige (onderhouds)contracten om de exploitatiediensten te realiseren.

3.5.4 Event Management:

Monitoring van de diensten.

- Specifiek betreft het de monitoring van de in Exploitatie zijnde platformen en servers. Zowel performantie als beschikbaarheid worden opgevolgd.
- Verder wordt het gebruik van de platformen en servers opgevolgd zodat zowel abnormaal hoog gebruik of inbreuken op de veiligheid snel gedetecteerd worden.
- Vanuit een centraal monotoring systeem worden alarmberichten uitgestuurd die automatisch Incidenten en Problemen melden als bepaalde alarmdrempels worden overschreden.

3.5.5 Capacity management:

- De belangrijke parameters van i.v.m. de platformen en servers worden opgevolgd, gemonitord en de Klant wordt ingelicht indien er afgesproken capaciteitsdrempels worden overschreden.

3.5.6 Availability management:

- Het operationeel beheer van de platformen en servers om deze Diensten conform de gevraagde beschikbaarheidsniveaus te garanderen;
- Het beschikbaar houden van alle onderliggende infrastructuur en alle processen die noodzakelijk zijn om de functionaliteit met betrekking tot de platform- en serverdiensten te kunnen aanbieden;
- De DC/Cloud ICT-Dienstverlener zorgt voor de nodige redundancy- en failover mogelijkheden om de gevraagde beschikbaarheid te garanderen;
- Het opnemen in de operationele omgeving van bijkomende standaard platformen en servers via het proces “Beheer van de Service Portfolio en de Service catalogus ” en nadat deze werden overgedragen vanuit projectwerking naar Exploitatie.
- Het nemen van de nodige back-up van de bestanden op de platformen en servers om te garanderen dat het verlies van data maximaal ingedekt is (inclusief het veilig bewaren van de back-ups). Van de data in de beheerde databanken en van de bestanden in de beheerde servers wordt minstens dagelijks een back-up genomen die bewaard wordt in een ander datacenter. De back-ups worden 30 dagen bewaard.

- De backup modaliteiten zijn als volgt te omschrijven: de standaard retentie periode voor de backup is 30 dagen, deze wordt zowel onsite als offsite gedurende deze periode bijgehouden. De klant is zelf verantwoordelijk om te bepalen wat gebackupped dient te worden en wat niet, rekening houdend met het feit dat in deze backup data ook het besturingssysteem gebackupped wordt. Op die manier kan bij een restore van een volledige server de laatst werkende configuratie terug gezet worden. Standaard voorzien we een dagelijkse backup van de volledige server. De Klant moet zelf zorgen voor de back-up van eventuele databanken naar een bestand zodat dit vervolgens met de standaard systeem back-up kan meegenomen worden. De Klant kan aanpassingen vragen aan de beschreven standaard opzet : hij kan vragen om bepaalde gegevens niet te backuppen door middel van een project of in samenspraak met de SDM via regie prestaties.
- De DC/Cloud ICT-Dienstverlener voert de nodige Updates en Upgrades uit van de software die wordt gebruikt met betrekking tot de platform- en serverdiensten.
- Het starten, stoppen en herstarten van servers;
- Installatie van service packs en hotfixes;
- Implementeren van antivirusmaatregelen;
- Tunen van de syteemcomponenten;
- Alle storage moet redundant uitgevoerd zijn. Data deduplicatie moet steeds deel uitmaken van de oplossing voor storage.

3.5.7 Configuratiebeheer:

- Up-to-date houden van de Configuratiedatabank m.b.t. de inventariselementen voor alle platform- en serverdiensten en zorgen dat de gegevens ontsloten worden naar het DDC-DWH zodat ze beschikbaar zijn voor de rapportering;
- Onderhouden en actualiseren van de documentaire configuratiegegevens m.b.t. de platform- en serverdiensten.

3.5.8 Beveiligingsbeheer:

Voor het operationele beheer van het managed DC zijn volgende processen en tools noodzakelijk:

- Security event notificaties worden gerapporteerd:
    - De Applicatieleverancier (Perceel 5), of klantenteam, en de Service Integrator, beschikken elke dag over actuele en accurate rapporten inzake security events.
    - Alle relevante informatie, zoals OS release, patching level, endpoint protection, .. gedetecteerde security events en logs (bijv. alerts van een bepaald niveau) dienen te worden gecommuniceerd naar de globale SIEM van de VO (SIAM) voor interpretatie binnen de SIEM en de overkoepelende security monitoring;
    - Raw data dient steeds adhoc toegankelijk te zijn voor het VO SOC team om redenen van investigation/ tracking /evidence /forensics.
    - Klantenteams, applicatieleveranciers, … hebben enkel inzage in de event notificaties van hun eigen entiteit/applicatie en niet die van andere entiteiten/applicaties;
- Network flow monitoring
- Threat intelligence/ Threat hunting tools in functie van de processen voor beveiligingsbeheer;

De DC/Cloud dienstenleverancier:

- regelt de netwerk (seggregatie) in conform de VO policies;
- beheert de identiteiten en autorisaties van klantenteams, applicatieleveranciers,… op de verschillende rapporten en tools die hij ter beschikking stelt; Bij voorkeur kan hij daarvoor beroep doen op de WebIDM en VO-toegangsbeheer bouwstenen van HFB;
- beheert toegangsrechten op niveau van de serverdiensten en bewaakt de correcte werking van het toegangsbeheer om ongeoorloofde toegang van personen of systemen tot de gegevens in het beheerde platformen en servers te vermijden. Hierbij gelden hogere eisen voor de toegang met uitgebreidere rechten (o.a. voor beheer-doeleinden) en voor toegang tot Persoonsgegevens. De toepasselijke organisatorische en technische maatregelen worden opgenomen in het exploitatiedossier van de platformen en servers;
    - Zie ook de toepassing van PAMaas in 2.4.6.8 Packaging en Delivery;
- voorziet bescherming tegen malware op de beheerde platformen en servers;
- installeert beveiligingspatches.
- stelt op elk ogenblik een goede beschrijving beschikbaarn van de infrastructuur die de DC/Cloud ICT-Dienstverlener inzet voor de server-en platformdiensten. Hierbij wordt ook aangegeven in welk datacenter van de DC/Cloud ICT-Dienstverlener deze infrastructuur staat en hoe dit datacenter geconnecteerd wordt met de VO-WAN en het internet (netwerk- en beveiligings-componenten). Met betrekking tot de infrastructuur die onderliggend gebruikt wordt voor het bewaren en verwerken van persoonsgegevens is een verhoogd veiligheidsniveau van toepassing. Deze infrastructuur maakt mee het voorwerp uit van de controles m.b.t. de wet op de privacy. Een vereiste bovendien is dat deze infrastructuur uitsluitend binnen de Europese Unie mag geplaatst worden;
- voorziet bescherming tegen malware op de beheerde servers;
- voorziet het managed DC voor de publieke ontsluiting van de toepassingen van een eigen redundante Internet verbinding en perimeter beveiligingsdiensten zoals Internet border protection next-gen Firewall, aDDOS / IPS, generieke Web Application Firewall en dienen voor allle instanties het principe van netwerksegregatie te respecteren: het opsplitsen in verschillende lagen en zones die logisch bij elkaar horen, eenzelfde risiconiveau hebben (cfr VO dataclassificatie) of dezelfde security maatregelen vereisen.

3.5.9 Log management

- Analoog aan 2.4.6.7 Log Management

3.5.10 Packaging en Delivery

- Analoog aan 2.4.6.8 Packaging en Delivery

3.5.11 Exploitatiedossier

- De DC/Cloud ICT-Dienstverlener zal voor de aangeboden platform (PaaS) en serverdiensten (IaaS) een exploitatiedossier aanleggen en up to date houden waarin minstens volgende elementen worden opgenomen:
    - Een beschrijving van alle services die zijn inbegrepen in de dienst:
        - Frequentie van updates: minimaal vereiste frequentie maandelijks
        - beschikbaarheid planning
        - ondersteuning versie N en N-1
    - Een beschrijving van de wijze waarop migratie en upgrade van bovenliggende toepassingen moet gebeuren.

3.5.12 Continu versiebeheer:

- Upgrades en patches moeten zoveel mogelijk uitgevoerd worden in continue mode, waarbij updates kunnen worden gedeployed in een draaiend systeem zonder de actieve toepassingen en transacties te hinderen.

3.6 SLA en prijsmechanisme

Zowel LINUX servers als Wintel servers dienen deel uit te maken van deze Diensten. Ook het beheer van virtualisatielaag (bv VMWARE, …) dient inbegrepen te zijn in deze Dienst.

M.b.t. het dienstverleningsniveau moeten verschillende varianten en opties aangeboden worden (productie, ontwikkeling/ test). De Klant kan dit per server bepalen.

Er zullen Eenheidsprijzen opgenomen worden : prijzen per (fysieke of virtuele) server per maand enerzijds en prijzen per GB per maand voor de storage en back-up anderzijds. Het optimaliseren en migreren van data is inbegrepen in deze Dienst.

3.6.1 De dienst wordt geconcretiseerd door

- Identificatiegegevens van de Klant die instaat voor betalingen met betrekking tot de betrokken of servers (Financieeel Beheerder);
- Gevraagde beschikbaarheidsvenster (Uigebreide Kantooruren; 24/7)
- Aantal gigabyte en type storage (storage tier)
- Aantal gigabyte en type/speciale vereisten back-up
- Roadmap o.a. i.k.v. life cycle management
- Beschrijving van de technische en organisatorische maatregelen voor de bescherming van de binnen de servers verwerkte Persoonsgegevens en van de verantwoordelijk-heden van de Klant en de DC/Cloud ICT-Dienstverlener in dit verband. Minstens alle in artikel 30 punt 2 van de AVG opgesomde gegevens worden hierin opgenomen
- Fysieke server: small, medium, large, extra large

- Virtuele server: volgens T-shirt sizes inzake CPU en RAM
- OS licentie voor besturingssysteem (Linux, Windows)
- Mét of zonder beheer OS (Linux, Windows)
- Beheer van OS volgens 24/7 of uitgebreide kantooruren SLA
- Middleware licentie PAAS (Oracle RDBMS EE, EDB Postgresql Std, Oracle Weblogic, Apache Tomcat)
- De Middleware instance
- Mét of zonder beheer van de Middleware instance, volgens 24/7 of uitgebreide kantooruren SLA
- De bijkomende beveiligingsfuncties die toegepast worden: Next-gen FW, WAF, Load Balancer//RP, enz…
- Voor het beheer van de eigen infrastructuur van de Klanten en eventueel daarop draaiende middleware en de bijhorende (onderhouds-)contracten worden de concrete modaliteiten afgesproken in een exploitatiedossier per Klant.
- Identificatiegegevens van de Klant die instaat voor betalingen met betrekking tot de betrokken computerzaalfaciliteiten (Financieel Beheerder);

3.6.2 SLA

3.6.2.1 Beschikbaarheid van de server- en platformdiensten

Beschrijving en definitie

De beschikbaarheid van een server of middleware (platform) instance wordt beschouwd als het percentage van de tijd dat de server beschikbaar is voor de Gebruikers overeenkomstig het per server of middleware instance afgesproken beschikbaarheidsvenster en beschikbaarheidsniveau. Dit wil zeggen dat alle componenten en processen moeten functioneren en dat de onderliggende netwerken en netwerkcomponenten moeten beschikbaar zijn.

Met betrekking tot het beschikbaarheidsvenster wordt een onderscheid gemaakt tussen Uitgebreide Kantooruren en 24/24 7d/7d.

Service Level

Service Level voor een server of middleware (platform) instance

beschikbaarheidsvenster	beschikbaarheidsniveau	% beschikbaar op maandbasis tijdens de Uitgebreide Kantooruren	% beschikbaar op maandbasis buiten de Uitgebreide Kantooruren
24/24 7/7	hoog	99,70 %	99,70 %
24/24 7/7	normaal	99,50 %	99,50 %
Uitgebreide Kantooruren	hoog	99,50 %	95 %
Uitgebreide Kantooruren	normaal	99,30 %	95%

Storage

Indicator	Dienstverleningniveau
Storage systemen Tier 1, 2,3 Backup systemen	99,95 %

Geplande onbeschikbaarheden voor o.a. onderhoud zijn niet inbegrepen. De geplande onbeschikbaarheden welke de DC/Cloud ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 9 weekends per jaar) en nemen maximum 16u per maand in beslag. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

De planning wordt jaarlijks gepubliceerd naar de Klanten toe op het ICT-extranet. Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn wordt de Klant geïnformeerd over de geplande start- en eindtijden van de wijzigingen

Randvoorwaarden, assumpties en uitzonderingen

De volgende onbeschikbaarheden worden niet in aanmerking genomen voor het bepalen van de onbeschikbaarheidsduur:

- Onbeschikbaarheid veroorzaakt door bovenliggende IT-componenten die niet in beheer zijn bij de DC/Cloud ICT-Dienstverlener. Voor IaaS light servers geldt deze randvoorwaarde ook voor onbeschikbaarheid tengevolge van door de Klant uitgevoerde manipulaties met betrekking tot het besturingssysteem.
- Voor de bij de start van de overeenkomst bestaande servers: onbeschikbaarheid veroorzaakt door IT-componenten die niet langer ondersteund worden door de betrokken leverancier.

Meetelementen en –methode

De beschikbaarheid van de infrastructuurdiensten dwordt gemeten op basis van metingen met een monitoring systeem.

Voor de IaaS-Light servers wordt de beschikbaarheid van de server gemeten op basis van het registratie- en afsluitingstijdstip in het Incident managementsysteem.

3.6.2.2 Beschikbaarheid van de Internet en VO MPLS connectiviteit

Beschrijving en definitie

De beschikbaarheid van de connecties naar VO-WAN en naar internet service providers (ISP) op maandbasis wordt beschouwd als een end to end beschikbaarheid voor de Gebruiker.

Service Level

Het beschikbaarheidsvenster is 24/24 7/7 met uitzondering van de afgesproken periodes voor gepland onderhoud.

Indicator	Dienstverleningniveau

Beschikbaarheid naar VO-WAN (redundant) en naar ISP (redundant)	99,95 %

Geplande onbeschikbaarheden voor o.a. upgrades zijn niet inbegrepen. De geplande onbeschikbaarheden welke de ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 4 weekends per jaar dienstenpakket) en nemen maximum 4u per maand in beslag. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

De planning wordt jaarlijks gepubliceerd naar de Klanten toe op het ICT-extranet. Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn wordt de Klant geïnformeerd over de geplande start- en eindtijden van de wijzigingen dit minstens 14 kalenderdagen voor de uitvoering.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en worden niet in rekening gebracht bij de berekening van de SLA:

- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.

Meetelementen en –methode

De end tot end beschikbaarheidsgegevens worden maandelijks gemeten via monitoringsystemen van de ICT-Dienstverlener.

3.6.2.3 Beschikbaarheid van de centrale DC netwerk- en beveiligingsdiensten (binnen het managed DC)

Beschrijving en definitie

De beschikbaarheid van de centrale DC netwerk- en beveiligingsdiensten per afzonderlijke dienst op maandbasis. Dit omvat DC Firewall service, Next-gen FW, WAF, aDDOS, DC load balancing services, DDI (DNS, DHCP, en NTP)

Service Level

Het beschikbaarheidsvenster is 24/24 7/7 met uitzondering van de afgesproken periodes voor gepland onderhoud.

Indicator	Dienstverleningniveau
Beschikbaarheid DC/Internet Firewall services,	99,95 %
Beschikbaarheid Next-gen FW (ngFW)	99,95 %
Beschikbaarheid WAF	99,95 %
Beschikbaarheid aDDOS	99,95 %
Beschikbaarheid load balancing (reverse proxy) services (high availabilty)	99,95 %
Beschikbaarheid DDI (DNS, DHCP en NTP) (high availabilty)	99,95 %
Beschikbaarheid DC LAN service	99,95 %

Geplande onbeschikbaarheden voor o.a. upgrades zijn niet inbegrepen. De geplande onbeschikbaarheden welke de ICT-Dienstverlener nodig acht, worden in overleg met de Klant bepaald. Deze vallen telkens in een weekend (maximum 4 weekends per jaar per afzonderlijke diensten) en nemen maximum 4u per maand in beslag. De geplande onbeschikbaarheidsduur die dit maximum overschrijdt, wordt toegevoegd aan de ongeplande onbeschikbaarheidsduur.

De planning wordt jaarlijks gepubliceerd naar de Klanten toe op het ICT-extranet. Zodra de geplande wijzigingen tijdens een onderhoudsperiode gekend zijn wordt de Klant geïnformeerd over de geplande start- en eindtijden van de wijzigingen dit minstens 14 kalenderdagen voor de uitvoering.

Randvoorwaarden, assumpties en uitzonderingen

Sommige externe factoren vallen buiten de verantwoordelijkheid van de ICT-Dienstverlener en de worden niet in rekening gebracht bij de berekening van de SLA

- Specifieke gevallen van overmacht die in een overleg tussen beide partijen worden erkend.

Meetelementen en –methode

De end tot end beschikbaarheidsgegevens worden maandelijks gemeten via monitoringsystemen van de ICT-Dienstverlener.

3.6.3 Prijsmechanisme

Alle kosten inzake de hulpmiddelen voor het leveren van de managed DC infrastructuurdiensten, en ook alle ondersteunende systemen zoals hardware, software licenties, storage en backup, operationeel beheer, monitoring, logging, beveiligingsdiensten (o.a. FW, DAR en DIM encryptie), … zijn in de prijs van de diensten inbegrepen; Alle beveiligingsdiensten, tools en processen, die niet via afzonderlijke eenheidsprijzen en werkaanvragen worden aangerekend, zijn in de eenheidsprijzen van de IAAS en PAAS diensten inbegrepen;

3.6.3.1 IAAS Fservers

- Forfaitaire eenheidsprijzen per maand en per instance voor IAAS FServers

IAAS server - Ter beschikking gestelde fysieke server Small 8 cores, 16 Threads, 32 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Small 10 cores, 20 Threads, 32 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Medium 8 cores, 16 Threads, 64 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Medium 10 cores, 20 Threads, 64 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Large 16 cores, 32 Threads, 384 GB RAM
IAAS server - Ter beschikking gestelde fysieke server Large 20 cores, 40 Threads, 384 GB RAM
IAAS server - Ter beschikking gestelde fysieke server XLarge 32 cores, 64 Threads, 512 GB RAM
IAAS server - Ter beschikking gestelde fysieke server XLarge 40 cores, 80 Threads, 512 GB RAM

    - Deze prijs omvat

- De prijs van de ter beschikking gestelde Fserver hardware inclusief de onderliggende CZF diensten, de onderliggende DC netwerkdiensten, alle beheerstaken die gebonden zijn aan het operationele beheer van de Fserver

- Bemerk dat de eenheidsprijzen betrekking hebben op alle Fserver types, maar dat het actuele aanbod kan beperkt zijn tot één Fserver type per categorie: Small, Medium, Large, XLarge;

3.6.3.2 IAAS Fserver Operating System

- Forfaitaire eenheidsprijzen per maand en per instance voor IAAS FServer OS licenties
  - Er is een keuze tussen
    - Windows Server Datacenter
    - Windows Server Standard
    - Red Hat Enterprise Linux Server - Standard of Premium
    - Red Hat Enterprise Linux Server for Virtual Datacenters - Standard of Premium

Licenties Windows Server Datacenter (als onderdeel van Managed DC IAAS - Fysieke Server met 8 cores, 16 threads)
Licenties Windows Server Datacenter (als onderdeel van Managed DC IAAS - Fysieke Server met 10 cores, 20 threads)
Licenties Windows Server Datacenter (als onderdeel van Managed DC IAAS - Fysieke Server met 16 cores, 32 threads)
Licenties Windows Server Datacenter (als onderdeel van Managed DC IAAS - Fysieke Server met 20 cores, 40 threads)
Licenties Windows Server Datacenter (als onderdeel van Managed DC IAAS - Fysieke Server met 32 cores, 64 threads)
Licenties Windows Server Datacenter (als onderdeel van Managed DC IAAS - Fysieke Server met 40 cores, 80 threads)
Licenties Windows Server Standard (als onderdeel van Managed DC IAAS - Fysieke Server met 8 cores, 16 threads)
Licenties Windows Server Standard (als onderdeel van Managed DC IAAS - Fysieke Server met 10 cores, 20 threads)
Licenties Windows Server Standard (als onderdeel van Managed DC IAAS - Fysieke Server met 16 cores, 32 threads)
Licenties Windows Server Standard (als onderdeel van Managed DC IAAS - Fysieke Server met 20 cores, 40 threads)
Licenties Windows Server Standard (als onderdeel van Managed DC IAAS - Fysieke Server met 32 cores, 64 threads)
Licenties Windows Server Standard (als onderdeel van Managed DC IAAS - Fysieke Server met 40 cores, 80 threads)
Licenties Red Hat Enterprise Linux Server Standard (als onderdeel van Managed DC IAAS - Fysieke Server)
Licenties Red Hat Enterprise Linux Server Premium (als onderdeel van Managed DC IAAS - Vserver of Fysieke Server)
Licenties Red Hat Enterprise Linux Server for Virtual Datacenters - Standard (als onderdeel van Managed DC IAAS - Fysieke Server)
Licenties Red Hat Enterprise Linux Server for Virtual Datacenters - Premium (als onderdeel van Managed DC IAAS - Fysieke Server)

3.6.3.3 IAAS Fserver OS beheer

- Forfaitaire eenheidsprijzen per maand en per instance voor OS beheer van een IAAS FServer;

Beheer van OS - FYS server	Managed DC - IAAS Server	UKT	LINUX
Beheer van OS - FYS server	Managed DC - IAAS Server	UKT	Windows
Beheer van OS - FYS server	Managed DC - IAAS Server	24/7	LINUX
Beheer van OS - FYS server	Managed DC - IAAS Server	24/7	Windows

3.6.3.4 IAAS Vservers

IAAS Vservers

- Forfaitaire eenheidsprijzen per maand en per instance voor IAAS VServers
    - De prijs van een IAAS Vserver wordt samengesteld uit
        - het aantal VCPUs x de eenheidsprijs per “Ter beschikking gestelde VCPU”
        - De hoeveelheid VRAM x de eenheidsprijs per “Ter beschikking gestelde VRAM”
    - Deze eenheidsprijzen kunnen gecombineerd worden in de verschillende T-shirt sizes van Vservers die toegepast worden;
    - Deze prijs omvat
        - De prijs van de ter beschikking gestelde Fserver hardware inclusief de onderliggende CZF diensten, de Server Virtualisatie licentie en beheer, de onderliggende DC netwerkdiensten, alle beheerstaken die gebonden zijn aan het operationele beheer van de Fserver, de server virtualisatie;
        - De kostprijs van de redundante DC Internet toegang
        - De kostprijs van de netwerkverbinding (2x10Gbps naar de VO POPs)
        - De kostprijs van de basis beveiligingsdiensten, tools en processen
            - Basic Firewall
            - Threat intelligence/ Threat hunting
            - Logging van alle DC security functies, incl FW, en de opslag en het doorsturen van de log informatie naar de SIAM (SIEM service);
        - De kostprijs van de extra beveiligingsdiensten is niet inbegrepen, en wordt apart aangerekend:
            - Load Balancer/RP;
            - Next-gen FW (ngFW);
            - WAF;

3.6.3.5 IAAS Vserver Operating System

- Forfaitaire eenheidsprijzen per maand en per instance voor het ter beschikking stellen van een IAAS VServer OS licentie
    - Er is een keuze tussen
        - Windows Server: - Standard of Datacenter licentie
        - Red Hat Enterprise Linux Server: - Standard of Premium
    - "IAAS Vserver OS beheer" maakt deel uit van de "IAAS" dienst, waarin steeds ook de gerelateerde IAAS diensten moeten afgenomen worden: IAAS Vserver of Fserver;

3.6.3.6 IAAS Vserver OS beheer

- Forfaitaire eenheidsprijzen per maand en per instance voor OS beheer van een IAAS VServer
    - Er is een keuze tussen
        - Uitbatings SLA: 24/7 of uitgebreide kantooruren (UKT)
        - Operating System: Linux of Windows

Beheer van OS - Vserver	Managed DC/Cloud Traditioneel	24/7	LINUX
Beheer van OS - Vserver	Managed DC/Cloud Traditioneel	24/7	Windows
Beheer van OS - Vserver	Managed DC/Cloud Traditioneel	UKT	LINUX
Beheer van OS - Vserver	Managed DC/Cloud Traditioneel	UKT	Windows

    - De kostprijs omvat ook de Anti-Virus en Anti-malware oplossing voor de Vserver;
    - De eenheidsprijs is van toepassing voor Managed DC – beheer van een IAAS Vserver, (en ook voor Cloud Traditioneel beheer);
    - "IAAS Vserver OS beheer" maakt deel uit van de "IAAS" dienst, waarin steeds ook de gerelateerde IAAS diensten moeten afgenomen worden: IAAS Vserver of Fserver, Server OS licentie;

3.6.3.7 IAAS Vserver Active-Active opstelling

- Forfaitaire eenheidsprijzen per maand en per instance voor IAAS VServer Active-Active opstelling;
    - Dit is een toeslag ingeval voor DR een Active-Active server opstelling wordt toegepast.
    - De prijs wordt 1 keer aangerekend per server-opstelling (2 servers: één in DC site A en één in DC site B)
    - De totale prijs voor een Active-Active server opstelling bestaat dus uit de prijs van 2 Vservers (CPU, RAM, OS licentie, OS beheer) plus de prijs voor de Vserver opstelling

- Bemerk dat voor de Storage diensten een Active-Active opstelling dient toegepast te worden, en dat de applicatie hierop moet ingericht zijn;
- Bemerk dat de DC/Cloud dienstverlener normaliter geen interventie uitvoert om de fail-over te laten uitvoeren; De overschakeling gebeurt op vlak van de infrastructuurlaag transparant;

3.6.3.8 IAAS Vserver Active-Passive opstelling

- Forfaitaire eenheidsprijzen per maand en per Vserver instance voor IAAS VServer Active-Passive opstelling;
  - De prijs wordt aangerekend per Vserver in Site A waarop de Active-Passive-opstelling op van toepassing is, voor eenzelfde aantal VCPU en VRAM als de Vserver in Site A.
  - Dit is een toeslag ingeval voor DR een Active-Passive opstelling wordt toegepast, die de kosten voor de reservering van de Vserver hardware (VCPU en RAM) in DC site B omvat;
    - IAAS Server - Gereserveerde VCPU in DC site B
    - IAAS Server - Gereserveerde VRAM in DC site B
  - De prijs voor de gereserveerde hoeveelheid op Site B is maximaal de prijs voor hoeveelheid VCPU en VRAM van de Vserver;

- Forfaitaire eenheidsprijzen per maand en per instance voor het beheer van een server Active-Passive opstelling
  - Dit is een toeslag ingeval voor DR een Active-Passive opstelling wordt toegepast, die de kosten voor het beheer van de Active Passive opstelling omvat, zoals de kosten voor het omschakelen van Site A naar Site B en vice versa;
  - De totale prijs voor een Active-Passive server opstellling bestaat dus uit de prijs van 1 Vserver (CPU, RAM, OS licentie, OS beheer) in Site A plus de prijs voor de reservering van de Vserver hardware in Site B plus de kost voor het beheer van de Active-Passive opstelling, dus met inbegrip van de overschakeling;
  - Bemerk dat de DC/Cloud dienstverlener zorgt voor het opstarten van de servers op Site B, en het koppelen van de servers aan de storage. Ingeval een hypervisor image werd gemaakt, kan de volledige server image met de applicatiecomponenten opgestart worden; De dienstenleverancier staat niet in voor de database-restore noch voor de applicatie herstart;

3.6.3.9 IAAS Storage

IAAS Storage

- een Eenheidsprijs per ter beschikking gestelde netto gigabyte per maand voor gegevensopslag volgens opslag Tier

IAAS Storage - ter beschikking gestelde gegevensopslag Tier 1 non-replicated
IAAS Storage - ter beschikking gestelde gegevensopslag tier 2 non-replicated
IAAS Storage - ter beschikking gestelde gegevensopslag tier 3 non-replicated
IAAS Storage - ter beschikking gestelde gegevensopslag Tier 1 replicated
IAAS Storage - ter beschikking gestelde gegevensopslag tier 2 replicated
IAAS Storage - ter beschikking gestelde gegevensopslag tier 3 replicated

  - Deze prijs omvat
    - De prijs van de ter beschikking gestelde Storage hardware en software inclusief de onderliggende CZF diensten, de onderliggende DC netwerkdiensten,
    - alle beheerstaken die gebonden zijn aan het operationele beheer van de Storage systemen en operaties:
  - “IAAS storage” maakt deel uit van de “IAAS” dienst, waarin steeds ook de gerelateerde IAAS diensten moeten afgenomen worden: IAAS Vserver of Fserver, Server OS licentie, server OS beheer;
  - De prijs voor storage wordt berekend op het volledige door de klant gealloceerde volume en omvat ook het volume nodig voor de snapshot copieën;
  - De prijs voor een “replicated” storage omvat de kostprijs van de beide copieën, en de kostprijs voor de Storage replicatie;

3.6.3.10 IAAS Backup

- een Eenheidsprijs per op back-up-medium opgeslagen gigabyte per maand voor back-up.
  - Deze prijs omvat
    - De prijs van de ter beschikking gestelde backup hardware en software inclusief de onderliggende CZF diensten, de onderliggende DC netwerkdiensten, alle backup software- en tools:
    - alle beheerstaken die gebonden zijn aan het operationele beheer van de backup systemen en operaties, met uitzondering voor de betalende service requests;

- "IAAS backup" maakt deel uit van de "IAAS" dienst, waarin steeds ook alle onderliggende diensten moeten afgenomen worden: IAAS Vserver of Fserver, Server OS licentie, server OS beheer, IAAS Storage, enz…

3.6.3.11 Middleware beheer

Managed DC Middleware beheer

- Forfaitaire eenheidsprijzen per maand en per instance voor beheer van een Middleware instance
    - Deze prijs is specifiek voor elk type van middleware – zie tabel met middlewares hieronder
    - Er wordt een onderscheid gemaakt tussen 24/7 en uitgebreide kantooruren
    - De prijs is van toepassing op de diensten
        - Managed DC beheer van middelware
        - Cloud deel 2.B (CloudOPS beheer)
        - Cloud deel 3.B (Cloud Traditioneel beheer)
    - Deze prijs omvat
        - alle beheerstaken die gebonden zijn aan het operationele beheer van de middleware:
    - "Managed DC Middleware beheer" maakt deel uit van de "PAAS" dienst, waarin steeds ook alle onderliggende diensten moeten afgenomen worden: IAAS Vserver of Fserver, Server OS licentie, server OS beheer, IAAS Storage, IAAS Backup, enz…

Beheer van middleware ACTIVEMQ Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux
Beheer van middleware Apache HTTP SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux
Beheer van middleware TOMCAT Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux
Beheer van middleware POSTGRES PLUS ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware .NET FRAMEWORK Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Windows
Beheer van middleware INTERNET INFORMATION SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Windows
Beheer van middleware SQL SERVER ENTERPRISE Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware SQL SERVER STANDARD Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware NGINX Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux
Beheer van middleware INTERNET APPLICATION SERVER ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware JDK Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux
Beheer van middleware MYSQL Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows

Beheer van middleware ORACLE APPLICATION EXPRESS (APEX) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux
Beheer van middleware ORACLE CONTAINER FOR JAVA EE (OC4J) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware ORACLE DATABASE ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware ORACLE DATABASE STANDARD EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware WEBLOGIC SERVER ENTERPRISE Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux
Beheer van middleware WEBLOGIC SERVER STANDARD Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux
Beheer van middleware POSTGRESQL Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware JBOSS APPLICATION SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware JBOSS ENTERPRISE APPLICATION PLATFORM (EAP) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	UKT	Linux/ Windows
Beheer van middleware ACTIVEMQ Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux
Beheer van middleware Apache HTTP SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux
Beheer van middleware TOMCAT Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux
Beheer van middleware POSTGRES PLUS ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware .NET FRAMEWORK Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Windows
Beheer van middleware INTERNET INFORMATION SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Windows
Beheer van middleware SQL SERVER ENTERPRISE Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware SQL SERVER STANDARD Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware NGINX Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux
Beheer van middleware INTERNET APPLICATION SERVER ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware JDK Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux
Beheer van middleware MYSQL Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware ORACLE APPLICATION EXPRESS (APEX) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux
Beheer van middleware ORACLE CONTAINER FOR JAVA EE (OC4J) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware ORACLE DATABASE ENTERPRISE EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware ORACLE DATABASE STANDARD EDITION Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware WEBLOGIC SERVER ENTERPRISE Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux
Beheer van middleware WEBLOGIC SERVER STANDARD Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux
Beheer van middleware POSTGRESQL Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows

Beheer van middleware JBOSS APPLICATION SERVER Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows
Beheer van middleware JBOSS ENTERPRISE APPLICATION PLATFORM (EAP) Cloud Deel 2.B. Cloud Deel 3.B. , Managed DC middleware	Managed DC/Cloud Traditioneel/CloudOPS	24/7	Linux/ Windows

3.6.3.12 PAAS licenties

- Forfaitaire eenheidsprijzen per maand en per instance voor het ter beschikking stellen van een licentie voor een Middleware instance, als onderdeel van Managed DC - PAAS
    - In deze prijs is de licenties en de software maintance inbegrepen.

Licenties (als onderdeel van Managed DC PAAS) TOMCAT; per Instance
Licenties (als onderdeel van Managed DC PAAS) ORACLE DATABASE ENTERPRISE EDITION; Per VCPU, oversubscription = 4
Licenties (als onderdeel van Managed DC PAAS) ORACLE WEBLOGIC; Per VCPU, oversubscription = 4
Licenties (als onderdeel van Managed DC PAAS) EDB POSTGRESQL Standard; Per VCPU, oversubscription = 4

    - Waar de eenheidsprijs steunt op een VCPU, gebeurt de omrekening naar Cores op basis van een oversubscription factor = 4;
    - Voor werkaanvragen en service requests geldt:
        - “applicatie servers”: Tomcat en Oracle Weblogic
        - “database servers”: Oracle Database EE en EDB PostgreSQL
    - Voor alle andere middleware producten dient de klant via een werkaanvraag de nodige software licenties aan te kopen;
    - Indien de klant al over een geschikte licentie beschikt, dan kan hij die toepassen (Bring your own license); Dit is de keuze van de klant;
    - PAAS licenties maken deel uit van de “PAAS” dienst, waarin steeds ook het beheer van de middleware moet afgenomen worden, en ook alle onderliggende diensten: Vserver of Fserver, Server OS licentie, server OS beheer, Storage, Backup.

- prijzen voor VO specifieke contracten. Het betreft hier de in de VO-specifieke contracten afgesproken Eenheidsprijzen. Voor VO-specifieke contracten die gebruikt worden voor meerdere servers , wordt een zo correct mogelijke versleuteling gebruikt.

In de bovenstaande prijzen zijn alle door de DC/Cloud ICT-Dienstverlener te leveren Diensten verrekend opdat de Gebruiker de platform- en serverdiensten zou kunnen gebruiken vanaf zijn werkplek, met inbegrip van het beheer van de bijbehorende storage en back-up-omgevingen,de computerzaalfaciliteiten ,de erbij horende netwerkcomponenten alsook alle nodige licenties en (onderhouds)contracten nodig om de server omgevingen volgens de afgesproken vereisten te exploiteren. In deze prijzen zijn eveneens inbegrepen : redundante internet toegang, redundante Datacenter netwerkomgeving en redundante Datacenter Firewall/IPS omgeving

Voor wat betreft de Exploitatie van netwerk en beveiliging op infrastructuur van de DC-Dienstleverancier:

- een Eenheidsprijs voor een DC Firewall service per toepassing
- een Eenheidsprijs voor een Loadbalancing/Reverseproxy service per toepassing (op basis van één VIP)
- een Eenheidsprijs voor redundante DC Internet toegang (per 1 Gbit/s)

3.6.3.13 IAAS Storage - SMB File Server

IAAS Storage - SMB File Server - ter beschikking gestelde gegevensopslag en File Server

- een Forfaitaire eenheidsprijs per maand en per klant per ter beschikking gestelde gigabyte per maand op een SMB File Server.
    - Deze prijs omvat alle hard- en software, en alle diensten die nodig zijn om de dienst te leveren:
        - De prijs van de SMB File Server; De licentie is op basis van de Windows Server licentie;
        - De prijs van de storage. Die is gebaseerd op de prijs en karakteristieken van Storage Tier 2
        - De prijs van de ter beschikking gestelde File Server en Storage hardware en software inclusief de licenties voor OS, Backup, beheertools, en de server hardware, OS licentie incl File Server licentie, server virtualisatie licentie, ook de onderliggende CZF diensten, de onderliggende DC netwerkdiensten en verbindingen met de VO POPs;
        - alle beheerstaken die gebonden zijn aan het operationele beheer van de File Server, zoals afhandeling van requests van gebruikers, met uitzondering voor de betalende service requests of werkaanvragen;
        - Alle beheerstaken die gebonden zijn aan het operationele beheer van de File Server, de server zelf (OS beheer, beheer van server virtualisatie), de Storage systemen, Backup systemen en File Server operaties:

3.6.3.14 IAAS Beveiligingsdiensten

Aanvullend worden ook kosten aangerekend voor de bijkomende beveiligingsdiensten in het managed DC, die de klant inzet, zoals WAF, Next-Gen FW (ngFW), enz….

- Het betreft hier maandelijkse eenheidsprijzen die per beveiligingsdienst en per eenheid worden verrekend aan de klant;
- Alle kosten inzake managed DC infrastructuurdiensten, software, licenties, operationeel beheer, logging, doorsturen van logs, … zijn in de prijs inbegrepen;
- De forfaitaire maandelijkse eenheidsprijs voor het ter beschikking stellen van een Next-Gen FW (ngFW) in het managed DC.
  - Het betreft hier een maandelijkse eenheidsprijs die per virtueel systeem wordt verrekend aan de klant, volgens bandbreedte,
    - € per 200M virtueel systeem
    - € per 500M virtueel systeem
    - € per 1000M virtueel system
- De forfaitaire maandelijkse eenheidsprijs voor het ter beschikking stellen van een WAF in het managed DC.
  - Het betreft hier een maandelijkse eenheidsprijs die per VIP/APP wordt verrekend aan de klant, volgens bandbreedte, met een beperking van max 3 backend servers
    - € per VIP-25M
    - € per VIP-200M
- De forfaitaire maandelijkse eenheidsprijs voor het ter beschikking stellen van een Load Balancer / Reverse Proxy in het managed DC
  - Het betreft hier een maandelijkse eenheidsprijs die VIP wordt verrekend aan de klant;

3.6.3.15 VO specifieke contracten

Aanvullend worden ook kosten aangerekend voor de VO-specifieke contracten die nodig zijn voor de te beheren platform- en serverinstanties en die maandelijks verrekend worden;

- Het betreft hier de in de VO-specifieke contracten afgesproken Eenheidsprijzen die maandelijks of jaarlijks per eenheid worden verrekend aan de klant;
- Voor VO-specifieke contracten die gebruikt worden voor meerdere Klanten, wordt een zo correct mogelijke versleuteling gebruikt

3.6.3.16 Facturatie

Maandelijks wordt de factuur overgemaakt aan de Klant die de bestelling heeft geplaatst. Deze factuur bevat:

- Het totaal voor het beschikbaar houden van de platformen voor de betrokken Klant, volgens de gevraagde beschikbaarheid;
- Het totaal voor het beschikbaar houden van de server,storage en back-up capaciteit voor de betrokken Klant, volgens de gevraagde beschikbaarheid;
- Het totaal voor het beschikbaar houden van een DC Firewall service voor de betrokken klant;
- Het totaal voor het beschikbaar houden van een loadbalancing/Reverseproxy service voor de betrokken klant;
- Het totaal voor het beschikbaar houden van 2x 10Gbits/s redundante private connectiviteit naar 2 VO POPs voor de betrokken klant;
- Het totaal voor het beschikbaar houden van redundante DC Internet toegang voor de betrokken Klant
- De maandelijks verrekende kosten voor de voor de managed datacenterdiensten gebruikte VO-specifieke contracten. Deze worden onderbouwd door de geldende contractuele documenten van die VO-specifieke contracten in DDC-DMS. Indien de contractkost volume-gedreven is, dient naast de onderbouwing van de gebruikte Eenheidsprijzen ook een rapportering meegegeven te worden waaruit de reële volumes blijken.
- Indien de SLA m.b.t. de beschikbaarheid van de managede datacenterdienst niet gehaald wordt dan is de Prijscorrectie zoals voorzien in het Basiscontract van toepassing, maar deze wordt niet toegepast op het bedrag dat betrekking heeft op de VO-specifieke contracten. Daarnaast zijn ook de in het kader van de VO-specifieke contracten bepalingen m.b.t. eventuele prijsverminderingen bij het niet halen van de afspraken in dat contract ook van toepassing.

3.6.3.17 Rapportering

Maandelijks wordt per Klant een overzicht gegeven van :

- De SLA-metrieken.
- Rapportering van de als onderbouwing van de facturen vereiste gegevens waaronder de hoeveelheden die in de voorbije periode werden afgenomen voor volume-gedreven kosten.

3.6.4 Eenvoudige Werkaanvragen

Het bestelproces (opmaken van een offerte – uitvoering - facturatie) voor het afnemen van platformdiensten is snel, flexibel en transparant voor de Klant. De bestellingen zullen net zoals andere bestellingen m.b.t. exploitatiegebonden Diensten via één bestelkanaal kunnen ingediend worden.

Bij het ter beschikking stellen, wijzigen en stopzetten van een PaaS-dienst is het van groot belang om de gevraagde dienst snel en geautomatiseerd te kunnen provisioneren, wijzigen en stopzetten.

Voor platformdiensten waarbij de klant gebruik wenst te maken van legacy en internet protocollen om de toepassing te ontsluiten naar hun gebruikers op het intranet dienen bijkomend een Firewall werkaanvraag

Bij het plaatsen van een bestelling zal de DC/Cloud ICT-Dienstverlener nakijken of de persoon die de bestelling plaatst daartoe geautoriseerd is volgens de afspraken die met de Klant gemaakt zijn en of de nodige identificatiegegevens voor facturatie van de bestelling zijn opgegeven.

Er wordt voor gezorgd dat de Klant zicht heeft op de status van zijn bestellingen.

De DC/Cloud ICT-Dienstverlener stuurt de verschillende operationele betrokkenen aan voor de uitvoering van de betrokken Diensten. Hieronder worden de specifieke uitvoeringsmodaliteiten per Dienst beschreven.

Onderstaande types Eenvoudige Werkaanvragen hebben enkel betrekking op PaaS-Diensten die afgenomen worden op de platformen van de DC/Cloud ICT-Dienstverlener, tenzij expliciet anders vermeld.

3.6.4.1 Eenvoudige werkaanvragen platformdiensten

3.6.4.1.1 Wijzigingen m.b.t. gebruikersidentificatie: nieuwe gebruikersID's aanmaken, bestaande gebruikersID's wissen of wijzigen

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een nieuwe gebruikersID aan te maken, te wijzigen of te wissen.

3.6.4.1.2 Verlenen/Wijzigen/Verwijderen van toegang tot een databankplatform of applicatieserver

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om voor een bepaalde Gebruiker, welke reeds beschikt over een gebruikersID, toegangsrechten m.b.t. een databankplatform of applicatieserver te verlenen, te wijzigen of te verwijderen.

3.6.4.1.3 Aanvragen van een PAAS databaseplatform met een niet gedeeld OS/MW

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een databankplatform met niet gedeeld OS/MW ter beschikking te stellen en maandelijks beschikbaar te houden. Deze Dienst is inclusief het verlenen van toegangsrechten voor 1 beheerder, opzetten van OS en Middleware storage/Backup

Hiervoor worden volgende activiteiten uitgevoerd en ingeregeld:

- Validatie van de bestelling, opzetten van de server en installatie van de PaaS component.
- Indien gevraagd ontsluiting naar het internet
- De inregeling van de nodige toegangen tot deze component
- De inregeling van de monitoring: Klant notificaties en beheer monitoring
- CMDB registratie van het bestelde platform.

Bijkomende vragen kunnen behandeld worden via ondersteuning in regie m.b.t. Cloud- en Datacenterdiensten.

3.6.4.1.4 Aanvraag voor stopzetten van een PAAS databaseplatform (met een niet gedeeld OS/MW)

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een databankplatform (met niet gedeeld OS/MW) stop te zetten. Deze Dienst is inclusief het verwijderen van alle toegangsrechten (inclusief deze van beheerders), nemen van

backups, verwijderen netwerk configuratie, updaten van CMDB, stopzetten van bijhorende storage (OS en bijkomende storage), en het verwijderen van de monitoring.

3.6.4.1.5 Aanvragen van een PAAS application server met een niet gedeeld OS/MW

Via deze Dienst kan gevraagd worden aan de DC/Cloud ICT-Dienstverlener om een applicatieserver met niet gedeeld OS/MW ter beschikking te stellen en maandelijks beschikbaar te houden. Deze Dienst is inclusief het verlenen van toegangsrechten voor 1 beheerder, opzetten van een gedeelde OS en Middleware storage/Backup

Hiervoor worden volgende activiteiten uitgevoerd en ingeregeld:

- Validatie van de bestelling, opzetten van de server en installatie van de PaaS component.
- Indien gevraagd ontsluiting naar het internet
- De inregeling van de nodige toegangen tot deze component
- De inregeling van de monitoring: Klant notificaties en beheer monitoring
- CMDB registratie van het bestelde platform.

Bijkomende vragen kunnen behandeld worden via ondersteuning in regie m.b.t. Cloud- en Datacenterdiensten.

3.6.4.1.6 Aanvraag voor stopzetten van een PAAS application server (met een niet gedeeld OS/MW)

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een application server (met niet gedeeld OS/MW) stop te zetten. Deze Dienst is inclusief het verwijderen van alle toegangsrechten (inclusief deze van beheerders), nemen van backups, verwijderen netwerk configuratie, updaten van CMDB, stopzetten van bijhorende storage (OS en bijkomende storage), en het verwijderen van de monitoring

3.6.4.1.7 Wijzigen storage en/of back-up capaciteit

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om de storage- en/of backup capaciteit te wijzigen.

3.6.4.2 Eenvoudige Werkaanvragen serverdiensten

3.6.4.2.1 Wijzigingen m.b.t. gebruikersidentificatie: nieuwe gebruikersID's aanmaken, bestaande gebruikersID's wissen of wijzigen

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een nieuwe gebruikersID aan te maken, te wijzigen of te wissen.

3.6.4.2.2 Verlenen/Wijzigen/Verwijderen van toegang tot een server

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om voor een bepaalde Gebruiker, welke reeds beschikt over een gebruikersID, toegangsrechten m.b.t. een server te verlenen, te wijzigen of te verwijderen.

3.6.4.2.3 Ter beschikking stellen en opzetten van een fysieke server

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een fysieke server in een datacenter van de DC/Cloud ICT-Dienstverlener ter beschikking te stellen en op te zetten zodat de server gebruiksklaar is voor en kan benaderd worden door de Klant (voor installatie middlewares, toepassingen,…). De Klant kan hierbij kiezen uit enkele mogelijke configuraties. Het betreft het ter beschikking stellen van een fysieke server voor een Klant die enkel infrastructuurdiensten wenst en alle bovenliggende middleware en toepassingen zelf of door derden wenst te (laten) installeren en beheren. De dienst is inclusief basis installatie van het Operating systeem en integratie in het netwerk, in combinatie met de onderliggende computerzaalfaciliteiten en de configuratie, integratie van 100 GB storage voor het OS en het opzetten van toegangsrechten voor 1 beheerder.

Het opzetten van bijkomende storage maakt deel uit van een ander type Eenvoudige Werkaanvraag (wijzigen storage capaciteit) .

3.6.4.2.4 Stopzetten van een fysieke server (incl. bijhorende storage and backup)

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een fysieke server in een datacenter van de DC/Cloud ICT-Dienstverlener stop te zetten. De Klant kan hierbij kiezen om een backup van de server te vragen (vb:server image). Het betreft het stopzetten van een fysieke server door de Klant gebruikt voor infrastructuurdiensten. De dienst is inclusief nemen van server backup, stopzetten computerzaalfaciliteiten, verwijderen netwerk configuratie, opruimen materiaal, updaten van CMDB, stopzetten van storage (OS en bijkomende storage), het verwijderen van toegangsrechten van beheerders alsook het exporteren en in een standaard uitwisselingsformaat ter beschikking stellen van alle software en gegevens van de Klant.

3.6.4.2.5 Ter beschikking stellen en opzetten van een virtuele server

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een virtuele server met een bepaalde capaciteit ter beschikking te stellen en op te zetten. De Klant kan hierbij kiezen uit enkele mogelijke afmetingen.

De dienst is inclusief basis installatie van het Operating systeem en integratie in het netwerk, in combinatie met de onderliggende computerzaalfaciliteiten, de configuratie en integratie van 100 GB storage voor het OS, evenals het opzetten van toegangsrechten voor 1 beheerder.

Het opzetten van storage maakt deel uit van een ander type Eenvoudige Werkaanvraag (wijzigen storage capaciteit) .

3.6.4.2.6 Stopzetten van een virtuele server (incl. bijhorende storage and backup)

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een virtuele server in een datacenter van de DC/Cloud ICT-Dienstverlener stop te zetten. De Klant kan hierbij kiezen om een backup van de server te vragen (vb:snapshot). dienst is inclusief nemen van server backup, stopzetten computerzaalfaciliteiten, verwijderen netwerk configuratie, updaten van CMDB, stopzetten van storage (OS en bijkomende storage), het verwijderen van toegangsrechten van beheerders alsook het exporteren en in een standaard uitwisselingsformaat ter beschikking stellen van alle software en gegevens van de Klant.

3.6.4.2.7 Wijzigen van een virtuele server capaciteit

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om de capaciteit van een virtuele server te wijzigen. Bij de uitbreiding van de capaciteit (bijkomende virtuele CPU's en/of bijkomende GB RAM-geheugen) zal, afhankelijk van de standaard configuraties van de DC/Cloud ICT-Dienstverlener steeds gekozen worden voor de configuratie die het best beantwoordt aan de vraag van de Klant.

3.6.4.2.8 Wijzigen storage capaciteit

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om de storage capaciteit horende bij een afgenomen virtuele of fysieke server te wijzigen.

De Klant kan kiezen uit enkele mogelijke storage kwaliteitsklassen (tier 1, tier 2, tier 3, ..), afhankelijk van de omgeving waarvoor de storage gebruikt wordt, variërend van hoge performantie, lagere antwoordtijd tot lage performantie, hogere antwoordtijd.

3.6.4.2.9 Stopzetten afname storage en/of backup

Via deze Dienst kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om de afname van storage en/of backup stop te zetten. Dit omvat ook het exporteren en in een standaard uitwisselingsformaat ter beschikking stellen van alle software en gegevens van de Klant.

3.6.4.2.10 Data restore op verzoek van de Klant van maximum 50 aparte files of 5 directories (maximum capaciteit 200 GB) per aanvraag met behoud van de oorspronkelijke locatie

Via deze Werkaanvraag kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om door de Gebruikers gewiste bestanden van een back-up medium terug te halen (maximum 50 files of 5 directories, met een maximum totaal volume van 600 GB). Deze werkaanvraag betreft enkel het terugzetten van door een Gebruiker gewiste bestanden en niet een restore na een technisch falen, welke onderdeel is van de recurrente exploitatie-activiteiten.

3.6.4.2.11 Data restore op verzoek van de Klant van een onbeperkt aantal files of directories met behoud van de oorspronkelijke locatie of voor een data

restore uit de laatste back-up naar een andere locatie dan de oorspronkelijke

Via deze Werkaanvraag kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om door de Gebruikers gewiste bestanden (onbeperkt aantal) van een back-up medium terug te halen.

3.6.4.2.12 Data restore op verzoek van de Klant van een volledige server

Via deze Werkaanvraag kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om de data van een volledige server te restoren (exclusief OS).

3.6.4.3 Eenvoudige werkaanvragen netwerk en beveiliging

Voor de forward proxy functionaliteit (URL filtering etc) evenals voor ‘authoritative DNS’ kan beroep gedaan worden op de diensten van de Netwerk leverancier.”

3.6.4.3.1 Werkaanvraag mbt het toevoegen/wijzigen/verwijderen van configuraties op loadbalancers / WAF/Next-Gen FW

Deze Dienst richt zich op Klanten die gebruik wensen te maken van de loadbalancer/proxy functionaliteit binnen het DC. Via deze Dienst kunnen ze een aanvraag doen voor het toevoegen, verwijderen of wijzigen van een configuratie

Voorbeelden hiervan zijn :

- Aanmaken/aanpassen/verwijderen van een VIP
- Veranderen van de throughput parameter;
- Veranderen van een parameter op de Next-Gen FW
- Doorverwijzen van een URL:
    - Bron-URI:http://www.vlaanderen.be/cultuur
      Doel-URI: https://cjsm.be/cultuur/
- SSL offloading
- Activeren of desactiveren van een doorverwijzing met daarop een instelbare boodschap naar een standaard Sorry pagina

3.6.4.3.2 Werkaanvraag voor het aanpassen van datastromen op de DC/Internet Firewall(s)

Via deze dienst kan de Klant aan de DC-Dienstverlener een aanvraag doen voor het aanpassen van datastromen op de DC/Internet firewall. Deze firewalls worden door de ICT-Dienstverlener beschikbaar gehouden maar op vraag van de Klant is het mogelijk om via deze dienst bijkomende datastromen open te zetten of bestaande datastromen af te sluiten.

3.6.4.4 Geconcretiseerd door

- Identificatiegegevens van de Klant die instaat voor betalingen met betrekking tot de betrokken dienst;
- Type platform (databaseplatform,applicatieserver);
- Productie, ontwikkel/testplatform;
- Gevraagde beschikbaarheidsvenster (Uigebreide Kantooruren; 24/24);
- aantal gigabyte en type storage
- aantal gigabyte en type/speciale vereisten back-up
- Beschrijving van specifieke taken die uit te voeren zijn met betrekking tot de platformen.
    - Beheerstools en de toepasselijke gebruiksmodaliteiten voor de Klant, die bij het platform horen en mee aangeboden worden. Incl. integratiemogelijkheden (bijv. DNS naam, te gebruiken API's, protocol en poort, …) i.f.v. een reële benutting van het platform.
- Roadmap o.a. i.k.v. life cycle management
- Fysieke server: small, medium, large, extra large
- virtuele server: extra small, small, medium, large, extra large, extra extra large
- Mét of zonder beheer OS
- Besturingssysteem (Linux, Windows)
- Productie-, ontwikkel/testserver
- Beschikbaarheidsvenster: 24/24 7d/7d, Uitgebreide Kantooruren
- aantal gigabyte en type storage
- aantal gigabyte /speciale vereisten back-up
- Beschrijving van de technische en organisatorische maatregelen voor de bescherming van de binnen het platform en/of server verwerkte Persoonsgegevens en van de verantwoordelijkheden van de Klant en de DC/Cloud ICT-Dienstverlener in dit verband. Minstens alle in artikel 30 punt 2 van de AVG opgesomde gegevens worden hierin opgenomen.

3.6.4.5 SLA

3.6.4.5.1 Tijdige uitvoering van Eenvoudige Werkaanvragen i.k.v. platformdiensten

Beschrijving en definitie

Per Dienst zal gemeten worden of deze Dienst binnen de contractuele Service level (zie in onderstaande tabel opgenomen uitvoeringstermijnen) of de met de Klant afgesproken uitvoeringstermijn werd uitgevoerd.

De met de Klant afgesproken uitvoeringstermijn kan niet korter zijn dan de contractuele Service Level en dient gestaafd te kunnen worden door een akkoord van de betrokken Klant (bv. Een e-mail).

	Service Level (uitvoeringstermijn)

Wijzigingen m.b.t. gebruikersidentificatie: nieuwe gebruikersID's aanmaken, bestaande gebruikersID's wissen of wijzigen	4 uur
Verlenen/Wijzigen/Verwijderen van toegang tot een databankplatform of applicatieserver	1 Werkdag
Aanvragen van een databaseplatform met niet gedeeld OS/MW	5 Werkdagen
Aanvragen van een applicatieserver met niet gedeeld OS/MW	5 Werkdagen
Wijzigen storage en/of back-up capaciteit	1 Werkdag

Service Level

100 %.

Randvoorwaarden, assumpties en uitzonderingen

De uitvoering van dit Dienstenpakket gebeurt tijdens de Kantooruren.

Meetelementen en -methode

Voor elke Werkaanvraag wordt op de Service desk het tijdstip van indiening van de Werkaanvraag en het tijdstip van afsluiten geregistreerd. Indien de Werkaanvraag uit verschillende Diensten bestaat worden dezelfde gegevens per Dienst geregistreerd.

De registratie bestaat uit:

- Datum en uur van indiening de Werkaanvraag;
- Datum en uur van het einde van de uitvoering van alle activiteiten m.b.t. de Dienst;
- Datum en uur goedkeuring door de Klant van de Dienst/Werkaanvraag;

Mislukt een eerste poging om de Dienst succesvol uit te voeren, dan volgt hiervoor niet de goedkeuring door de Klant, maar een terugmelding door de Klant naar de Service desk zodat dit geregistreerd en opgevolgd kan worden. De uitvoering van de Dienst wordt pas afgesloten na succesvolle afwerking ervan en na expliciete goedkeuring door de Klant en na aanpassing van de gegevens in de Configuratiedatabank. Ingeval een terugmelding gebeurt, omdat de Klant niet tevreden is over de uitvoering (zowel op niveau van de Werkaanvraag als op het niveau van de Dienst), wordt de registratie als volgt aangevuld:

- Datum en uur van deze terugmelding;
- Datum en uur van het einde van de nieuwe acties;
- Datum en uur goedkeuring door de Klant;

De registratie herhaalt zich tot het moment dat de Klant zijn goedkeuring geeft.

Na goedkeuring door de Klant van de Dienst:

- Datum en uur afsluiten van Dienst/Werkaanvraag;

De volledige uitvoeringstermijn voor een Dienst wordt berekend als volgt:

- De looptijd tussen het tijdstip waarop de Dienst toekomt bij de Service desk (=datum van indiening) of het tijdstip dat de uitvoering kan starten (in het geval een afhankelijke Dienst besteld binnen dezelfde Werkaanvraag is uitgevoerd) en het tijdstip van het einde van de uitvoering van alle activiteiten van de Dienst volgens de DC-Dienstleverancier DC/Cloud ICT-Dienstverlener;
- Indien de interventie niet wordt goedgekeurd door de Klant en er bijgevolg een terugmelding gebeurt, wordt de uitvoeringstermijn vermeerderd met de tijd tussen begin- en eindtijd van elke bijkomende activiteit, totdat de Klant de Dienst heeft goedgekeurd.

Dit betekent dat de uitvoeringstermijn, die zal getoetst worden aan de Service Level, enkel de effectieve uitvoeringstermijn berekent tot de Dienst is afgesloten, en niet de tijd nodig voor goedkeuring door de Klant.

3.6.4.5.2 Tijdige uitvoering van Eenvoudige Werkaanvragen i.k.v. serverdiensten

Beschrijving en definitie

Per Dienst zal gemeten worden of deze Dienst binnen de contractuele Service level (zie in onderstaande tabel opgenomen uitvoeringstermijnen) of de met de Klant afgesproken uitvoeringstermijn werd uitgevoerd.De met de Klant afgesproken uitvoeringstermijn kan niet korter zijn dan de contractuele Service Level en dient gestaafd te kunnen worden door een akkoord van de betrokken Klant (bv. Een e-mail).

	Service Level(uitvoeringstermijn)
Wijzigingen mbt gebruikersidentificatie: nieuwe gebruikersID's aanmaken, bestaande gebruikersID's wissen of wijzigen	4 uur
Verlenen/Wijzigen/Verwijderen van toegang tot een server	1 Werkdag
Ter beschikking stellen en opzetten van een fysieke server	5 Werkdagen
Ter beschikking stellen en opzetten van een virtuele server	5 Werkdagen
Wijzigen van een virtuele server capaciteit	5 Werkdagen
Wijzigen storage capaciteit	5 Werkdagen
Stopzetten afname servercapaciteit (inclusief bijhorende storage en back-up)	5 Werkdagen
Stopzetten afname storage en/of back-up	5 Werkdagen
data restore op verzoek van de Klant van maximum 50 aparte files of 5 directories per aanvraag met behoud van de oorspronkelijke locatie	4 uur
data restore van een onbeperkt aantal files of directories met behoud van de oorspronkelijke locatie of voor een data restore uit de laatste back-up naar een andere locatie dan de oorspronkelijke	2 Werkdagen

data restore op verzoek van de Klant van een volledige server (exclusief OS)	2 Werkdagen
Toevoegen/wijzigen/verwijderen van configuraties op loadbalancers /WAF/next-gen FW	Einde volgende Werkdag
aanpassen van datastromen op de DC/Internet Firewall(s)	Einde volgende Werkdag

Service Level

100 %.

Randvoorwaarden, assumpties en uitzonderingen

Niet van toepassing.

3.6.4.5.3 Tijdige uitvoering van Eenvoudige Werkaanvragen netwerk en beveiliging

Beschrijving en definitie

Per Dienst zal gemeten worden of deze Dienst binnen de contractuele Service level (zie in onderstaande tabel opgenomen uitvoeringstermijnen) of de met de Klant afgesproken uitvoeringstermijn werd uitgevoerd.De met de Klant afgesproken uitvoeringstermijn kan niet korter zijn dan de contractuele Service Level en dient gestaafd te kunnen worden door een akkoord van de betrokken Klant (bv. Een e-mail).

	Service Level(uitvoeringstermijn)
Toevoegen/wijzigen/verwijderen van configuraties op loadbalancers /WAF/Next-gen FW	Einde volgende Werkdag
aanpassen van datastromen op de DC/Internet Firewall(s)	Einde volgende Werkdag

Service Level

100 %.

Randvoorwaarden, assumpties en uitzonderingen

Niet van toepassing.

3.6.4.6 Prijsmechanisme

- Een éénmalige prijs voor wijzigingen m.b.t. gebruikersidentificatie: nieuwe gebruikersID's aanmaken, bestaande gebruikersID's wissen of wijzigen;
- Een éénmalige prijs voor verlenen/wijzigen/verwijderen van toegang tot een databankplatform of applicatieserver;
- Een éénmalige prijs voor het aanvragen van een PAAS databaseplatform met niet gedeeld OS/MW;
- Een éénmalige prijs voor het aanvragen van een PAAS applicatieserver met niet gedeeld OS/MW;
- Een éénmalige prijs voor het wijzigen van storage en/of back-up capaciteit;

- Een éénmalige prijs voor wijzigingen m.b.t. gebruikersidentificatie: nieuwe gebruikersID's aanmaken, bestaande gebruikersID's wissen of wijzigen;
- Een éénmalige prijs voor het verlenen/wijzigen/verwijderen van toegang tot een server;
- Een éénmalige prijs voor het ter beschikking stellen en opzetten van een fysieke server
- Een éénmalige prijs voor het ter beschikking stellen en opzetten van een virtuele server
- Een éénmalige prijs voor het wijzigen van een virtuele server capaciteit
- Een éénmalige prijs voor het wijzigen van storage capaciteit
- Een éénmalige prijs voor het stopzetten afname servercapaciteit inclusief bijhorende storage en back-up
- Een éénmalige prijs voor het stopzetten afname storage en/of back-up
- Een eenheidsprijs voor het uitvoeren van een data restore van maximum 50 aparte files of 5 directories per aanvraag met behoud van de oorspronkelijke locatie
- Een prijs per server voor het uitvoeren van een data restore van een volledige server
- Een prijs per uur voor het uitvoeren van een data restore van een onbeperkt aantal files of directories met behoud van de oorspronkelijke locatie of voor een data restore uit de laatste back-up naar een andere locatie dan de oorspronkelijke
- Een éénmalige prijs voor het Toevoegen/wijzigen/verwijderen van configuraties op loadbalancers /WAF/Next-gen FW
- Een éénmalige prijs voor het aanpassen van datastromen op de DC/Internet Firewall(s)

3.6.4.7 Facturatie

De factuur bevat de in de afgelopen maand afgesloten en door de Klant geaccepteerde eenvoudige werkaanvragen.

4 Datacenter Outsourcing

4.1 Omschrijving

Datacenter Outsourcing betreft het beheren van datacenters van de VO-entiteiten :

- VO-eigen DC-infrastructuur gehuisvest in (voornamelijk bestaande) VO-eigen datacenters. Het gaat ondermeer over de datacenter diensten voor netwerk-functies van Perceel 4. In november 2020 zijn deze sites NMC4 (Colt Nossegem) en DR Antwerpen (datacenter VVC Antwerpen). Door de uitfasering van NMC4 datacenter zijn vanaf midden 2021 Conscience en DR Antwerpen de twee centrale datacenters
    - Bemerk dat datacenter NMC-4 in de loop van de eerste helft van 2021 zal uitgefaseerd worden; De applicaties die daar gehost werden, worden ondergebracht in VPC-Mechelen of public cloud; De netwerkfuncties die gehost werden in NMC4 worden gemigeerd naar Conscience computerzaal (CON);
- DC-infrastructuur van Klanten die in de loop van de Overeenkomst instappen (onboardings)

Binnen DC outsourcing zullen in eerste instantie geen bijkomende vereisten worden opgelegd dan het overnemen en beheren van de huidige situatie. De graad van automatisatie zal zich dan ook beperken tot wat tot op heden effectief werd ingericht en in gebruik is.

De dienstverlening mbt de exploitatie en de benodigde werkingsprocessen hebben over het algemeen de karakteristieken van een ‘traditioneel DC’. De Operationele verwachtingen liggen grotendeels in lijn met wat gevraagd wordt voor het managed DC.

Bij een DC outsourcing is de DC/Cloud ICT-Dienstverlener geen ‘Design Autoriteit’.

Er dient ook een traditionele dienstverlening voorzien te worden, waarbij Klanten nog hun eigen infrastructuur en eventueel daarop draaiende OS/middleware en de door deze servers gebruikte bestaande storage en back-up kunnen laten beheren door de DC/Cloud ICT-Dienstverlener. Er wordt een onderscheid gemaakt tussen

- bij de start van de overeenkomst bestaande VO-infrastructuur
- infrastructuur van Klanten die tijdens de looptijd van het contract instappen.

Het NMC4 datacenter zal uitgefaseerd worden uiterlijk 31 augustus 2021 (voor meer info zie ook referentiebibliotheek “ICT-Contract 2022 – Referentiebibliotheek – Datacenter en Computerzaalfaciliteiten/CZaaS”)

De DC/Cloud ICT-Dienstverlener dient deze infrastructuur verder te beheren bij de start van de overeenkomst (en in een eerste fase bij onboarding van nieuwe klanten). Voor de infrastructuur die onderliggend is aan beheerde toepassingen, verzorgt de ICT-dienstverlener bovendien ook de nodige afstemming en ondersteuning aan de betrokken applicatiedienstverlener.

4.2 Meerwaarden voor de Klanten

- Uitbesteding van het beheer, verlaging van de administratieve lasten

- Uitbesteding van het beheer van de onderliggende (onderhouds)contracten met onderaannemers/leveranciers
- Uitbesteding van licentiebeheer
- Garanties op kwaliteit (beschikbaarheid, performantie, beveiliging) en mogelijkheid tot differentiatie (o.a. in SLA's); garanties op beschikbaarheid ondersteund door afdwingbare Service Level eisen;
- Voor wat betreft het 'DC-outsourcing' zijn de te beheren items beperkt en gekend waarbij er wel een duidelijk afgebakende lijst van componenten kan worden opgemaakt.
- Transparante prijsstructuur in functie van de afnames en de evolutie in de tijd
- Mechanismen voor samenwerking met andere diensten (service interfaces)
- Een performante monitoring van de beheerde omgevingen en een efficiënte behandeling van eventuele incidenten en problemen.
- Innovatie: van de dienstverlener wordt verwacht dat hij voorstellen doet ter verbetering van de dienstverlening en dat hij hierbij actief op zoek gaat naar mogelijkheden om innovatieve oplossingen te incorporeren in de dienstverlening.

4.3 Specifieke kenmerken

Van de DC/Cloud ICT-Dienstverlener wordt verwacht dat hij de bestaande kenmerken – zoals beschreven/opgelijst in de AS-IS referentiebibliotheek overneemt en operationeel ondersteunt.

4.4 Overzicht van de DC Outsourcing

4.4.1 Exploitatie

4.4.1.1 Scope en doel

DC Outsourcing kan alle Diensten omvatten m.b.t. het ter beschikking houden en beheren van DC infrastructuur van Klanten en DC infrastructuur die door de vorige ICT-Dienstverlener wordt gebruikt voor toepassingen van Klanten. In de meeste gevallen zal dit handelen over de volgende domeinen:

- Beheer van verwerkingscapaciteit (op fysieke en virtuele servers),
- Beheer van opslagcapaciteit en backup
- Beheer van computerzaalfaciliteiten (IT gedeelte) (zie hoofdstuk 5 computerzaalfaciliteiten).

De exacte activiteiten zullen per DC-outsourcing project worden vastgelegd in een RASCI matrix. Een niet limitatieve lijst van mogelijke activiteiten die bijvoorbeeld kunnen gevraagd worden:

- Validatie storage-componenten bij operationele problemen met Storage-gekoppelde servers
- Extra storage toekennen bij operationele kruip-groei
- Performance management van de centrale omgeving
- Dagelijkse controle van de storage componenten op fouten

- Dagelijkse controle van de storage-switches op fouten
- Uitvoeren van, of assisteren bij firmware-upgrades + coördinatie naar systeembeheer.
- LUNs herlocaliseren (data move)
- Opvolgen van hardware incidenten
- Initiëren van changes en afstemmen bij interventies met impact (bv herstart storage processoren)
- Opvolgen van SW versies (Technology Policy, Product Life Cycle)
- Snapshots
- Controles en onderhoud van mirrorview (indien van toepassing)
- Opvolgen van de back-up op de back-up server (contact op nemen met Systeem beheerders in geval van fouten)
- Instructies voorbereiden en geven voor de "Wekelijkse tape wissel"
- In de robot geladen tapes labelen en toewijzen aan back-up groepen
- Dagelijks beschikbare versus vereiste "Tape volume" controleren
- Dagelijks beschikbare versus vereiste hoeveelheid controleren en bijsturen
- Beheer van Back-up Pools om de back-up windows te kunnen garanderen
- Opvolgen van het cloning proces
- Support verlenen voor restores
    - Instructies naar CFZ voor manuele tape loads in de Tape robot indien de data niet meer beschikbaar is online
    - Vrij maken van een correct tape drive (als het cloning proces nog bezig is)
- CZF aansturen voor manuele acties tgv incidenten of restores
- Oplossen van back-up/restore incidenten in relatie tot de back-up omgeving
- Incidenten in relatie tot het back-up platform, loggen en opvolgen bij de vendor
- Nodige tapewissels
- Off-site bewaren van tapes
- Ondersteuning bij hardware interventies
- Onderhoudscontracten voor alle storage en back-up gerelateerde componenten.
- Storage en Back-up gerelateerde licenties voor zowel de centrale als afzonderlijke componenten

In “DC outsourcing” zullen alle exploitatie diensten die betrekking hebben op Netwerk of Netwerk beveiliging voor rekening zijn van de Netwerk Leverancier (contract Netwerken).

Voor het beheer van de eigen infrastructuur van de Klanten en eventueel daarop draaiende middleware en de bijhorende (onderhouds-)contracten worden de concrete modaliteiten afgesproken in een exploitatiedossier per Klant.

4.4.1.2 Geconcretiseerd door

Dezelfde werkwijze zal hier worden gehanteerd als het managed DC.

4.4.1.3 SLA

SLA’s zullen op dezelfde wijze worden geformaliseerd als het managed DC.

4.4.1.4 Prijsmechanisme

Voor wat betreft de Exploitatie van bij de start van de overeenkomst aanwezige infrastructuur van de Klant:

Beheer van FYS server	DC Outsourcing	24/7	ander
Beheer van FYS server	DC Outsourcing	24/7	LINUX
Beheer van FYS server	DC Outsourcing	24/7	UNIX
Beheer van FYS server	DC Outsourcing	24/7	Windows
Beheer van Vserver	DC Outsourcing	24/7	UNIX
Beheer van Vserver	DC Outsourcing	24/7	LINUX
Beheer van Vserver	DC Outsourcing	24/7	Windows
Beheer van FYS server	DC Outsourcing	UKT	LINUX
Beheer van FYS server	DC Outsourcing	UKT	UNIX
Beheer van FYS server	DC Outsourcing	UKT	Windows
Beheer van Vserver	DC Outsourcing	UKT	LINUX
Beheer van Vserver	DC Outsourcing	UKT	UNIX
Beheer van Vserver	DC Outsourcing	UKT	Windows
Beheer van een ESX host	DC Outsourcing	UKT	nvt
Beheer van een Oracle Enterprise Edition database	DC Outsourcing	UKT	nvt
Beheer van een niet-Oracle Enterprise Edition database	DC Outsourcing	UKT	nvt
Beheer van een applicatie server	DC Outsourcing	UKT	nvt
Beheer van storage	DC Outsourcing	UKT	nvt
Beheer backup	DC Outsourcing	UKT	nvt
beheer storage en back-up capaciteit gerelateerd aan de van bij de start van de overeenkomst bestaande fysieke en virtuele servers met gebruik van de gemeenschappelijke infrastructuur	DC Outsourcing	UKT	nvt
Beheer storage en back-up servers gerelateerd aan de bestaande fysieke en virtuele servers met dedicated storage en back-up infrastructuur.	DC Outsourcing	UKT	nvt

- Een eenheidsprijs per uur voor tape handling
- Prijzen voor de VO-specifieke contracten die nodig zijn voor de te beheren server instanties
  Het betreft hier de in de VO-specifieke contracten afgesproken Eenheidsprijzen. Voor VO-specifieke contracten die gebruikt worden voor meerdere Klanten, wordt een zo correct mogelijke versleuteling gebruikt

Voor wat betreft de Exploitatie van bij de start van de overeenkomst bestaande toepassingsondersteunende infrastructuur van de vorige ICT-Dienstverlener in VPC:

- Een eenheidsprijs per maand en per toepassing voor het beschikbaar houden van bij de start van de overeenkomst bestaande toepassingsondersteunende infrastructuur in VPC, inclusief het beheer van de onderliggende computerzaal

- Prijzen voor de VO-specifieke contracten die nodig zijn voor de te beheren toepassingsondersteunende infrastructuur
  Het betreft hier de in de VO-specifieke contracten afgesproken Eenheidsprijzen. Voor VO-specifieke contracten die gebruikt worden voor meerdere Klanten, wordt een zo correct mogelijke versleuteling gebruikt

Voor wat betreft de Exploitatie van infrastructuur van de Klant die tijdens de looptijd van de overeenkomst instapt:

- Een forfaitaire eenheidsprijs per maand en per virtuele server unix/linux met standaard OS (Red Hat, Solaris).
- Een forfaitaire eenheidsprijs per maand en per fysieke server unix/linux met standaard OS (Red Hat, Solaris).
- Een forfaitaire eenheidsprijs per maand en per virtuele server unix/linux met non-standaard OS.
- Een forfaitaire eenheidsprijs per maand en per fysieke server unix/linux met non-standaard OS.
- Een forfaitaire eenheidsprijs per maand en per virtuele server met Windows OS.
- Een forfaitaire eenheidsprijs per maand en per fysieke server met Windows OS.
- Een forfaitaire eenheidsprijs per maand en per ESX host.
- Een forfaitaire eenheidsprijs per maand en per instance voor het beschikbaar houden van een Oracle Enterprise Edition database.
- Een forfaitaire eenheidsprijs per maand en per instance voor het beschikbaar houden van een niet-Oracle Enterprise Edition database.
- Een forfaitaire eenheidsprijs per maand en per instance voor het beschikbaar houden van een applicatie server.
- Een forfaitaire eenheidsprijs per maand voor storage beheer (per Gb)
- Een forfaitaire eenheidsprijs per maand voor backup beheer (per Gb processed)
- Prijzen voor de VO-specifieke contracten die nodig zijn voor de te beheren serverinstanties.
  Het betreft hier de in de VO-specifieke contracten afgesproken Eenheidsprijzen. Voor VO-specifieke contracten die gebruikt worden voor meerdere Klanten, wordt een zo correct mogelijke versleuteling gebruikt.

4.4.2 Eenvoudige Werkaanvragen

Eenvoudige werkaanvragen voor DC outsourcing zullen op dezelfde wijze worden geformaliseerd als het managed DC.

5 Computerzaal Faciliteiten (CZF)

5.1 Omschrijving

Deze dienst omvat zowel het beheer van computerzalen in VO-gebouwen (rubriek 5.2.1 Beheer van computerzalen) als het beschikbaar stellen van professioneel beheerde computerzaalfaciliteiten (rubriek 5.2.2. Het beschikbaar stellen van professioneel beheerde computerzaalcapaciteit CZF (inclusief stroomverbruik en koeling).

Het Dienstenpakket voor beschikbaarstellen van professioneel beheerde computerzaalfaciliteit kan apart worden afgenomen door Klanten die hun eigen infrastructuur in een professioneel beheerde computerzaal van de DC/Cloud ICT-Dienstverlener willen plaatsen. Het betreft een housing dienst die bestaat uit gebouw, fysieke beveiliging, stroomvoorziening, koeling, kooi en racks. De locatie dient bij voorkeur gelijk te zijn aan die van de managed DC dienst, zodat connectiviteit naar Internet, VO MPLS, managed DC optimaal kan worden ingericht.

Voor disaster recovery wordt een tweede site met computerzaalfaciliteten voorzien. Bij de start van het contract is er nog geen behoefte voor een tweede site maar dit kan later via project worden toegevoegd.

De dienst moet kunnen afgenomen worden ‘as a service’, als een volledig rack of een aantal hoogte-eenheden in een rack in een professioneel beheerde computerzaal van de DC-Dienstleverancier. Hierbij moeten ook de nodige procedures afgesproken worden voor de toegankelijkheid van de infrastructuur van de betrokken Klant. Deze Dienst omvat gespecialiseerde ondersteuning inzake beheer van energiegebruik en koeling en zorgt ervoor dat de optimale fysieke beveiligingsmaatregelen getroffen worden. Binnen deze Dienst valt ook het onderhoud van de fysieke site en het voorzien van voldoende energie back-up (batterij en diesel generatoren), en brandblusinstallatie. In deze Dienst is ook het beheer van databekabeling en elektriciteitsaansluitingen en tape handling inbegrepen.

Beide diensten omvatten ook het opstellen en updaten van (fysieke) exploitatiedossiers en procedures voor gebruik van de computerzalen.

Bemerk: de dienst DC-Outsourcing.laat klanten toe om hun eigen infrastructuur in de CZF te plaatsen, en te laten beheren door de DC/Cloud dienstverlener.

5.2 Meerwaarden voor de Klanten

De dienstverlening voor beheer van computerzalen in VO gebouwen biedt Vlaamse overheid de mogelijkheid om computerzalen professioneel te laten beheren met betrekking tot het IT gedeelte.

Tape handling voor een VO site is een beschikbare dienstverlening (cf. refbib document Datacenter en Computerzaalfaciliteiten C2022.

De dienstverlening voor ter beschikking stellen van een professioneel beheerde computerzaal is bedoeld voor Klanten die eigen fysieke apparatuur (servers, appliances …) wensen te behouden (om redenen die divers van aard zijn), maar niet meer wensen te investeren in eigen lokale computerzalen.

- Verlaging van de administratieve lasten voor het afnemen van CZF
- Schaalvoordelen op het vlak van prijs
- Uitbesteding van het beheer van de onderliggende (onderhouds)contracten met onderaannemers/leveranciers
- Voldoende capaciteit en flexibele uitbreidingsmogelijkheden
- Transparante prijsstructuur (per rack, per hoogte-eenheid, …)
- Een monitoring van de beheerde omgevingen (elektrische storingen, water, rook/brand, ..)
- Het Facilitair Bedrijf wil het gebruik van compacte datacenters met een hoge energie-efficiëntie verder stimuleren zodat we meerwaarden kunnen realiseren op het vlak van kost en energie-efficiëntie.

5.2.1 Het beheren van computerzaalcapaciteit CZF

Deze dienst omvat volgende activiteiten en processen:

- Het beheer van een computerzaal van de VO, in een VO gebouw heeft, of betrekt via een ander contract; Deze computerzaal site ligt in het Vlaams gewest of het Brussel hoofdstedelijk gewest; Bij het inregelen van de dienstverlening wordt rekening gehouden met de geldende (veiligheids- en operationele) richtlijnen die van toepassing zijn voor het gebouw.
- Het IT beheer omvat databekabeling en patching (met inbegrip van patchings naar telecom rack, patching in meet me room in geval van aanwezigheid meet me room) met bijhorende labeling; beheer rackreservatie, afstemming met beheer van technische installaties, beheer van personen met toegang tot de computerzaal, elektrische aansluiting IT materiaal in samenwerking met beheerder technische installaties.
- Hands&Eyes;
- Beschermen van de computerzaalfaciliteiten tegen oneigenlijke toegang van buitenaf:
    - Het beheren van maatregelen inzake fysieke beveiliging van de externe computerzalen: de toegang tot de computerzaal gebeurt in principe op basis van VO toegangsbadge. De dienstverlener volgt op wie toegang heeft en voert een periodieke audit van de effectieve toegang (met eventueel de vereiste aanpassingen).
- Tape-handling is een dienstverlening die ook apart kan afgenomen worden, t.t.z. de tape handling dienst kan afgenomen worden zonder dat de computerzaal voor de desbetreffende site beheerd wordt door de ICT dienstverlener.

- Op basis van een werkaanvraag kan ook het benodigde materiaal voorzien voor beheer van de computerzaal (bv. databekabeling, rack en toebehoren,…)

Buiten bereik

- Het beheer van de technische installaties (HVAC, elektriciteit, brandbeveiliging, UPS, noodstroomgenerator, waterlekdetectie) is buiten bereik.
- Het stroomverbruik is buiten bereik, capactiteitsplanning voor stroomverbruik is wel in scope;

5.2.2 Het beschikbaar stellen van professioneel beheerde computerzaalcapaciteit CZF (inclusief stroomverbruik en koeling)

Deze dienst omvat volgende activiteiten en processen:

- Het ter beschikking stellen van een computerzaal (omgerekend naar een prijs per hoogte-eenheid/rack + werkelijk elektriciteitsverbruik) In de financiële bijlage vertegenwoordigd 1KW het daadwerkelijk beschikbaar vermogen in de computerzaal, de leverancier dient voor de kostprijsbepaling dit te verhogen met de gemiddelde PUE waarde voor het datacenter.
- Alle activiteiten die opgesomd worden bij “Het beheren van computerzaalcapaciteit CZF”
- De personen die toegang tot een computerzaal willen krijgen dienen de procedure voor de desbestreffende computerzaalfaciliteiten te volgen. Bv. dienen ze zich kenbaar te maken door middel van hun identiteitskaart en moeten op voorhand een autorisatiedocument ondertekenen. Indien het gaat over een geldige aanvraag zal er een toegangsbatch ter beschikking liggen bij de uitbater van de infrastructuur. Deze batch zal enkel overhandigd worden aan geautoriseerde personen in ruil voor hun identiteitskaart.

  Het Bestuur of een door het Bestuur bevoegd verklaarde instantie, behoudt het recht tot (onaangekondigde) toegang tot de computerzalen (bv. voor de controle op het naleven van het Algemeen Reglement voor. de Arbeidsbescherming). Daartoe zal het Bestuur aan de DC/Cloud ICT-Dienstverlener een lijst bezorgen van de personen aan wie toegang dient verschaft te worden. Enkel de personen op deze lijst aanwezig zijn geautoriseerd om toegang te verkrijgen tot de computerzalen.
- Een goed capaciteitsmanagement voor het geheel van de zaal wordt voorzien. De capaciteitsbehoefte van 2KW/m2 of 4KW/rack kan nodig zijn voor een individueel rack maar over de totale CZAAS zaal zal het gemiddeld lager zijn.
- De DC/Cloud ICT-Dienstverlener speelt in op wijzigingen in de zakelijke behoeften van VO (bv. bij uitbreiding of inkrimping, en andere wijzigingsverzoeken) en zorgt ervoor dat de technologie in de colocatieruimte en van alle componenten actueel gehouden wordt.
- Het beheer van de technische installaties (HVAC, elektriciteit, brandbeveiliging, UPS, noodstroomgenerator, waterlekdetectie) is in scope.
- Beheer van stroomverbruik, koeling, verzekering, huur, …

- Event Management: monitoring van de basisfaciliteiten van de computerzaalfaciliteiten;
    - deze basisfaciliteiten (zoals koeling, elektriciteit, brandbeveiliging) en de monitoring (detectie en alarmmelding) ervan vallen voor de computerzalen van de DC/Cloud ICT-Dienstverlener volledig onder zijn bevoegdheid.

5.2.2.1 Gevraagde kenmerken

De nodige technische aanpassingen zijn ten laste van de DC/Cloud ICT-Dienstverlener. Minimum moet in een beveiligde omgeving aan volgende vereisten voldaan worden:

- De onderhavige computerzalen voldoen minimaal aan de vereisten voor een tier III-datacenter volgens de tier-classificatie van Uptime Institute.
- Bij voorkeur ligt de CZF in de nabijheid van de sites van het Managed DC – zie beschrijving in 3.3.1.2 Vereisten datacenter;
- Een geografisch redundante verbinding met met het backbone netwerk van de VO is vereist (inbegrepen in de prijs);
    - Bij voorkeur kan gebruik gemaakt wordeen van de redundante verbinding met met het backbone netwerk van de VO die voorzien is voor het Managed DC – zie beschrijving in 3.3.1.3 Vereisten netwerk connectiviteit
- Er is een netwerk verbinding voorzien met het Managed DC; Bij voorkeur heeft deze verbinding een bandbreedte van minimaal 10 Gbps en een lage latency van 2 ms;
- Er dient Ethernet Layer-2 connectiviteit voorzien te worden vanuit het managed DC naar de CZF infrastructuur. Er zal mbt het onderliggende netwerk bij voorkeur dus geen onderscheid gemaakt worden tussen managed DC en CZF qua mogelijkheden, beschikbare bandbreedtes en toegangspoorten. Het is niet de bedoeling om een apart netwerk op te bouwen voor CZF.
- De jaarlijks gemiddelde energie efficiëntie waarde (Power usage effectiveness (PUE™) bedraagt maximaal 1,6.
- De capaciteit van de aangeboden computerzaaldienst bedraagt minimaal 2kW/m2 of 4kW/rack
- De computerzaalbeheerders volgen de goede werking van de computerzalen op in 24/7/365 regime. (24/7/365 werking zonder onderbreking)
- Air-conditioning die een constante omgevingstemperatuur waarborgt en een relatieve vochtigheidsgraad garandeert zodanig dat de apparatuur geen schade wordt toegebracht en in optimale condities kan functioneren.
- UPS voorzieningen die voldoende continuïteit verzekeren zodoende dat er genoeg tijd is om de back-up generators in werking te laten treden.
- De stroomvoorziening van het gehele datacenter betrokken wordt door middel van twee gescheiden en apart geroute circuits naar de lokale elektriciteitsleverancier.
- Een brand detectie systeem dat uitgevoerd is met waarschuwingssystemen en met optische, thermische of ionische rookdetectors. Tevens moeten de normale brandbeveiligingsfaciliteiten zoals onder andere brandblussers aanwezig zijn.
- Een toegangscontrolesysteem dat enkel toegang verschaft aan geautoriseerd personeel.
- Een monitoringsysteem voor elektrische en mechanische storingen en aanwezigheidsdetectie van of water.
- Beveiligingsbeheer mbt computerzalen.
- Redundante verbinding met met het backbone netwerk van de VO (inbegrepen in de prijs)

5.3 Overzicht van de CZF

5.3.1 Exploitatie beheer van computerzalen

5.3.1.1 Scope en doel

Zie voorgaande paragrafen

5.3.1.2 Geconcretiseerd door

Het beheren van computerzaalcapaciteit CZF

- Per site
- En het aantal racks

Tape handling kan als aparte dienst afgenomen worden

SLA – beheer van computerzaal in VO

Beschrijving en definitie

De beschikbaarheid van de computerzaalfaciliteiten en de geleverde diensten zoals fysieke beveiliging, hands&eyes, en exclusief HVAC, elektriciteit, brandbeveiliging, UPS, noodstroomgenerator, waterlekdetectie);

Voor beheer van computerzaal dient de dienstverlener:

- de nodige documentatie te voorzien

- de nodige afspraken te maken met gerelateerde diensten (bv. beheerder technische installaties)

- 6 maandelijks audit toegangscontrole

Service Level

De computerzaalfaciliteiten dienen 99,99% beschikbaar te zijn.

Beschikbaarheidgraad van de technische installatie is niet inbegrepen in de SLA, het betreft enkel het IT-beheer.

Randvoorwaarden, assumpties en uitzonderingen

Enkel specifieke gevallen van overmacht die in overleg tussen de DC/Cloud ICT-Dienstverlener en de Klant worden erkend vallen buiten beheer van de DC/Cloud ICT-Dienstverlener en mogen bijgevolg uitgefilterd worden voor de end to end SLA.

Meetelementen en –methode

Beschikbaarheid van de computerzaal, documentatie, rapportering 6 maandelijkse audit toegang

.

5.3.1.3 Prijsmechanisme - Het beheren van computerzaalcapaciteit CZF

De prijs bestaat uit :

- Een maandelijkse prijs per Klant en per site
  - Berekend op het totaal van alle CZF sites per klant
- Een maandelijkse prijs per Klant per rack
  - Berekend op het totaal van alle racks per klant
- (aparte) prijs voor tape-handling

5.3.1.4 Facturatie

Maandelijks wordt de factuur overgemaakt aan de Klant die de bestelling heeft geplaatst. Deze factuur bevat:

- Het totaal voor het beheren van de computerzaalfaciliteit as a service (aantal sites en racks voor de betrokken Klant;
- En/of de prijs voor tape-handling

5.3.2 Exploitatie ter beschikking stellen van professioneel beheerde computerzalen

5.3.2.1 Scope en doel

Zie voorgaande paragrafen.

5.3.2.2 Geconcretiseerd door

Het beschikbaar stellen van professioneel beheerde computerzaalcapaciteit CZF (inclusief stroomverbruik en koeling)

- Het aantal hoogte-eenheden; Een rack is 42 hoogte-eenheden;
- Elektriciteitsverbruik per KWH per maand
- (eventuele) tapehandling

5.3.2.3 SLA - Het beschikbaar stellen van professioneel beheerde computerzaalcapaciteit CZF (inclusief stroomverbruik en koeling)

Beschrijving en definitie

De beschikbaarheid van de computerzaalfaciliteiten (incl HVAC, elektriciteit, brandbeveiliging, UPS, noodstroomgenerator, waterlekdetectie);

Service Level

De computerzaalfaciliteiten dienen 99,99% beschikbaar te zijn.

In de maximale onbeschikbaarheidsduur zijn alle onderbrekingen inbegrepen die noodzakelijk zijn voor het organiseren van een goede ICT-Dienstverlening zoals onderhoudswerken op basisvoorzieningen, shutdowns,…

Randvoorwaarden, assumpties en uitzonderingen

Enkel specifieke gevallen van overmacht die in overleg tussen de DC/Cloud ICT-Dienstverlener en de Klant worden erkend vallen buiten beheer van de DC/Cloud ICT-Dienstverlener en mogen bijgevolg uitgefilterd worden voor de end to end SLA.

Meetelementen en –methode

De beschikbaarheid van de computerzaalfaciliteiten wordt gemeten op basis van metingen met een monitoring systeem.

5.3.2.4 Prijsmechanisme - Het beschikbaar stellen van professioneel beheerde computerzaalcapaciteit CZF (inclusief stroomverbruik en koeling)

De prijs bestaat uit :

- Een maandelijkse prijs per Klant en per hoogte-eenheid voor het gebruik van de beheerde computerzaalruimte (incl. alle infrastructuur voor koeling, noodstroomvoorziening, racks, …., verzekering, huur, en alle dienstverlening, en excl stroomverbruik)
    - Een rack is 42 hoogte-eenheden;
- Een aparte prijs voor het stroomverbruik in KWH per maand, per Klant;
    - Het stroomverbruik wordt gemeten aan het rack, en het stroomverbruik van koeling enz… wordt verrekend door dit stroomverbruik te vermenigvuldigen met de PUE factor;

5.3.2.5 Facturatie- Het beschikbaar stellen van professioneel beheerde computerzaalcapaciteit CZF (inclusief stroomverbruik en koeling)

Maandelijks wordt de factuur overgemaakt aan de Klant die de bestelling heeft geplaatst. Deze factuur bevat:

- Het totaal voor het beschikbaar houden van de computerzaalfaciliteit as a service (aantal hoogte eenheden voor de betrokken Klant;
- En/of de prijs voor tape-handling

5.3.3 Eenvoudige Werkaanvragen computerzaalfaciliteiten

5.3.3.1 Aanvraag voor ter beschikking stellen, wijzigen, opzeggen van computerzaalruimte

Via deze Werkaanvraag kan aan de DC/Cloud ICT-Dienstverlener computerzaalruimte aangevraagd, gewijzigd of stopgezet worden.

5.3.3.2 Aanvraag voor het afnemen/opzeggen van doorpatching naar een telecom rack

De Klant die Computerzaalruimte as a service afneemt, kan per ICT-component, kiezen voor de optie van een doorpatching naar het telecommunicatierack van zijn ISP. De telecom racks bevinden zich doorgaans in de “meet-me rooms” van het datacenter.

Via deze Werkaanvraag kan aan de DC/Cloud ICT-Dienstverlener gevraagd worden om een doorpatching uit te voeren naar een telecom rack.

De klant dient verder zelf nog de nodige afspraken te maken met zijn telecom partner om connectiviteit met het datacenter van de DC/Cloud ICT-Dienstverlener te bekomen

5.3.3.3 Geconcretiseerd door

- Identificatiegegevens van de Klant die instaat voor betalingen met betrekking tot de betrokken dienst;
- Het aantal hoogte-eenheden

5.3.3.4 SLA

5.3.3.4.1 Tijdige uitvoering van Werkaanvragen i.k.v. computerzaalfaciliteiten

Beschrijving en definitie

Per Dienst zal gemeten worden of deze Dienst binnen de contractuele Service level (zie in onderstaande tabel opgenomen uitvoeringstermijnen) of de met de Klant afgesproken uitvoeringstermijn werd uitgevoerd.

De met de Klant afgesproken uitvoeringstermijn kan niet korter zijn dan de contractuele Service Level en dient gestaafd te kunnen worden door een akkoord van de betrokken Klant (bv. Een e-mail).

	Service Level(uitvoeringstermijn)
Aanvraag voor het ter beschikking stellen, wijzigen, opzeggen van computerzaalruimte	Afgesproken termijn

Service Level

100 %.

Randvoorwaarden, assumpties en uitzonderingen

Niet van toepassing.

5.3.3.5 Prijsmechanisme

- Een prijs per ICT-component voor het ter beschikking stellen, wijzigen, opzeggen van computerzaalruimte
- Een prijs per ICT-component voor het afnemen/opzeggen van doorpatching naar een telecom rack /telecom lokaal (toegang naar VO backbone, Managed DC, Netwerk/ISP van Klant …)

5.3.3.6 Facturatie

De factuur bevat de in de afgelopen maand afgesloten en door de Klant geaccepteerde eenvoudige werkaanvragen.

6 Ondersteuning in regie m.b.t. Cloud- en Datacenterdiensten

6.1 Scope en doel

Naast de recurrente taken die nodig zijn voor de exploitatie van deze dienst kan, in functie van de in een exploitatiedossier met de Klant gemaakte afspraken, ook het uitvoeren van ad hoc taken deel uitmaken van deze dienst. Op vraag van de Klant kan samen met de Service Delivery Manager een prognose opgesteld worden van dergelijke kleine aanpassingen die verwacht worden in het komende jaar. Op basis van deze prognose kunnen in de loop van het jaar, opdrachten gegeven worden door de door de betrokken Klant hiertoe aangewezen personen, om kleine aanpassingen in middelenverbintenis uit te voeren.

Het kan over alle wijzigingen gaan waarvoor het niet mogelijk of niet efficiënt zou zijn om dit te realiseren via het Dienstenpakket Infrastructuurprojecten m.b.t. Cloud- en Datacenterdiensten of via Eenvoudige Werkaanvragen.

De raming van het aantal te voorziene VTE's per profiel voor het uitvoeren van deze ad hoc taken en de afspraken m.b.t. de wijze waarop dergelijke opdrachten worden gegeven worden op voorhand gedocumenteerd in een exploitatiedossier.

De DC/Cloud ICT-Dienstverlener richt de nodige processen, procedures in om dit soort aanvragen snel en vlot te laten verlopen. Indien hiervoor een ondersteunende tool nodig is wordt die ook door de DC/Cloud ICT-Dienstverlener ter beschikking gesteld. M.b.t. de opvolging van deze opdrachten en de eraan gekoppelde taken is er een volledige transparantie voor de klant op basis van een meekijkfunctionaliteit in de ondersteunende tool.

Ikv clouddiensten is een een ondersteuning door een Technical Accountmanager (TAM) van de cloud provider inbegrepen in de dienst, er wordt standaard echter geen lokale Nederlandstalige SDM-functie gevraagd. In regie kan wel een lokale Nederlandstalige SDM ondersteuning gevraagd wordenRegieprestaties voor bv. opzet van automatisatie en Cloudops beheer kunnen onsite of offsite uitgevoerd worden; ze steunen:

- enerzijds op cloud specialisten met de nodige certifiëring en ervaring
- anderzijds op door het bedrijf aangeleverde template scripts, referentie architecturen en bouwstenen;
- de leverancier voorziet voldoende lokale resources die kunnen ingeschakeld worden in een on-site devops team;

6.2 Geconcretiseerd door

De opdrachten voor "Ondersteuning in regie" in het kader van de Cloud- en Datacenterdiensten worden geconcretiseerd door:

- Identificatiegegevens van de Klant (naam, entiteit, telefoonnummer);
- Een duidelijke omschrijving van de opdracht en uit te voeren taken.

6.3 Prijsmechanisme

De prijzen voor de prestaties voor kleine aanpassingen via “Onderstening in regie m.b.t. de Cloud- en Datacenterdiensten worden bepaald op basis van de geldende Eenheidsprijzen van de betrokken Profielen die ingezet worden voor het uitvoeren ervan. Deze Eenheidsprijzen zijn opgenomen in de Profielencatalogus Cloud- en Datacenterdiensten

6.4 Facturatie

De facturatie gebeurt maandelijks en de factuur bevat:

- Het totaal van de prestaties m.b.t. de kleine aanpassingen op basis van de door de Klant goedgekeurde prestatieregisters.

6.5 Rapportering

Maandelijks rapport m.b.t. de prestaties uitgevoerd in de betrokken maand gekoppeld aan de unieke identificatie van de opdracht waarin de prestaties kaderen.

7 Infrastructuurprojecten m.b.t. Cloud- en Datacenterdiensten

7.1 Scope en doel

Grotere wijzigingen aan de dienstverlening m.b.t. de Cloud- en Datacenterdiensten of aan de hiervoor gebruikte omgevingen dienen projectmatig aangepakt te worden. Het kan gaan om alle wijzigingen, studies, aanvullingen die niet via de éénmalige diensten via een Werkaanvraag of via een ondersteuning in regie kunnen uitgevoerd worden. De Projecten kunnen betrekking hebben op infrastructuur- en platformdiensten of kunnen onderdeel zijn van een globaal Project dat ruimer kadert dan de dienstverlening in deze Service Portfolio. In dit laatste geval zal de DC/Cloud ICT-Dienstverlener moeten samenwerken met andere DC/Cloud ICT-Dienstverleners obv de afspraken die opgenomen worden in het Projectvoorstel.

Het doel van dit Dienstenpakket is het uitvoeren van alle nodige activiteiten om een Project te realiseren. Het rapporteren, het geven van feedback aan de projectleider van de Klant aangaande de voortgang van het Project en alle niet nader opgesomde maar normaal geachte projectactiviteiten maken eveneens deel uit van de scope van dit Dienstenpakket.

Alle Projecten moeten uitgevoerd worden conform de beschrijving van het proces Projectmanagement in het document “Vereisten ondersteunende processen en overlegfora”.

Deze Dienst wordt geïnitieerd via het indienen van een Werkaanvraag voor het opmaken van een Projectvoorstel en eindigt bij de Oplevering (via een PV van Oplevering), facturatie en betaling door de Klant van de laatste projectfase.

Er kunnen een aantal veel voorkomende types van Projecten onderkend worden waarvoor de te doorlopen fasen en de op te leveren specifieke Werkproducten vooraf kunnen bepaald worden.

Hierna volgt een mogelijke niet limitatieve lijst van dergelijke projecttypes:

- Het realiseren van een nieuwe infrastructuuromgeving: Het einddoel is het beschikbaar stellen van een nieuwe infrastructuuromgeving die operationeel is en aan de noden van de Klant voldoet;
- Het aanpassen van een bestaande infrastructuuromgeving: Het einddoel is een gewijzigde infrastructuur die operationeel is en aan de gewijzigde behoeften van de Klant voldoet. Hiertoe behoort eveneens het aanpassen van de actuele infrastructuur naar aanleiding van structurele veranderingen als gevolg van onvoorzienbare omstandigheden of als gevolg van veranderingen in de technologie markt. Deze Projecten kunnen ook betrekking hebben op optimalisatie en automatisatie van de infrastructuuromgeving;
- Het overnemen en/of integreren en of overdragen/isoleren van een bestaande infrastructuuromgeving. Dit betreft bijvoorbeeld de onboarding van nieuwe Klanten;
- Het projectmatig stopzetten van exploitatiediensten waarvoor er geen expliciete omschrijving is opgenomen in de Service Portfolio.
- Het opzetten van automatisatie ikv Cloudops beheer : ontwikkeling van automatiseringsscripts m.b.t. infrastructuur opzet (“infrastructure as code”) en inzake cloud operations (operationele activiteiten die zich herhalen, automatiseren), in de cloud technologie en automatiserings technologie die de klant toepast;

- Het initiëren of verlengen van VO-specifieke contracten. Voor wat het verlengen betreft gaat het om verlengingen waarbij er significante wijzigingen zijn van het voorwerp of verhoging van de prijs. Andere verlengingen gebeuren conform de bepalingen in het document Vereisten Ondersteunende Processen en Overlegfora hoofdstuk 3.32."

7.2 Geconcretiseerd door

Een Project zal in principe steeds starten met een Werkaanvraag voor het opmaken van een Projectvoorstel. Nadien volgen dan een of meerdere Werkaanvragen voor de bestelling van opeenvolgende fasen (overeenkomstig de offerte) of voor het bestellen van wijzigingen.

De Klant dient in zijn Werkaanvraag voor de opmaak van een Projectvoorstel steeds de volgende elementen op te nemen:

- De identificatiegegevens van de Klant: de organisatorische eenheid en de naam van de persoon die voor dit Project bevoegd is om beslissingen te nemen voor de Klant (projectleider van de Klant) en die dus o.a. de PV van Oplevering zal tekenen. ;
- De omschrijving van de huidige situatie, duiden van de huidige problematiek;
- De omschrijving van de gewenste situatie: geven van een visie van waar men naartoe wil en omschrijving van wat men wil bereiken (doelstellingen);
- De precisering van de gewenste Werkproducten;
- De functionele vereisten: beschrijving van de functionaliteiten die verwacht worden van het te realiseren systeem;
- De niet-functionele vereisten: Beschrijving van niet-functionele eisen waaraan het systeem moet voldoen (bijvoorbeeld flexibiliteit, documentatie, uitbreidbaarheid, capaciteit, interfaces, performantie, aanduiding van specifieke SLA, beschikbaarheid, , veiligheidsvereisten (o.a. m.b.t. persoonsgegevens), ...);
- Eventuele locatie-vereisten. In het bijzonder indien de Klant eist dat alle of bepaalde activiteiten op een locatie bij de Klant moeten worden uitgevoerd.
- De aard van de verbintenis: resultaatsverbintenis of middelenverbintenis
- De bijlagen: een lijst van documenten, die als bijlage (of via een referentie (link) naar een elektronische versie in een daarvoor geëigend systeem dat voor alle voor alle partijen toegankelijk is) zijn opgenomen (bijvoorbeeld bestaande installatiedossier, exploitatiedossier, broncodes,…).

De volledigheid en de mate van detail waarin bovenstaande elementen beschreven dienen te worden, is afhankelijk van het type Project en van het feit of het om een nieuwe infrastructuur/toepassing gaat dan wel om een aanpassing aan de bestaande ICT-infrastructuur/toepassing.

In de Werkaanvragen voor de bestelling van de uitvoering van de Project of Projectfase moet verwezen worden naar het betrokken Projectvoorstel.

In een Werkaanvraag voor de bestelling van een projectwijziging, verwijst de Klant naar:

- Het bestelde Project waarop de wijziging betrekking heeft
- Een vooraf opgesteld wijzigingsvoorstel, dat werd opgesteld als onderdeel van wijzigingsbeheer in de projectuitvoering, en dat het doel, het bereik en de impact van de wijziging op alle projectaspecten (planning, scope, kosten, …) helder beschrijft.

7.3 Uitvoering

7.3.1 Werkaanvraag voor opmaken van een Projectvoorstel

Om een Project te kunnen uitvoeren moet voorafgaand een Projectvoorstel bij de ICT-Dienstverlener gevraagd worden.

Inhoud

Een Projectvoorstel geeft o.a. aan tegen welke prijs en met welke doorlooptijd de dienstverlener een Project of specifieke projectdelen van een Project dient uit te voeren. Het Projectvoorstel omvat minstens een projectplan met o.a. een duidelijke omschrijving van het bereik, de te bekomen projectresultaten of op te leveren producten (in de zin van Prince-2), de planning (bijv. GANTT) en de prijs.

De aspecten scope, tijd en kost komen expliciet aan bod, en worden in een consistente verhouding tot elkaar opgenomen in het projectvoorstel, conform aan de vooropgestelde projectmethodiek.

Aanpak van de offerteopmaak

De dienstverlener bereidt een professionele offerte voor die een geschikt antwoord biedt op de geformuleerde werkaanvraag. Waar nodig of waar expliciet als werkwijze voorzien en gevraagd, wordt er afgestemd met de klant:

- Meestal zal in de opmaakfase een afstemmingsgesprek met de Klant gebeuren, om de verwachtingen en vereisten scherp te stellen en toe te laten een correct projectvoorstel neer te leggen dat daarmee maximaal overeenstemt.
- Eventueel wordt afgesproken om tijdens offerteopmaak een preliminaire voorstelling te doen van de oplossing die zou worden voorgesteld, t.t.z.. ‘pitching’ van een oplossingsalternatief en -aanpak, waarbij in beperkte sessie de oplossingspiste wordt gepresenteerd en afgetoetst met de klant, of een essentieel element van oplossing wordt getoetst aan de klantverwachting.

Termijn

De offerteopmaak moet in elk geval zo spoedig mogelijk na de aanvraag effectief opgenomen en aangevat worden, en moet een beperkte doorlooptijd kennen. Een verwachte antwoorddatum (NDD) kan worden afgesproken of bijgesteld tijdens de offerteopmaak, met akkoord van de klant, indien voortschrijdend inzicht leidt tot een aangepaste opdrachtformulering of er belangrijke aangepaste verwachtingen inzake de oplossing zijn, die nopen tot (gedeeltelijke) herwerking van een gevorderd ontwerp van projectvoorstel.

Indien de dienstverlener meent dat er geen professioneel antwoord kan geleverd worden binnen een voor een dergelijke offerteopmaak redelijke termijn, omdat er in aanzienlijk meer of langer durende voorbereidingen nodig zijn om zover te geraken als in de aanvraag werd gesteld, dan is het wenselijk om dit als dusdanig met de aanvrager te bespreken en een preliminair voorbereidingstraject als bestelbaar projectvoorstel voor te stellen. De uitvoering en het resultaat daarvan zal vervolgens toelaten om een professioneel en geschikt antwoord te bieden op de oorspronkelijke vraagstelling, en dit bestelbaar voor te leggen als projectvoorstel.

Voor alle projectvoorstellen wordt een geldigheidstermijn van minstens 3 maanden gerespecteerd, of een andersluidende geldigheidsperiode en dus uiterste besteldatum mits de nodige valabele verantwoording op basis van objectieve elementen van het projectvoorstel.

Product-focus

Bij een Project heeft de Klant steeds een bepaald resultaat voor ogen. In functie van het gewenste resultaat en van de vertreksituatie zullen meer of minder activiteiten moeten uitgevoerd worden.

Naast de generieke Werkproducten die bij ieder Project noodzakelijk zijn in het kader van het projectbeheer (onder andere het projectplan) zijn er ook een reeks specifieke Werkproducten die in het kader van het Project zullen moeten geleverd worden. Deze specifieke Werkproducten kunnen voor elk Project verschillend zijn en worden gepreciseerd in het Projectvoorstel. In elk geval moet de projectaanpak methodisch zijn, en in lijn met de betreffende methodiek worden ook de planning, fasering, beheerwijze en uitvoeringsmethode opgenomen, die gericht zijn op en zo effectief mogelijk zullen leiden tot een gewenst en afdoend resultaat of product.

Passsend projectbeheer

De uitvoering van een Project gebeurt, afhankelijk van het type Project, in één of meerdere fasen en resultaatgericht, waarbij het aandeel van de projectmanagement activiteiten (planning, budgettering, opvolging van globale voortgang en oplevering, escalaties en beheer van de klant-relaties i.v.m. het project, projectrapportering, …) steeds in verhouding zal staan tot het uit te voeren werk. Het voor projectmanagement voorziene bedrag mag maximaal 15% bedragen van het totale bedrag voor prestaties voor het Project. Het aandeel projectmanagement kan per fase in een Project hoger of lager liggen, maar voor het totale Project dient het maximaal percentage gerespecteerd te worden. Enkel in uitzonderlijke gevallen en op basis van concrete argumenten kan hier in het Projectvoorstel van afgeweken worden.

Sjablonen

Als onderdeel van de beschrijving van de Serviceorganisatie dienen ook een sjabloon opgesteld en beheerd te worden voor Projectvoorstellen. Hierin bepaalt de ICT-Dienstverlender welke elementen minstens dienen opgenomen te worden in een Projectvoorstel. Meerdere sjablonen zijn mogelijk per onderscheiden projecttype of methodiek. In functie van een vormelijke en inhoudelijke consistentie van de projectvoorstellen over de dienstverleners heen, wordt dit maximaal afgestemd met de andere ICT-Dienstverleners, en met de ICT-Dienstverlener voor de integratiediensten en HFB.

Algemeen

De output van alle voorgaande fasen vormen de input voor de fase uit de projectlevenscyclus waarop het Projectvoorstel betrekking heeft.

De Klant staat centraal m.b.t. de specificatie van de verwachtingen en de vereisten, en zal ook alle Werkproducten accepteren; voor beide zal hij een gedegen begeleiding krijgen vanwege de ICT-Dienstverlener.

7.3.2 Werkaanvraag voor uitvoering van een Project of Projectfase

Op basis van het ontvangen Projectvoorstel kan de Klant beslissen om de uitvoering van het Project (of van een of meerdere Projectfasen) te bestellen.

Minstens op het einde van het Project, maar voor zover afgesproken bij de bestelling ook op het einde van een fase van het Project, wordt een Oplevering gevraagd van de betrokken Werkproducten.

Om een Project te realiseren zal de ICT-Dienstverlener gebruik maken van een erkende projectmethodologie (PRINCE2 of gelijkwaardig)..

Voor elk Project wordt afgesproken welke specifieke overlegstructuren er voorzien worden en wat hun respectievelijke bevoegdheden zijn.

Voor elk Project zal er minstens een Project stuurgroep voorzien worden die formele beslissingen kan nemen met betrekking tot het Project. In die Project stuurgroep zal minstens de projectleider van de Klant en de projectleider van de ICT-Dienstverlener zetelen. Minstens bij mijlpalen, dient een Project stuurgroep samengeroepen te worden om het afsluiten van de vorige fase en de start van de volgende fase goed te keuren.

Daarnaast moet er regelmatig ad hoc contact zijn tussen de beide projectleiders.

Bij de start van het Project wordt de “base line” voor uitvoering vastgelegd, conform aan het goedgekeurde Projectvoorstel. Deze kan nadien enkel gewijzigd worden bij formeel goedgekeurde wijzigingen aan het projectplan. Tijdens de realisatie van het Project zal de ICT-Dienstverlener aan de Klant rapporteren conform de afspraken die gemaakt zijn in het Projectvoorstel. Minimaal zal de projectleider van de Klant regelmatig een voortgangsrapportering t.o.v. van het oorspronkelijk projectplan ontvangen. De vooruitgangsrapportering moet de actuele situatie vergelijken met de “base line”. Hierbij kan gebruik gemaakt worden van “earned value” –berekeningen. Bijkomende rapporteringseisen kunnen per Project worden afgesproken.

Na afwerking van de verschillende in het Projectvoorstel vermelde Werkproducten (inclusief Project-documenten) kan de ICT-Dienstverlener aan de Klant vragen om de Oplevering te laten plaatsvinden op basis van de in het Projectvoorstel opgenomen acceptatiecriteria. Voorafgaand zullen (gedeeltelijke) acceptatietesten plaats vinden. Vanaf het moment dat de ICT-Dienstverlener formeel de afwerking van de in het Projectvoorstel opgenomen Werkproducten meldt en de Oplevering vraagt beschikt de Klant over een termijn van één kalendermaand binnen dewelke hij de Oplevering moet uitvoeren, tenzij er in het Projectvoorstel een andere regeling is afgesproken.

De ICT-Dienstverlener dient voor de uitvoering van deze Dienst Profielen in te zetten met de juiste competenties. De lijst van competenties met de detailomschrijving van de kwalificaties worden opgenomen in het gedeelte “Serviceorganisatie”.

7.3.3 Werkaanvraag voor de bestelling van een projectwijziging

In de loop van de uitvoering van een Project, kan het nodig blijken dat belangrijke wijzigingen aan een Project nodig zijn die formeel dienen te worden besteld en doorgevoerd.

Projectwijzigingen die een wezenlijke impact hebben op de projectuitvoering, worden conform methodologisch bepaalde processen van wijzigingsbeheer (zie bijv. PRINCE-2) voorbereid. Deze voorbereiding resulteert in het opstellen van een onderbouwd en helder wijzigingsvoorstel vanwege de ICT-Dienstverlener, dat aan de Klant wordt voorgelegd voor goedkeuring en bestelling.

De uitvoering van zulke projectwijziging kan besteld worden door de Klant, door het indienen van een Werkaanvraag voor projectwijziging.

De wijziging wordt vervolgens in het Project doorgevoerd, conform het goedgekeurde en bestelde wijzigingsvoorstel. De wijziging zelf wordt volledig geïntegreerd in de (aangepaste) uitvoering van het Project. Een Werkaanvraag voor projectwijziging wordt op zich niet apart opgeleverd.

Ook een opdracht vanwege de Klant om het Project voortijdig te beëindigen, wordt als een dergelijke formeel te bestellen wijziging beschouwd.

7.4 SLA

7.4.1 Tijdige uitvoering van Projecten

Beschrijving en definitie

Deze indicator meet de verhouding tussen de effectieve projectduur en de afgesproken projectduur. Indien een Project bestaat uit verschillende afzonderlijk op te leveren fasen dan geldt deze indicator voor elke op te leveren fase. De projectduur start op het ogenblik van de bestelling van het Project (of de betrokken fase) en loopt tot op het ogenblik van de Oplevering van het Project (of de betrokken fase).

Service Level

De effectieve duur (in Werkdagen) voor het Project (of de betrokken fase) mag de afgesproken duur voor het Project (of betrokken fase) met niet meer dan 10% overschrijden. Die toegelaten overschrijding bedraagt vijf Werkdagen voor projecten met een afgesproken duur van minder dan 50 werkdagen.

Wanneer een Project uit verschillende afzonderlijk op te leveren fasen bestaat, dan zal bij het niet halen van de vooropgestelde duur voor een bepaalde fase, de einddatum van de daaropvolgende fases aangepast worden. Echter de duurtijd (aantal Werkdagen) van de van de daaropvolgende fases blijft ongewijzigd.

Randvoorwaarden, assumpties en uitzonderingen

In het Projectvoorstel wordt de baseline-planning opgenomen. De planning dient alle activiteiten te omvatten vanaf de bestelling tot de Oplevering. De baseline van een Project kan enkel herzien worden via een beslissing van de Project stuurgroep. Hierbij kunnen eventuele vertragingen te wijten aan de Klant, alsook de gevolgen van eventuele belangrijke wijzigingen in rekening gebracht worden.

Meetelementen en –methode

Op het ogenblik van de bestelling van een Project (of een fase) wordt de besteldatum geregistreerd als aanvangsdatum van het Project (of van de fase). Op basis van deze aanvangsdatum en de in het Projectvoorstel opgenomen planning worden de geplande data geregistreerd voor elke voorziene mijlpaal, waaronder de geplande datum van Oplevering van het Project (of de fase). Naarmate het Project (of de fase) uitgevoerd wordt, worden de effectieve data voor elk van de mijlpalen geregistreerd. Op het ogenblik van Oplevering van het Project (of de fase) wordt dan de effectieve doorlooptijd in Werkdagen, tussen besteldatum of de startdatum van de fase uit de baseline en datum van Oplevering, vergeleken met de geplande doorlooptijd in Werkdagen voor dezelfde periode.

De start- en einddata van Projecten en de eventuele fasen binnen het Project dienen ook geregistreerd te worden in de Gemeenschappelijke Ondersteunende Systemen.

7.5 Prijsmechanisme

Voor een Project wordt steeds afgerekend op basis van de kosten opgenomen in het Projectvoorstel. De kosten voor het opmaken van het Projectvoorstel zelf, worden verondersteld verrekend te zijn in de algemene Overhead.

De prijs voor deze Dienst bestaat uit de volgende delen:

- De prijs voor de door de te leveren prestaties;
- De prijs voor de te leveren Producten (Hardware/Software);
- De prijs voor de door Onderaannemers te leveren prestaties (o.a. indien er specifieke competenties vereist zijn waarover de ICT-Dienstverlener niet beschikt)

Voor wat betreft de prijs van de prestaties, zijn er per fase drie opties : in resultaatsverbintenis (RV) tegen vaste prijs, in middelenverbintenis (MV) of volgens Target cost (TC).

Voor de Projecten of projectfasen die in “resultaatsverbintenis” uitgevoerd worden, wordt de uiteindelijk te betalen prijs bepaald door de forfaitaire prijs die bepaald werd in het Projectvoorstel.

Voor de Projecten of projectfasen die in “middelenverbintenis” uitgevoerd worden, wordt de uiteindelijk te betalen prijs bepaald door het reëel gepresteerde aantal uren per Profiel en hun Eenheidsprijs en de werkelijk geleverde Producten met hun Eenheidsprijs. Dit wordt gestaafd op basis van timesheets die wekelijks aan de projectleider van de Klant ter goedkeuring dienen voorgelegd. Bij projectfasen in middelenverbintenis kunnen eventueel wel bepaalde delen in resultaatsverbintenis aangeboden worden.

Target cost zoals in deze Overeenkomst toegepast, betekent:

- Een Target kostprijs wordt vooraf in offerte vastgesteld, voor een geheel van te leveren prestaties. Dit geeft een totaalprijs aan waartegen de fase normaliter gerealiseerd kan worden, en die aldus ook het bedrag aangeeft voor de kostprijs van betreffende fase of project.
- De Target kost komt tot stand door een professionele raming met kennis van zaken, op basis van een zo concrete mogelijke vooropgestelde opdrachtbeschrijving (bijv. user stories), en eventueel na een vorm van onderhandeling. De Target kost is een zo goed als mogelijk ingeschatte kostprijs, die in overeenstemming is met en akkoord kan krijgen van de Klant. Voor opdrachten waar een redelijke inschatting onmogelijk vooraf te maken is, is Target cost niet aangewezen.
- Er wordt ook een “Cap” bedrag vooraf vastgesteld, dat de absolute bovengrens aangeeft. Het kostendeel bovenop een bereikte Cap-kostprijs, wordt niet aangerekend, aangerekend aan de Klant. Per default wordt de Cap vastgesteld op: Target kost + 40%.
- Prestatiekosten waarmee de Target wordt overschreden, tot aan de Cap, worden aan 50% van dit kostendeel aangerekend. Aldus wordt de overschrijding van de Target kostprijs ontmoedigd.
- Indien een fase of project kan worden gerealiseerd met minder dan de geplande prestatieskost van de Target kost, dan wordt het verschil tussen de aangerekende feitelijk geleverde prestaties en de voor dezelfde opdracht geldende Target kost, aan 50% gefactureerd aan de Klant.

Formule:

Factuurprijs voor prestaties = 50% van Target kostprijs + 50% van kostprijs van feitelijke prestaties, en dit tot aan het Cap bedrag.

Voorbeeld ter illustratie: Target = 100K, Cap = 140K. Er zijn daarenboven 20K aan investeringen.

Indien bijv. reëel gepresteerd twv 80K + 20K investeringen

Factuur: 50K (50% target) + 40K (50% van 80K) = 90K + 20K investering = 110K

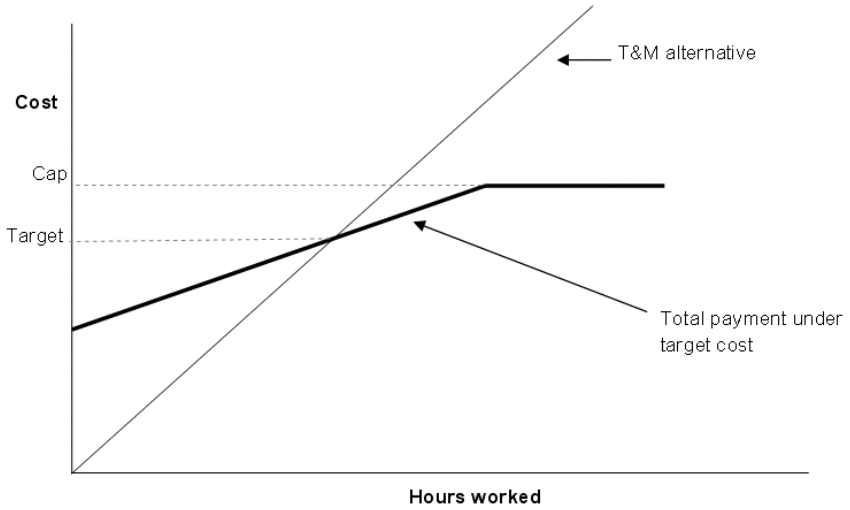
Indien bijv. reëel gepresteerd twv 120K + 20K investeringen

Factuur: 50K + 60K (50% van 120K) = 110K + 20K investering = 130K

Indien bijv. reëel gepresteerd boven Cap, bv. twv 200K prestaties + 20K investeringen

Factuur: CAPPED (50K + 50% x 200K = 150K >140K) = 140K + 20K investering = 160K

Grafisch geschetst (illustratie):



Deze TC-aanpak is bedoeld om het risico bij uitvoering te delen tussen Klant en ICT-Dienstverlener. Een Target kostprijs laat toe om minder risicopremie te verrekenen in de te bestellen totaalprijs, dan wat ingeval van een RV het geval zou zijn. Tegelijk stelt de Target cost een te verwachten totaalprijs, en bovendien nog eens een Cap, in tegenstelling tot een eventueel mogelijke belangrijke prestatie- en kostenverhoging indien een MV opdracht in de uitvoering zou uitlopen ten opzichte van de bij bestelling aangenomen verwachting; in een MV worden alle nodige effectieve prestaties aangerekend.

Een TC aanpak en kostprijs is aangewezen indien er in voldoende mate een normale verwachting ten aanzien van de werklast in de opdracht geraamd of berekend kan worden (de Target), wat bijvoorbeeld het geval is indien er op basis van een voldoende heldere behoeftenformulering een voorafgaande plannings- en ramingsoefening is kunnen gebeuren, waarmee het Target niveau voor betreffende bereik van de opdracht met voldoende vertrouwen vastgesteld is kunnen worden.

Ingeval van Target cost worden eventuele gedeelten tegen een forfaitaire vaste kost zoals investeringen, afzonderlijk behandeld en afgerekend, en deze worden niet in rekening gebracht in bovenvermelde verrekening van prestaties.

Voor wat betreft de door Onderaannemers te leveren prestaties, kunnen de prijzen van Onderaannemers in de offertes opgenomen worden. Overeenkomstig de in rubriek 8.2.3 van het Basiscontract beschreven basisprincipes, dienen deze prijzen via marktbevraging tot stand gekomen te zijn en kan er door de ICT-Dienstverlener geen Overhead en geen Mark-up op genomen worden.

7.6 Prijscorrectie

Er wordt automatisch en zonder notificatie een Prijscorrectie toegepast indien de effectieve duur (in Werkdagen) voor het Project (of de betrokken fase), de afgesproken duur voor het Project (of betrokken fase) met meer dan 10% overschrijdt.

Deze Prijscorrectie bedraagt 2.5% van de prijs (excl. de prijs van de Producten) voor het Project (of de betrokken fase) per begonnen bijkomende vertraging van 10% (minimaal 5 Werkdagen). Zo zal de prijscorrectie 2.5% bedragen met ingang van de eerste Werkdag volgend op de 10% vertraging (minstens de 6e Werkdag), 5% met ingang van de eerste Werkdag volgend op de 20% vertraging (minstens de 11e Werkdag), enzovoort.

Zodra op die wijze een Prijscorrectie van 10% is bereikt heeft de Klant de optie om het Project te doen verderzetten door de ICT-Dienstverlener, dan wel het Project stop te zetten zonder enige vergoeding aan de ICT-Dienstverlener.

7.7 Facturatie

Voor Projecten zal de Oplevering per Project of per op te leveren fase van het Project, indien er fasen met afzonderlijke facturatie voorzien zijn, plaatsvinden door de Klant die de bestelling heeft geplaatst. De facturatie gebeurt op basis van een proces verbaal van Oplevering.

7.8 Rapportering

Tijdens de uitvoering van een Project dient in een gemeenschappelijk met de Klant gedeeld documentatiesysteem een projectfolder up-to-date gehouden te worden met minstens de volgende elementen:

- Het goedgekeurde Projectvoorstel
- De eventueel goedgekeurde wijzigingen
- De actuele planning (GANTT)
- Het verslag van o.a. stuurgroep vergaderingen
- Voortgangsrapporteringen
- De documentaire Werkproducten
- De PV’s van Oplevering

De Klant (voor de door hem aangevraagde Projecten) en het Bestuur (voor het geheel van de aangevraagde Projecten) dienen op ieder ogenblik via intranet toegang te krijgen tot de informatiesystemen. Dit moet toelaten om een rapport te genereren met minstens de volgende elementen :

- Identificatie van het programma waartoe het Project behoort (optioneel en in te geven door de Klant);
- Identificatienummer van het Project (Werkaanvraagnummer);
- Korte omschrijving van het Project;
- Identificatie van de Klant;
- Datum indiening Werkaanvraag;
- Datum beschikbaarheid bestelbaar Projectvoorstel;
- Datum vastlegging (door Klant in te geven datum);
- Identificatie van de fase;
- Korte omschrijving van de fase;
- Datum bestelling (van de uitvoering van het Project als geheel of van de betrokken fase);
- Datum Oplevering (van de fase of van het Project);

8 Transitie

8.1 Initiële transitie

De algemene bepalingen van de Initiële Transitie zijn opgenomen in het Basiscontract (Hoofdstuk 9).

De Transitie van de Cloud- en datacenterdienstverlening is onderdeel van de Initële Transitie van het totale ecosysteem van de ICT-Dienstverlening.

De migratie van de Cloud- en datacenter dienstverlening dient uitgevoerd te worden als een project in resultaatsverbintenis.

Er wordt van de ICT-Dienstverlener verwacht dat hij volgende projectondersteuning voorziet:

- Een projectorganisatie met een projectleider en team dat verantwoordelijk is voor de opvolging, de coördinatie en de bijsturing van het Transitieproject voor de Cloud- en datacenter dienstverlening;
- Een vertegenwoordiging in de Stuurgroep Transitieproject van het ecosysteem van ICT-Diensten dat de Initiële Transitie voor het geheel van ICT-Diensten opvolgt;
- De ICT-Dienstverlener geeft een duidelijke omschrijving van het aantal VTE's, de functies en rollen met bijhorende competentieprofielen die door de ICT-Dienstverlener zullen ingezet worden tijdens de uitvoering van het transitieplan;
- De ICT-Dienstverlener geeft een duidelijke planning op voor het Transitieproject van de Cloud- en datacenterdiensten met minimaal een Gantt chart, een overzicht van de mijlpalen met per mijlpaal de op te leveren werkproducten, een lijst van risico's en bijbehorende mitigerende maatregelen, …
- De ICT-Dienstverlener geeft een totaalprijs voor de uitvoering van het Transitieproject voor de Cloud- en datacenterdiensten op basis van een resultaatsverbintenis. Alle eenmalige kosten (o.a. investeringen en ontwikkelingen) dienen integraal deel uit te maken van de totaalprijs voor dit Transitieproject. De kosten voor de effectieve ICT-Dienstverlening maken geen deel uit van de totaalprijs voor het Transitieproject. De totaalprijs voor de uitvoering van het Transitieproject voor de Cloud- en datacenterdiensten kan niet hoger liggen dan 2.400.000 € incl. BTW.

Onvermijdelijke dienstonderbrekingen dienen gepland te worden in de periodes dat de activiteit het laagst is. Er dient steeds een rollback procedure te worden voorzien teneinde adhoc de stabiliteit te kunnen herstellen bij onvoorziene problemen.

Voor de Cloud- en datacenter diensten wordt verwacht dat tijdens het Transitieproject minimaal volgende activiteiten voorzien worden:

- het verzekeren van de continuïteit van dienstverlening voor de betrokken klanten. De ICT dienstverlener zal daartoe alle infrastructuur ondersteunende VO-specifieke contracten overnemen die hiervoor vereist zijn. Het betreft alle VO-specifieke contracten die nodig zijn om de onderliggende infrastructuur voor de huidige diensten Application management en Computerzaal as a service te blijven verzekeren. De ICT-dienstverlener zal deze contracten overnemen (zie VO-specifieke contracten in de referentiebibliotheek) en deze gebruiken om het beheer van de onderliggende infrastructuur (met bijbehorende contracten) te verzorgen en te factureren aan de

betrokken klanten. Voor de infrastructuur die onderliggend is aan beheerde toepassingen, verzorgt de ICT-dienstverlener ook de nodige afstemming en ondersteuning aan de betrokken applicatiedienstverlener.

  - Voor wat betreft de toepassingen die momenteel draaien binnen hyperscale cloud cloud provider 1 (AWS, cloud provider 2 (Azure) en cloud regio's (AWS EU Dublin; Azure Amsterdam; en AWS EU Stockholm regio alleen voor data archivering) zal de migratie tijdens transitie zich vertalen in een administratieve migratie op vlak van de DC/Cloud dienst zelf wat een minimale migratie impact en zeer beperkte inspanning en kosten impliceert. De cloud regio's worden behouden;
  - Het co-locatiecontract met Colt voor NMC4 dient niet verdergezet omdat NMC4 uitgefaseerd wordt uiterlijk 31/08/2021.
  - De bestaande CZF diensverlening van Alphacloud Mechelen wordt verdergezet - zie supporting contract in de Refbib: VPC continuiteit - dienstbeschrijving Applicatie Management (1); Deze diensten worden verdergezet, maar zijn ook begrensd in de tijd tot eind 2024. De verderzetting gebeurt in hoofdzaak voor de continuïteit van de applicatiesystemen die vandaag al steunen op deze co-locatiedienst. HFB zal op deze CZF locatie ook geen DC connectiviteitsdiensten voorzien.

- de migratie van de actueel (vanuit VPC) aan de klanten aangeboden IaaS/PaaS diensten naar infrastructuur van de DC/Cloud ICT-Dienstverlener of naar infrastructuur van een publieke cloud provider. Alle dienstonderbrekingen als gevolg van een migratie dienen steeds tot een minimum te worden herleid.
  - Voor wat betreft de **IAAS/PAAS diensten** die steunen op DXC-VPC wordt een snelle afbouw voorzien tegen einde van het huidige contract. De DC/cloud dienstverlener voorziet een migratie tijdens de transitie via een logische lift&shift naar het nieuwe managed DC, van de infrastructuur- en platformdiensten. De klanzijde wordt hierbij betrokken, om aansluitend de applicatie zelf te migreren naar de nieuwe infrastructuur op het managed DC. **Deze migraties zijn binnen bereik van de transitie;**
  - Voor wat betreft de infrastructuurdiensten die onderliggend zijn aan de **Application Management dienst**, en die steunen op DXC-VPC-Mechelen wordt een continuïteit voorzien die beperkt is in de tijd, met als streefdatum eind 2024. DXC is bereid om de VPC-Mechelen gebaseerde managed DC diensten aan te bieden als subcontract naar de DC/Cloud leveranciers van contract 2022.
    - Er wordt in het bestek voorzien dat de DC Leverancier de onderliggende DC infrastructuurdiensten aanbiedt **zonder dat – voor de in VPC Mechelen gehoste applicatiesystemen obv de AM dienst - een migratie vereist** is, met als streefdatum eind 2024. Dit creëert een tijdsvenster van ruim 4 jaar om de hosting situatie van de applicaties aan te passen aan het nieuwe contract. Deze migraties zijn **buiten bereik** van de transitie;
- Voor datacenter outsourcing dient server en storagebeheer voorzien te worden voor de computerzalen Conscience en DR Antwerpen. De kosten voor implementatie van monitoring en beheer op afstand dient opgenomen te worden in de transitiekost
- Inrichten van alle processen/procedures/hulpmiddelen m.b.t. de nieuwe dienstverlening. Alle processen/procedures/hulpmiddelen om de diensten te kunnen leveren conform de vereisten in deze Service Portfolio moeten opgezet worden.

- Inrichten van alle processen/procedures/hulpmiddelen m.b.t. opzetten van de mogelijkheid tot het capteren van de bestellingen van Werkaanvragen vanuit een overkoepelende bestelinterface die deel uitmaakt van de Integratiediensten en verder het uitvoeren van deze Werkaanvragen voor de éénmalige diensten;

8.2 Deeltransitie tijdens de duur van de overeenkomst

Tijdens de duur van de overeenkomst kan de afname van de verschillende diensten stijgen of dalen.

De dienstverlener voorziet een flexibel model voor groei en inkrimping tot zelfs stopzetting van bepaalde diensten.

Het moet mogelijk zijn om tijdens de uitvoering van de Overeenkomst nieuwe Klanten te onboarden. Deze onboarding gebeurt via een Project. De DC/Cloud ICT-Dienstverlener voorziet de nodige processen/procedures en hulpmiddelen om onboarding van nieuwe Klanten mogelijk te maken en vlot te laten verlopen.

9 Exit

9.1 Maatregelen bij het beëindigen van de overeenkomst

De verschillende situaties waarin de overeenkomst beëindigd kan worden en de modaliteiten hierrond zijn beschreven in het basiscontract (hoofdstuk 10).

De DC/Cloud ICT-Dienstverlener zal er voor zorgen dat tijdens de volledige Duur van deze Overeenkomst elke vroegtijdige beëindiging steeds zonder problemen en tegen een vaststelbare en lage kostprijs kan gebeuren.

Dit betekent onder andere dat Inventarissen en documentatie steeds goed dienen bijgehouden te worden.

De volgende maatregelen zullen door de DC/Cloud ICT-Dienstverlener genomen worden:

- alle hardware-, software-investeringen zullen zoveel mogelijk conform zijn met de standaard van de ICT-markt. Daarom zal de ICT-Dienstverlener altijd het gebruik van standaarden, normen en richtlijnen aanbevelen waardoor het Bestuur zo weinig mogelijk zal gebonden zijn aan bedrijfseigen en -specifieke apparatuur of programmatuur die een beperkt marktaandeel bezit;
- Er wordt maximaal gebruik gemaakt van open standaarden en open source om een eenvoudige overdraagbaarheid maximaal te garanderen;
- Alle VO-specifieke contracten die afgesloten worden moeten kosteloos overdraagbaar zijn naar zowel de aanbestedende overheid als een Toekomstige ICT-Dienstverlener en dit met behoud van de voor de aanbestedende overheid of de betrokken Klanten bedongen voorwaarden, tenzij vooraf en expliciet anders afgesproken met de aanbestedende overheid of de betrokken Klanten. Verder moet ervoor gezorgd worden dat, tenzij vooraf en expliciet anders afgesproken met de Klant, alle onderliggende VO-specifieke contracten maandelijks of jaarlijks geheel of gedeeltelijk moeten kunnen stopgezet worden;
- Alle procedures en werkwijzen die door de ICT-Dienstverlener zullen gebruikt worden, zijn conform the “State-of-the-Art” (erkend door de internationale ICT-experten en ICT-consultants). Deze conformiteit is een garantie dat het Bestuur het gepaste personeel zal kunnen vinden zonder grote moeilijkheden;
- De ICT-Dienstverlener zal minstens één keer per jaar een controle uitvoeren van de betrouwbaarheid van de Configuratiedatabank (lijst van hardware, software-componenten, operationele procedures, lopende contracten, …). Deze controle wordt bijgevoegd aan de periodieke controles. Het doel is na te kijken dat de Inventarissen (hard-ware, software, configuraties,…) werkelijk op een kwalitatieve wijze bijgehouden worden.
- Alle kennis m.b.t. de ICT-omgeving van het Bestuur en m.b.t. de aan de Klanten geleverde Diensten (processen, procedures, richtlijnen, helpdeskdossiers, exploitatiedossiers, …) wordt systematisch opgeslagen en ter beschikking gehouden zodat een kosteloze kennisoverdracht op elk ogenblik mogelijk is.

9.2 Deelexit tijdens de duur van de overeenkomst

Aangezien er voor het geheel van de gevraagde ICT-Dienstverlening binnen deze Overeenkomst geen exclusiviteit wordt verleend aan de DC/Cloud ICT-Dienstverlener kunnen de verschillende Klanten ervoor opteren om alle of bepaalde Diensten niet meer af te nemen tijdens de Duur van deze Overeenkomst.

Voor sommige Diensten is in deze Service Portfolio een specifieke Werkaanvraag opgenomen waarbij de modaliteiten rond het stopzetten van de desbetreffende Dienst expliciet is beschreven.

Voor alle andere exploitatiediensten waarvoor er geen expliciete omschrijving is opgenomen in de Service Portfolio, dient de stopzetting projectmatig gerealiseerd te worden via een exit Project.

Default omvat het exit Project alle activiteiten die nodig zijn om de betreffende Dienst te stoppen en zal vanaf datum van stopzetting de facturatie van de maandelijkse eenheidsprijs stoppen.

Enkel in het geval dat in het Projectvoorstel voor het starten van de exploitatiedienst expliciet werd opgenomen en bijgevolg met de Klant werd afgesproken dat de onderliggende onderhoudscontracten en/of Licenties voor een langere periode dan 1 jaar worden afgesloten kan deze extra en nog niet verrekende reële kost in rekening gebracht worden naar de Klant toe via het betrokken exit-Project.