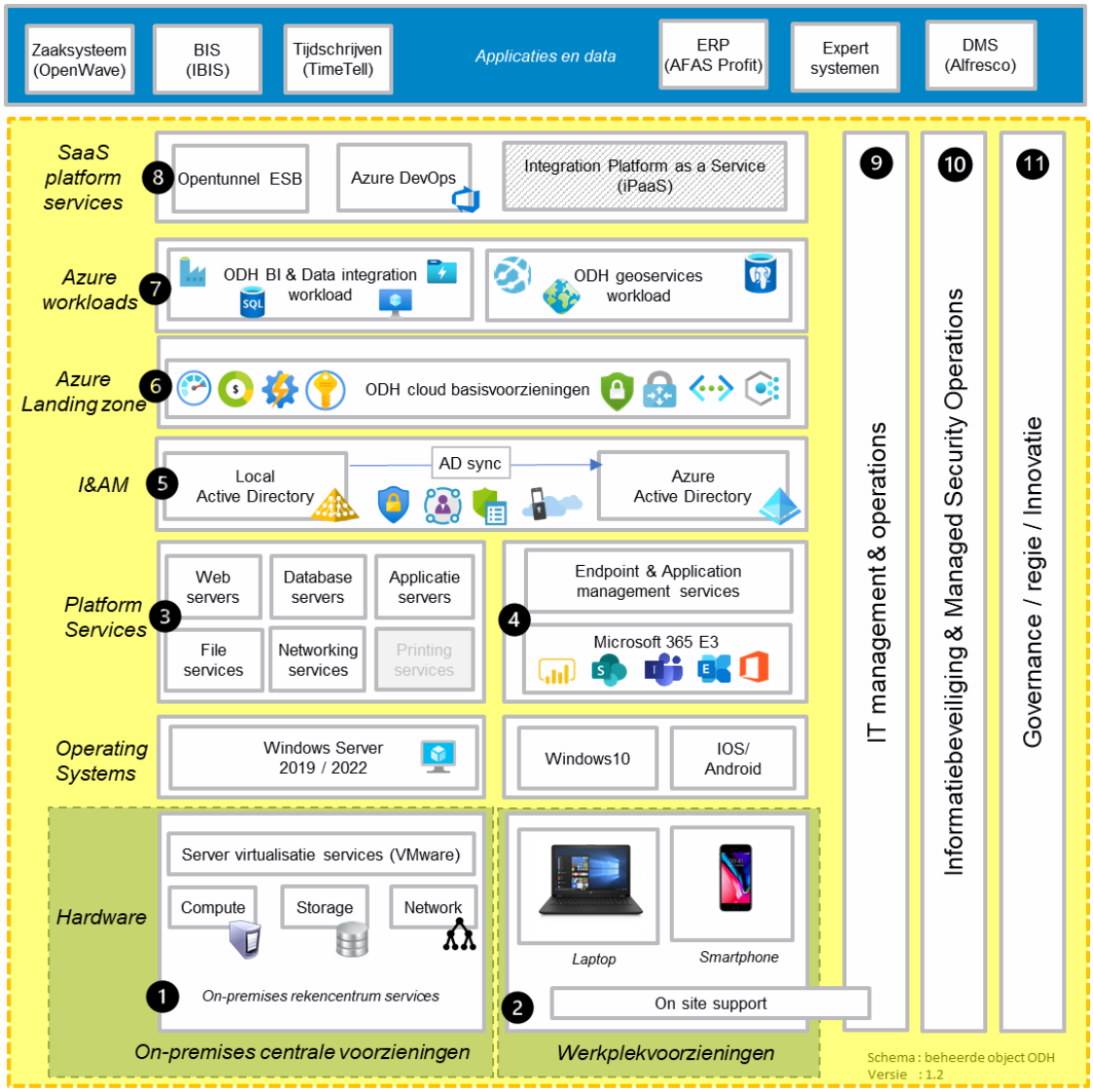
Beschrijving huidige situatie

De technische infrastructuur die door de leverancier van perceel 1 as-is in beheer dient te worden genomen na gunning duiden we aan als het Beheerde Object. In de huidige situatie wordt het technisch beheer op het Beheerde Object uitgevoerd door meerdere externe partijen:

- De eerste beheerpartij is verantwoordelijk voor het beheer van de on-premises centrale voorzieningen (servers, storage, netwerk, uitwijk), de werkplekomgeving, telefonie en Microsoft 365. Deze partij levert tevens een skilled service desk en on-site support aan eindgebruikers.
- De tweede beheerpartij is verantwoordelijk voor het beheer van de netwerkcomponenten (Fortigate firewall, Aruba componenten (inclusief Wifi) en Clearpass (network access protection).
- De derde beheerpartij is verantwoordelijk voor het beheer van de Azure Cloud omgeving en de daarin aanwezige workloads (dataplatform en geo-services).

Het beheer door deze partijen is volledig van elkaar gescheiden, zowel voor wat betreft de processen als de tooling. Consequentie hiervan is dat uniformiteit in het beheer ontbreekt en dat ODH geen integraal beeld heeft van de beheerstatus van de IT-omgeving. Dit bemoeilijkt de regievoering vanuit ODH.

Het te beheren object en de bijbehorende beheerprocessen zijn hieronder uitgewerkt in het gele kader. Aangezien de ODH constant werkt aan de verbetering van haar omgeving, kunnen er gedurende de aanbestedingsperiode wijzigingen plaatsvinden op de hieronder beschreven inrichting. ODH zal middels een nota van Inlichtingen eventuele wijzigingen c.q. de laatste stand van zaken communiceren voorafgaand aan de sluitingsdatum voor het indienen van de inschrijvingen.



De verschillende beheerdomeinen van het beheerde object worden hieronder toegelicht.

Alle hieronder beschreven beheeractiviteiten vallen binnen perceel 1 van de aanbesteding, m.u.v. de levering van hardware (perceel 2) en software (perceel 3).

1.1.1 On-premises datacenter services (beheerdomein 1 in de afbeelding)

ODH beschikt over een eigen datacenter in het kantoorpand aan het Zuid-Hollandplein en een fysieke uitwijkvoorziening elders in het land. In het verleden werden vrijwel alle diensten geleverd vanuit het eigen datacenter, maar door de transitie naar clouddiensten neemt de omvang van de on-premises diensten steeds verder af. Vrijwel alle primaire en secundaire bedrijfsapplicaties en data en documenten zijn reeds verplaatst naar de cloud of worden geleverd via Application hosting diensten. Het transitieproces is nog gaande en wordt de komende periode voortgezet. Het doel is om de on-premises IT-services uiteindelijk volledig te vervangen door cloud alternatieven en het ODH on-premises datacenter volledig te ontmantelen.

De on-premises servers (35) zijn gevirtualiseerd op een VMWare ESXi omgeving. Door de transitie naar de cloud is het aantal fysieke servers in de ESXi omgeving inmiddels gereduceerd van 6 naar 3. Er draait momenteel nog een NetApp SAN oplossing in het datacenter. Deze bevat de virtuele harddisks van de virtuele servers en een fileshare met bedrijfsdocumenten die nog naar de cloud moeten worden verplaatst.

Ook alle netwerkapparatuur is onderdeel van dit domein. De netwerkapparatuur bestaat uit:

- 4 x core HP FlexFabric 5700-32XGT-8XG-2QSFP en 12 x Aruba 2930F netwerk switches
- 19 Aruba AO-505 wireless access points
- Een WAN-access voorziening van 500 Mbit primair (KPN) en fallback verbinding van 100 MBit (COLT)
- Een Fortigate firewall cluster met 2 Fortinet 601E clusternodes
- Een Clearpass voorziening voor Network Acces Protection

De datacenter nutsvoorzieningen (kastruimte, toegangsbeveiliging, stroom/UPS) zijn eigendom van ODH en in scope voor het beheer. De voorzieningen voor ventilatie/koeling vallen buiten de scope van beheer.

1.1.2 Fysieke werkplekvoorzieningen (beheerdomein 2 in de afbeelding)

In dit domein valt het beheer (Perceel 1) van fysieke apparaten zoals laptops, randapparatuur en telefoons. De huidige werkplekapparatuur is eigendom van ODH. Alle mobiele telefoons zijn in april 2022 vervangen en worden voor 3 jaar ingezet. ODH maakt gebruik van iPhones (iPhone 13) en Android telefoons (Samsung S21). De ODH laptops zijn inmiddels meer dan 3 jaar oud. ODH is voornemens om na ingang van de overeenkomst voor de levering van hardware een vervangingstraject voor de laptops te starten op basis van een leaseconstructie (perceel 2).

De huidige client-architectuur is een fat-client architectuur waarbij de laptops (Windows 10) en applicaties centraal worden gemanaged via Microsoft Intune. Medewerkers van ODH hebben geen beheerrechten op hun laptops. Er worden meerdere modellen/types toegepast.

Plaats- en tijdonafhankelijk werken via de ODH laptops wordt ondersteund via een "AlwaysOn" VPN connectie. Apparaatonafhankelijk werken wordt niet ondersteund.

ODH staat open voor de modernisering van haar werkplekomgeving, bijvoorbeeld het toepassen van cloud based desktops en het ondersteunen van Bring Your Own Device (BYOD). De transitie naar dit soort oplossingen is onderdeel van het continu verbeteren en innoveren van de te beheren omgeving en zal mogelijk als (project)opdracht worden verstrekt aan de leverancier van perceel 1.

On-site support diensten vinden primair plaats binnen dit domein en bestaan onder andere uit de uitgifte/inname van laptops, telefoons en andere randapparatuur, alsmede het verhelpen van storingen die fysieke interventie vereisen zoals het heruitrollen van laptops.

1.1.3 Datacenter platform services (beheerdomein 3 in de afbeelding)

De datacenter platform services bevatten database servers (SQL Server), applicatieservers, fileservices, print- en scan services en infrastructurele services (Active Directory, etc.). De serverrollen zijn gebaseerd op Windows Server 2019 en 2022, met uitzondering van de file-services die rechtstreeks worden geleverd door de storagevoorziening in de vorm van een CIFS-fileshare. ODH host op dit moment zelf geen webservers. De ODH-website en het bijbehorende Web-CMS worden extern gehost en beheerd en vallen buiten de scope van deze opdracht.

Document management services (Alfresco), email services (Exchange online) en samenwerkingsservices (SharePoint online en Microsoft Teams) worden geleverd als SaaS-diensten. Hierop is geen technisch beheer vereist. Het functioneel beheer van Exchange, Sharepoint en Teams valt wel binnen de scope van de opdracht.

Het technisch beheer van de print- en scan services, alsmede het beheer en onderhoud van de multi-functionals (Xerox), is belegd bij een derde partij en valt buiten de scope van het beheer. Het beheer van de virtuele servers waarop de print- en scan services zijn geïnstalleerd, is wel in scope.

De beheer/monitoring-tooling (N-Central) van de on-premises platform services is eigendom van en ingericht door de huidige externe beheerpartij. Deze tooling wordt verwijderd na beëindiging van het huidige beheercontract. In de nieuwe situatie dient hiervoor een alternatieve oplossing te worden geïmplementeerd door de beheerpartij van perceel 1. ODH wenst een oplossing waarmee alle onderdelen van de omgeving zoveel mogelijk uniform en integraal gemonitord (en beheerd) kunnen worden.

Ook alle networking services vallen binnen dit beheerdomein, waaronder het technisch beheer van de firewall en het wireless network en het beheer van services zoals DNS, DHCP, network access protection (Clearpass) en VPN-services.

1.1.4 Endpoint & application management services (beheerdomein 4 in de afbeelding)

In dit domein worden de endpoint devices (laptops en smartphones) en applicaties beheerd. Hierbij wordt gebruik gemaakt van Microsoft Intune. Het applicatiebeheer betreft de deployment van applicaties en updates. Lokale applicaties worden fysiek op de laptops geïnstalleerd. ODH maakt nog geen gebruik van applicatievirtualisatie/streaming.

ODH maakt beperkt gebruik van aanvullende services zoals software assessment en metering. Er is wel behoefte aan dergelijke voorzieningen en dit is onderdeel van de scope van perceel 1.

De standaard browser (die belangrijk is vanwege grootschalig gebruik van web gebaseerde applicaties) is Microsoft Edge. Office-, email- en samenwerkings applicaties worden geleverd door Microsoft 365.

De ODH laptops draaien op Windows 10 en zijn Azure AD joined. De harddisks zijn versleuteld met Bitlocker en malware protection wordt geleverd door Microsoft Defender. Uitrol van werkplekken is image-based, waardoor bij uitrol van werkplekken altijd on-site support vereist is.

Binnen dit domein valt ook het beheer van de AV-middelen. Dit zijn voornamelijk Hisense Signage Displays met Android 7/8 en Yealink MVC Teams Room Systems met Windows IoT Enterprise. De besturinggsystemen van deze devices dienen periodiek te worden bijgewerkt. De AV-systemen zijn geplaatst in diverse vergaderkamers in het kantoorgebouw van ODH.

1.1.5 Identity & Access Management (beheerdomein 5 in de afbeelding)

Het hart van een goede beveiliging is te weten wie iemand is en diegene ook alleen toegang te geven tot informatie die nodig is om werkzaamheden uit te voeren. Om dit goed in te richten, is er steeds meer behoefte om zaken zoals IAM en RBAC. De ODH heeft recent een oplossing voor geautomatiseerde user-provisioning aangeschaft (Hello ID) en is nog bezig met de implementatie en inrichting daarvan. ODH verwacht van de toekomstige beheerpartij van perceel 1 dat zij hierin bijdraagt als onderdeel van het (doorlopend) optimaliseren van de inrichting van de omgeving.

Vanwege afhankelijkheden met applicaties die Windows Integrated / Kerberos authenticatie vereisen, maakt ODH op dit moment nog gebruik van een lokale Windows Server Active Directory. Deze wordt gesynchroniseerd naar Azure Active Directory. Naast de (Azure) AD identities, wordt voor diverse applicaties gebruik gemaakt van

applicatie-eigen identity stores. De ODH heeft als doel om in de toekomst alleen gebruik te maken van identiteiten in Azure Active Directory. Dit maakt het identity management eenvoudiger en veiliger en biedt de eindgebruikers een betere gebruikerservaring (in combinatie met Single Sign On) omdat zij niet langer meerdere gebruikersnamen en wachtwoorden hoeven te gebruiken.

De ODH heeft recentelijk Microsoft E5 Security en E5 Compliance add-on licenties aangeschaft om het juiste gereedschap te hebben om IAM en informatiebeveiliging goed in te richten. Nog niet alle functies en mogelijkheden worden op dit moment benut. De toekomstige beheerpartij van perceel 1 zal een belangrijke rol spelen in het verder inrichten en optimaliseren van deze voorzieningen.

1.1.6 ODH cloud-basisvoorzieningen (Azure landing zone) (beheerdomein 6 in de afbeelding)

ODH hanteert een Cloud tenzij-principe en als verfijning daarop een SaaS-tenzij principe. Het merendeel van de applicaties en services worden inmiddels als SaaS afgenomen. Daarnaast heeft ODH een eigen cloudomgeving ingericht in Microsoft Azure voor het hosten van intern ontwikkelde services (workloads). Op dit moment zijn workloads ingericht voor business intelligence en geoservices.

De Azure omgeving is opgebouwd volgens het landing zone model van Microsoft. Daarbij is een cloud basisomgeving ingericht dat fungeert als virtueel ODH datacenter. Deze omgeving levert de gemeenschappelijke beheer- en basisvoorzieningen die door alle workloads (kunnen) worden gebruikt, waaronder een Hub/spoke net architectuur, een VPN-connectie met de On-premises omgeving van ODH, Key Vaults, Log Analytics Workspaces, Storage accounts, Security Center, Azure Policy, Azure Advisor en Azure Monitor.

ODH beschouwt deployment (infrastructure as code) en beheer automation als randvoorwaardelijk voor effectief en efficiënt beheer van haar cloudomgeving. Daarom wordt gebruik gemaakt van ARM-templates en Azure DevOps CI/CD pipelines.

De ODH Azure omgeving is medio 2020 in eigen beheer ontworpen en geïmplementeerd. Vanwege de beperkte interne beheercapaciteit lag de nadruk daarbij op operationeel beheer en was er geen ruimte voor doorontwikkeling en innovatie. Het technisch beheer "as is" tijdelijk belegd bij een derde partij (Wortell).

De ODH Azure omgeving is globaal in lijn met best practices en referentiearchitecturen van Microsoft ontwikkeld. Er is echter geen cloud adoption framework toegepast. Mede als gevolg daarvan zijn er nog aandachtsgebieden op gebied van organisatie, processen en technologie. Zo moeten de governance en compliance processen strakker worden ingericht en moeten optimalisaties worden doorgevoerd in de configuratie van de omgeving, zoals de implementatie van private endpoints. Het doorontwikkelen (en waar nodig herzien) van de cloudomgeving is onderdeel van de beheertaken van de toekomstige beheerpartij in perceel 1.

1.1.7 Azure workloads (beheerdomein 7 in de afbeelding)

ODH heeft momenteel twee workloads ingericht in de Azure omgeving. De eerste workload is een Business Intelligence dataplatform. Deze workload maakt gebruik van voorzieningen zoals Azure Data Factory, Azure SQL DB, Azure SQL Managed Instance en Azure Datalake. Daarnaast worden Azure VM's ingezet voor de Self Hosted Integration Runtime van Azure Data Factory. Voor het presenteren van de BI-rapportages wordt gebruikt gemaakt van PowerBI online. De Azure Data Factory wordt ook gebruikt voor data-integraties (ETL) tussen diverse (SaaS) applicaties.

De tweede workload is een geoservices voorziening voor het verwerken en presenteren van geodata en kaartlagen. Deze omgeving is opgebouwd uit een Azure App Service met een Linux/Tomcat application server waarin een instantie van de open-source GIS-applicatie Geoserver wordt gehost. Tevens is een Azure PostgreSQL database met PostGis extensie ingericht voor de opslag van geodata.

Het technisch beheer van deze workloads bestaat uit de provisioning van de resources en de monitoring daarvan. Het functioneel beheer van de workloads wordt uitgevoerd door beheerders van ODH.

1.1.8 SAAS Platform Services (beheerdomein 8 in de afbeelding)

In dit domein vallen applicaties en platformservices die op basis van SaaS worden afgenomen. De SaaS-applicaties vallen zowel voor wat betreft hun technisch als hun functioneel beheer buiten de scope van de opdracht. Wel moeten

er (i.s.m. de leverancier van perceel 1) stappen worden gezet ten aanzien van de (keten)monitoring van deze applicaties, zodat ODH altijd een actueel beeld heeft van de status van de IV-voorzieningen als geheel.

Ook het technisch beheer van de SaaS platformservices valt buiten de scope van de opdracht, maar voor de volledigheid worden de belangrijkste service toch benoemd: de Enable-U/JNET Opentunnel ESB realiseert de (digi)koppelingen met diverse overheidsdiensten zoals de basisregistraties, het omgevingsloket online en de digitale stelselvoorzieningen van de nieuwe omgevingswet (DSO). Daarnaast wordt de Opentunnel ESB gebruikt voor de koppeling tussen het zaaksysteem (OpenWave) en het document management systeem (Alfresco).

Verder maakt ODH in dit domein gebruik van Azure DevOps. In Azure DevOps worden de repositories en pipelines beheerd voor de geautomatiseerde deployment (CI/CD) van Azure resources. Het beheer van deze omgeving komt bij de leverancier van perceel 1 te liggen.

Tot slot is in dit domein ook een iPaaS dienst ingetekend in de afbeelding. Deze is grijs gearceerd, omdat deze dienst nog niet aanwezig is. ODH is zich nog aan het oriënteren op de nut en noodzaak van een dergelijke voorziening. Vast staat dat ODH een aantal van haar eigen databronnen extern wil gaan ontsluiten/publiceren. Dit gebeurt nu al deels via losse voorzieningen/applicaties (Geoserver, BodemInformatie Online), maar mogelijk is minimaal een API-management oplossing vereist/gewenst. De leverancier van perceel 1 dient hierover te adviseren.

1.1.9 Beheerprocessen (beheerdomein 9 in de afbeelding)

De beheerdomeinen worden momenteel als losse silo's van elkaar beheerd. Daarbij wordt een breed palet aan gescheiden tools en processen gebruikt. Hierdoor ontbreekt integraal inzicht in de beheerstatus van de omgeving als geheel.

ODH gebruikt Topdesk is als het centrale service management systeem. De belangrijkste ITIL processen (incident, problem, change) zijn hierin geborgd en de leverancier van perceel 1 dient te werken met dit systeem. Het functioneel beheer van Topdesk wordt uitgevoerd door ODH, maar ODH wenst dit optioneel te beleggen bij de toekomstige beheerpartij van perceel 1.

ODH loopt tegen diverse issues aan in het huidige IT-beheer. Zo kost het bijvoorbeeld veel tijd om actuele overzichten te verkrijgen, evenals configuratie-items en hun status, zoals applicaties, hun versies en op welke systemen die zijn geïnstalleerd. Ook is er geen actueel en volledig beeld van de compliance en beveiligingsstatus van de omgeving als geheel. Er zijn geen tools die deze status constant inventariseren/monitoren en actueel houden. Ook de operationele monitoring van de systemen op gebied van prestaties, capaciteit en beschikbaarheid is niet volledig en centraal ingericht.

Tevens is er geen inzicht in de prestaties en beschikbaarheid van SaaS-applicaties. De verantwoordelijkheid daarvoor ligt primair bij de betreffende leveranciers, maar ODH beschikt niet over voorzieningen om deze aspecten vanuit haar regierol te kunnen monitoren. Gevolg hiervan is dat regelmatig reactief wordt gehandeld na meldingen van eindgebruikers. Daarbij is door het ontbreken van ketenmonitoring soms ook lastig om snel de oorzaak van problemen te achterhalen.

Een ander aandachtspunt vormt de aansluiting/integratie van de beheerprocessen van ODH en die van de externe leveranciers. ODH hanteert deels haar eigen ITIL-processen op gebied van o.a. incident-, problem- en changemanagement. Het blijkt lastig om deze processen goed te af te stemmen op die van de leveranciers. Gevolg hiervan is dat de doorlooptijden van changes onnodig lang zijn en dat niet altijd de juiste stakeholders zijn betrokken bij impactanalyses of de uitvoering. Daarnaast heeft het gebruik van cloud services de potentie om de time-to-market van nieuwe services en wijzigingen op bestaande services te bekorten, maar de "traditioneel" ingerichte ITIL-processen van ODH zijn hier nog niet op voorbereid.

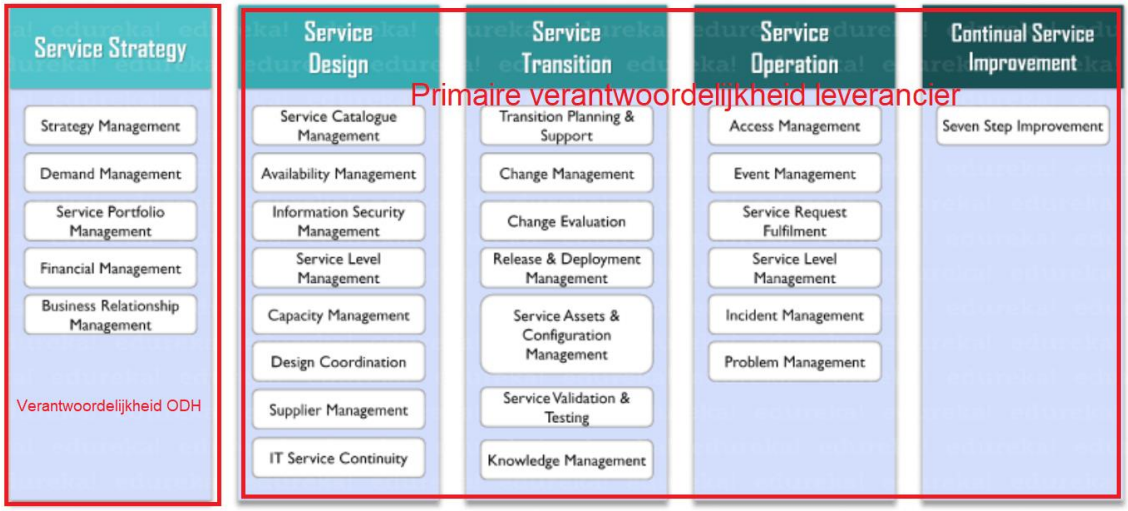
Binnen de scope van het beheerde object zijn momenteel 4 service desks ingericht:

1) Service desk voor de Azure Cloudomgeving (basisvoorzieningen en workloads);
2) Service desk voor netwerkbeheer
3) Service desk voor alle overige beheerdomeinen
4) On site support

Daarnaast wordt regelmatig gebruik gemaakt van de service desks van leveranciers van diverse SaaS diensten en applicaties.

Vanwege de beperkte resterende looptijd van de huidige beheercontracten, worden geen activiteiten meer uitgevoerd om de routering naar en tussen deze service desks te stroomlijnen. Het is voor ODH essentieel dat in de nieuwe beheersituatie alle service meldingen worden afgehandeld via een uniforme route en proces (one-stop-shop principe). Dit geldt zowel voor meldingen van eindgebruikers als voor het afhandelen van multidisciplinaire meldingen/wijzigingen waarbij meerdere leveranciers betrokken zijn. Van de beheerpartij (perceel 1) wordt verwacht dat zij namens ODH als intermediair optreedt tussen de verschillende partijen.

Niet alleen de routering van de processen moet worden verbeterd, maar ook de inrichting en uitvoering daarvan. ODH hanteert ITIL-v3 als framework voor de Service Management processen. Daarvan zijn vooral de processen rond incident-, probleem- en wijzigingenbeheer concreet uitgewerkt, maar moeten diverse processen nog nader worden uitgewerkt. Ook is nu niet altijd wie (ODH en/of leverancier) welke verantwoordelijkheden heeft binnen de verschillende processen. Het ondubbelzinnig en optimaal inrichten van deze processen is onderdeel van de inrichting van perceel 1. De ODH heeft hierbij de volgende globale scheiding van verantwoordelijkheden voor ogen:



Uit de verdeling wordt duidelijk dat ODH zoveel mogelijk ontzorgd wil worden. Essentieel daarbij is echter wel dat zij de controle en regie wel behoudt.

ODH hanteert nu de onderstaande incidentcategorieën en bijbehorende oplostijden. Deze moeten ook door de leveranciers van de verschillende percelen gehanteerd gaan worden:

Prioriteitenmatrix incidenten			
Impact / **Urgentie**	**Hoog** Het incident treft de gehele ODH organisatie	**Midden** Het incident treft meerdere afdelingen of teams	**Laag** Het incident treft één of enkele gebruikers
Hoog Belangrijke (primaire) processen zijn geblokkeerd.	P-dienst down	P-Spoed	P-Spoed
Middel Beperkingen in niet-bedrijfskritische werkzaamheden en/of processen.	P-Spoed	P-Spoed	P-Normaal
Laag Niet-storende fouten die zonder urgentie kunnen worden hersteld.	P-Normaal	P-Laag	P-Laag

De bijbehorende reactie en doorloop/oplostijden zijn:

Prioriteitenmatrix incidenten			
Responstijden / **Prioriteit**	**Service window**	**Reactietijd (inhoudelijke reactie)**	**Oplostijd (streeftijd)**
P-dienst down	24/7	0,5 klokuur	4 klokuren
P-spoed	Kantoortijden	1 uur	1 werkdag
P-normaal	Kantoortijden	1 werkdag	3 werkdagen
P-Laag	Kantoortijden	1 werkweek	14 werkdagen

De reactietijden voor het uitvoeren van probleemanalyses (Root Cause Analysis) zijn:

Prioriteitenmatrix Problems		
Responstijden / **Prioriteit**	**Service window**	**Opleveren Root Cause Analysis rapport**
Hoog (P-dienst down)	Kantoortijden	1 werkdag
Midden (P-spoed)	Kantoortijden	3 werkdagen
Laag (P-normaal)	Kantoortijden	RCA rapport alleen in overleg

Bovenstaande reactietijden zijn alleen van toepassing op het reactieve deel van problem management. Hiermee wordt bedoeld dat het probleem en de analyse daarvan worden getriggerd vanuit een (wederkerend) incident of een set van gerelateerde incidenten waarvan de oorzaak nog niet bekend is en/of waarvoor nog geen structurele oplossing beschikbaar is. Indien een RCA resulteert in een voorstel voor een structurele oplossing, dan wordt deze oplossing geïmplementeerd via het change management proces (indien nodig via spoed-changes). Het implementeren van de changes valt buiten bovengenoemde oplostijden.

1.1.10 Informatiebeveiliging en managed security operations (beheerdomein 10 in de afbeelding)

ODH heeft een eigen Information Security Officer die toeziet op het correct en volledig toepassen van het informatiebeveiligingsbeleid van ODH. Operationeel beschikt ODH over een vulnerability scanning oplossing (Insight VM van Rapid 7), die als scanning/monitoring tool aanvullend wordt ingezet op de tooling die wordt ingezet door de beheerpartijen van perceel 1.

Door de scheiding van beheerdomeinen (en partijen en tools) is er niet altijd een volledig overzicht van de beveiligingsstatus van de ODH-omgeving. Een voorbeeld hiervan is de scheiding van het Microsoft 365 beheer en de Azure omgeving die beiden gebruik maken van dezelfde Azure AD omgeving. Hoewel beide partijen hun best doen om de beveiliging en compliance voor hun eigen deel te waarborgen, blijken er in de praktijk soms toch zaken tussen wal en schip te belanden of niet (tijdig) opgepakt te worden. ODH is zelf soms de partij die onvolkomen/kwetsbaarheden in de beveiliging signaleert. De toekomstige leverancier van perceel 1 moet dit straks volledig onder controle hebben en ODH ook pro-actief informeren over potentiële bedreigingen.

1.1.11 Governance, regie en innovatie (beheerdomein 11 in de afbeelding)

ODH is nog bezig met de transitie naar de regierol binnen de IV-organisatie. Op dit moment zijn er op dit vlak niet veel specifieke processen ingericht, alhoewel er al wel belangrijke stappen zijn en worden gezet in het contract- en leveranciersmanagement en de service delivery naar de interne business organisatie.

Verder is op de meeste beheerdomeinen momenteel meer sprake van instandhouding dan innovatie. Op gebied van geogeoriënteerd werken en data analytics worden nu wel innovatieve stappen gezet die direct een herkenbare en gewaardeerde meerwaarde leveren voor de ODH business. De IV-voorzieningen van ODH moeten qua inrichting en beheer dusdanig doorontwikkelen in functionaliteit en kostenefficiëntie dat er meer ruimte en budget ontstaat voor focus op innovatieve ontwikkelingen die waarde toevoegen aan de ODH business. De leverancier van perceel 1 speelt hierin een belangrijke uitvoerende rol.