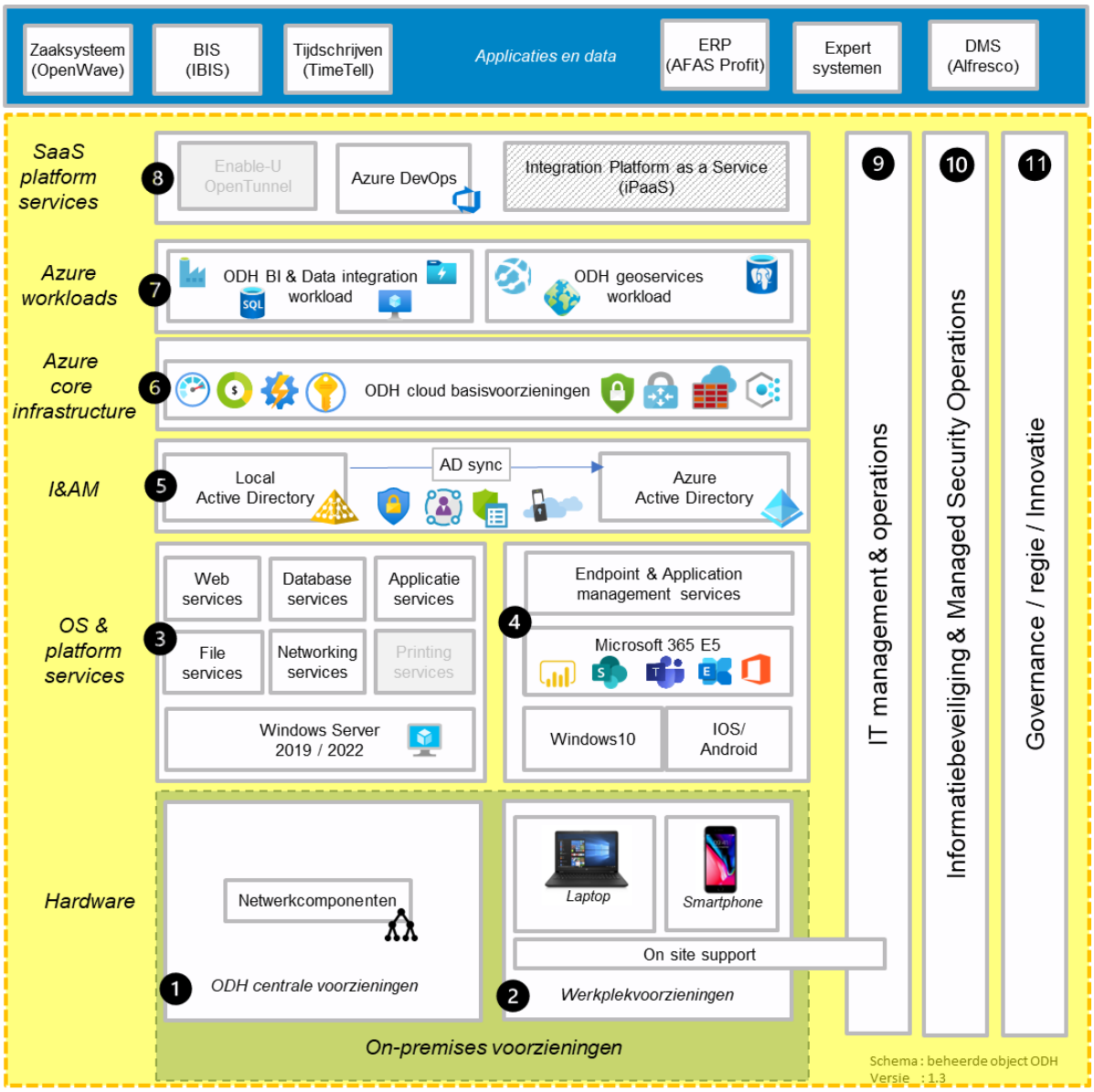
1. Beschrijving huidige situatie

De technische infrastructuur die as-is in beheer dient te worden, duiden we aan als het "beheerde object". De te beheren onderdelen van het beheerde object zijn weergegeven in het gele kader van het onderstaande diagram:



De te beheren onderdelen worden hieronder toegelicht op basis van de genummerde items uit het diagram. Alle hieronder beschreven beheeractiviteiten zijn onderdeel van de aanbesteding.

1.1 On-premises centrale voorzieningen (beheerdomein 1 in het diagram)

ODH beschikt over een eigen datacenter in het kantoorpand aan het Zuid-Hollandplein. In het verleden werden vrijwel alle diensten geleverd vanuit dit datacenter, maar door de transitie naar clouddiensten is de omvang van de on-premises omgeving sterk afgenomen. Vrijwel alle applicaties worden inmiddels geleverd via SaaS clouddiensten.

Daarnaast zijn recent de resterende on-premises virtual machines en file shares gemigreerd naar de ODH Azure omgeving. Als gevolg hiervan zijn de lokale fysieke servers, het VMWare cluster, de storage omgeving en de bijbehorende uitwijkvoorzieningen overbodig geworden. Deze voorzieningen worden binnenkort definitief uitgefaseerd en hoeven niet in beheer te worden genomen bij aanvang van het nieuwe beheercontract.

De volgende on-premises netwerkcomponenten zijn momenteel in beheer:

- 4 x core HP FlexFabric 5700-32XGT-8XG-2QSFP
- 12 x Aruba 2930F switches
- 19 Aruba AO-505 wireless access points
- WAN-access voorzieningen (500 Mbit primair en 200 Mbit secundair)
- Fortigate Fortinet 601E firewall met 2 clusternodes voor de internet break-out van lokale devices en de VPN-koppeling tussen de kantoorlocatie en de ODH Azure omgeving.
- Clearpass Network Acces Protection (de ClearPass servers zelf draaien in de ODH Azure omgeving)

Het beheer van deze componenten bestaat uit het beheer van de configuraties van deze componenten.

De huidige on-premises netwerkinrichting is nog deels gebaseerd op de situatie van voor de lift and shift naar Azure. Door het wegvallen van de fysieke servers, het VMWare cluster en de storage omgeving, zijn diverse onderdelen overbodig geworden zoals de server en storage VLAN's en de DMZ. Ook is de hardware nu overgedimensioneerd door de afname van de benodigde netwerkvoorzieningen. Om deze situatie te corrigeren, wordt een project gestart voor het herontwerpen (vereenvoudigen) van de on-premises netwerkinfrastructuur. Dit project zal worden afgerond voor de ingangsdatum van het nieuwe beheercontract. Het on-premises netwerkbeheer dat hierdoor resteert betreft alleen het beheer van de clientnetwerken (bedraad, draadloos, local internet breakout).

De te beheren datacenter voorzieningen bestaan uit de racks met netwerkcomponenten en de bijbehorende noodstroomvoorzieningen (UPS). Algemene voorzieningen voor stroom/ventilatie/koeling vallen buiten de scope van beheer. Door het wegvallen van de on-premises server en storage voorzieningen, onderzoekt ODH momenteel de mogelijkheid voor het afstoten van de huidige MER en het concentreren van de resterende netwerkcomponenten in de SER.

1.2 Werkplekvoorzieningen (beheerdomein 2 in het diagram)

In dit domein valt het beheer 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 huidige clientarchitectuur 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 hardware-typen toegepast. Plaats- en tijdonafhankelijk werken wordt ondersteund via een AlwaysOn VPN connectie op de ODH laptops. Apparaatonafhankelijk werken wordt niet ondersteund.

De huidige laptops zijn inmiddels meer dan 4 jaar oud en toe aan vervanging. ODH gaat met de huidige beheerpartij van de laptops starten met een vervangingstraject op basis van een leaseconstructie. De benodigde hardware wordt daarbij geleverd via de recent door ODH gecontracteerde nieuwe hardware leverancier (perceel 2 van de voormalige aanbesteding).

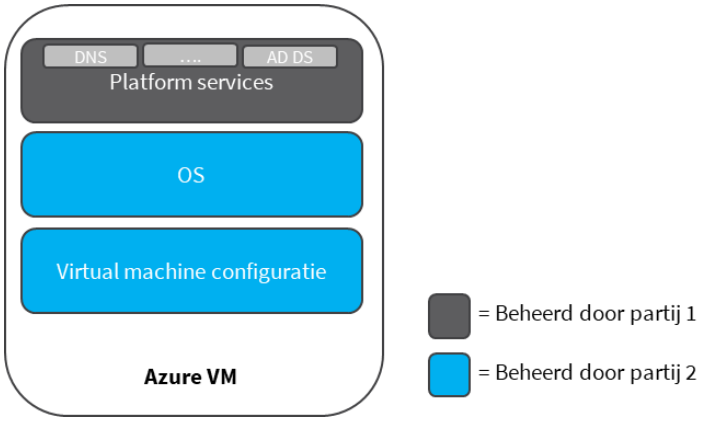
Hoewel ODH open staat voor de modernisering van haar werkplekarchitectuur, bijvoorbeeld door het toepassen van remote (cloud) based desktops en het ondersteunen van Bring Your Own Device (BYOD), wordt bij de aanstaande hardware vervanging in eerste instantie nog ingezet op het continueren van de bestaande fat-client architectuur. Daarbij worden de uitrolprocedures zoveel mogelijk geoptimaliseerd om de uitroltijd te bekorten en de handmatige handelingen door een beheerder (on-site-support) te minimaliseren of volledig te elimineren.

On-site support vindt primair plaats binnen het domein van de werkplekdiensten en bestaat voornamelijk uit de uitgifte en inname van laptops, telefoons en andere randapparatuur, alsmede het verhelpen van incidenten die fysieke aanwezigheid op de kantoorlocatie vereisen (heruitrol laptop, etc.).

1.3 OS & platform services (beheerdomein 3 in het diagram)

Dit domein bestrijkt het beheer van de virtuele servers en de platform services. Voorheen was er sprake van zowel on-premises VM's (op een VMWare cluster) als Azure VM's in de ODH Azure omgeving. Inmiddels zijn alle VM's gemigreerd naar Azure en worden alle Azure VM's op uniforme wijze beheerd en gemonitord.

Het beheer van de Azure VM's (inclusief OS-beheer) en het beheer van de daarop aanwezige platform services wordt momenteel gescheiden uitgevoerd door twee verschillende leveranciers zoals weergegeven in de onderstaande afbeelding:



Het OS-beheer van de Azure VM's (blauwe componenten) door partij 2 bestaat onder andere uit:

- Uitrollen en verwijderen van virtual machines (via change management procedures)
- Configuratiebeheer van de virtuele machines (inclusief beveiligingsinstellingen/hardening)
- Update management (maandelijkse en OOB uitrol van OS-updates via Azure update management)
- Backup en restore van VM's
- Disaster recovery van VM's
- Monitoring van VM's op OS-gerelateerde aspecten (beschikbaarheid, capaciteit, prestaties, beveiliging)
- Adviseren over en verwerken van aanbevelingen uit Azure Advisor en Microsoft Defender for Cloud. Hiervoor zijn op dit moment 6 wekelijkse overleggen gepland tussen ODH en de beheerpartij om de actuele status van de aanbevelingen door te nemen. ODH is tevreden over deze aanpak.
- Beheer van remote access voorzieningen (Azure Bastion).

Het beheer van de platform services (grijze componenten) door partij 1 bestaat onder andere uit:

- Beheer van Active Directory domain services (ADDS). De domain controllers draaien als Azure VM's in Azure
- Beheer van DNS-services
- Beheer van DHCP services
- Beheer van certificaat services (ODH root CA en CDP/CRL-endpoints)
- Beheer van SMTP (relay)-services
- Beheer van FileCap filesharing services
- Beheer van (twee) applicatie/fileservers
- Beheer van (vier) beheerservers met tooling voor de platform services
- Backup en restore van de platform services (voor zover niet afgedekt in de B&R van de VM's)
- Disaster recovery van de platform services
- Monitoring van de platform services (via NCentral)

Naast partij 1 en partij 2 is er nog een partij 3 die verantwoordelijk is voor het beheer van de on-premises firewall en de kantoorzijde van de VPN-connectie tussen de ODH kantoorlocatie en de ODH Azure omgeving.

Voorafgaand aan de lift and shift werd de on-premises firewall ingezet voor het routeren en filteren van alle verkeerstromen, inclusief de verkeerstromen van en naar de ODH Azure omgeving. Met de verhuizing van de core infrastructure services naar Azure is de rol van de on-premises firewall veranderd en wordt deze alleen nog ingezet voor het filteren van het lokale clientverkeer van en naar internet (local internet breakout).

On-premises clientverkeer bestemd voor de core infrastructure services in Azure wordt niet langer gefilterd door de on-premises firewall. Dit verkeer wordt ongefilterd doorgestuurd naar de ODH Azure omgeving en daar gefilterd door een nieuw gerichte Azure firewall (in combinatie met Network Security Groups). Het beheer van de Azure firewall is beschreven in hoofdstuk 1.6.

De ODH on-premises file share (5TB) die tot voor kort draaide op de storage-omgeving is gemigreerd naar een file share in Azure (Azure Files). Deze file share wordt via een private endpoint ontsloten op basis van Azure AD Kerberos authenticatie. Partij 2 is momenteel verantwoordelijk voor het beheer van de file share resources in Azure. Partij 1 is verantwoordelijk voor het beheer van de inrichting van de file share (folders, groepen, rechten).

De ODH-websites en het bijbehorende Web-CMS worden extern gehost en beheerd en vallen buiten de scope van deze opdracht. Het beheer van het intranet en interne subsites in SharePoint online ligt bij ODH.

Het technisch beheer van de print- en scan services, alsmede het beheer en onderhoud van de MFP's is belegd bij de leverancier van de printers en valt buiten de scope van de opdracht. Het OS-beheer van de Azure VM's waarop de printservices zijn geïnstalleerd, is wel in scope.

De N-central oplossing voor het monitoren van de platform services is eigendom van en ingericht door de huidige beheerpartij van de platform services. Deze tooling wordt verwijderd na beëindiging van het huidige beheercontract. In de nieuwe beheersituatie dient hiervoor een alternatieve oplossing te worden geïmplementeerd door de nieuwe beheerpartij. ODH wenst een oplossing (bij voorkeur Azure Monitor) waarmee alle onderdelen van de te beheren omgeving zoveel mogelijk uniform en integraal gemonitord kunnen worden. De licentie- en/of verbruikskosten van de nieuwe monitoring oplossing zijn voor ODH en hoeven niet te worden meegenomen in het prijzen blad.

Naast de bovengenoemde platform services, maakte ODH tot voor kort gebruik van een geclusterde SQL server op de on-premises VMWare omgeving. Deze server is uitgefaseerd tijdens de lift and shift naar Azure. Er draaien nu nog alleen nog twee SQL Server 2019 Express instances op de printserver VM's in Azure. Op deze instances hoeven geen (DBA) beheerwerkzaamheden te worden uitgevoerd. Wel worden deze instances periodiek voorzien van de noodzakelijke SQL-updates via het maandelijkse update management proces.

1.4 Endpoint & application management services (beheerdomein 4 in het diagram)

In dit domein worden de "endpoint devices" (laptops en smartphones) en applicaties beheerd. Hierbij wordt voornamelijk gebruik gemaakt van Microsoft Intune.

Het applicatiebeheer betreft de distributie van nieuwe applicaties en updates op bestaande applicaties. ODH maakt daarbij geen gebruik van applicatievirtualisatie oplossingen zoals streaming of virtual application delivery (VAD). Alle applicaties worden nog traditioneel lokaal geïnstalleerd op het device. Door de transitie naar cloud-diensten is het applicatieportfolio dat op deze wijze wordt beheerd de laatste jaren flink geslonken. De meeste applicaties worden nu web-based aangeboden. Zie bijlage 12 voor de softwarelijst met een overzicht van het ODH applicatie portfolio.

De office-, email- en samenwerkingsfuncties worden geleverd door Microsoft 365 (e5) en bestaan uit:

- Standaard Office KA-applicaties, zoals Word, Excel, PowerPoint en OneNote
- Outlook
- PowerBI
- Exchange online
- SharePoint online
- Onedrive
- Teams

Het beheer van de M365 applicaties en services is onderdeel van de beheerscope.

ODH maakt momenteel geen gebruik van tools/services voor software assessment management en metering. Er is wel behoefte aan dergelijke voorzieningen. Zie voor meer informatie de aanbestedingsleidraad.

De ODH laptops draaien op Windows 10 en zijn Azure AD joined. De Windows instellingen worden beheerd via Microsoft Intune. De harddisks zijn versleuteld met Bitlocker en malware protection wordt geleverd door Microsoft Defender. Voor remote support wordt Teamviewer gebruikt.

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

1.5 Identity & Access Management (beheerdomein 5 in het diagram)

Het hart van een goede beveiliging is te weten wie iemand is en diegene alleen toegang te geven tot de specifieke systemen en informatie die nodig zijn om de werkzaamheden uit te voeren. Om dit goed in te richten, heeft ODH behoefte aan adequate oplossingen op gebied van Identity & Access Management (IAM) en Role Based Access Control (RBAC).

In dit kader heeft ODH een cloud (SaaS) gebaseerde user-provisioning oplossing aangeschaft (HelloID) en daarin de processen voor in-dienst, uit-dienst en doorstroom van medewerkers ingericht. Voor nieuwe medewerkers wordt sinds kort bij indiensttreding automatisch een gebruikersaccount aangemaakt en bij uit-dienst worden de accounts automatisch uitgeschakeld. ODH is bezig om de toegangsrechten (ook voor bestaande gebruikers) steeds meer via de user-provisioning tool te gaan beheren. ODH voert daarbij zelf het beheer van de RBAC business rules uit. Als gevolg hiervan nemen de verantwoordelijkheden van de externe beheerpartij op gebied van gebruikersbeheer steeds verder af.

Vanwege afhankelijkheden met enkele applicaties die nog Windows Integrated (NTLMv2 / Kerberos) authenticatie vereisen, maakt ODH op dit moment nog gebruik van een lokale Windows Server Active Directory (ADDS). De domain controllers van dit domein zijn tijdens de lift and shift verhuisd naar Azure en worden later (mogelijk) nog vervangen door Azure Active Directory Services. De gebruikers en groepen van de lokale Active Directory worden via Azure AD Connect gesynchroniseerd naar Azure Active Directory.

Een punt van zorg/aandacht in de huidige inrichting van het technisch beheer door de externe partijen, is het gebruik van beheeraccounts. ODH staat alleen het gebruik van persoonlijke (op naam) beheeraccounts toe. Doordat één van de huidige beheerpartijen werkt met een grote pool van beheerders, zijn er (te) veel beheeraccounts aanwezig. Mede door het constante verloop van beheerders, is het beheer van deze accounts lastig. Idealiter zijn er alleen beheeraccounts aanwezig (of actief) voor beheerders die op een specifiek moment daadwerkelijk beheertaken uitvoeren. Deze accounts zouden dan alleen rechten moeten krijgen voor die specifieke taken en de objecten waarop ze het beheer uitvoeren. Dit is momenteel niet zo ingericht. ODH verwacht van de toekomstige beheerpartij dat zij met een oplossing komt om het aantal beheeraccounts zoveel mogelijk te beperken.

1.6 ODH cloud-basisvoorzieningen (Azure landing zone) (beheerdomein 6 in het diagram)

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 interne services (workloads). Op dit moment zijn workloads ingericht voor business intelligence / dataplatform en geoservices.

ODH maakt op dit moment gebruik van de onderstaande 24 virtuele servers. Deze zijn medio 2023 gemigreerd naar de ODH Azure omgeving.

Servernaam	Functie(s)	OS	Opmerkingen
VMAADC03	Azure AD Connect (actief) SMTP-relay (passief)	W2K17	
VMAADC04	Azure AD Connect (passief) SMTP-relay (actief) ODH CDP/CRL-endpoint	W2K19	
VMAPPS01	Applicatieserver Fileserver	W2K22	
VMAPPS02	Fileserver Webserver (IIS)	W2K22	
VMBH01	Beheerserver beheerpartij 1	W2K19	
VMBH02	Beheerserver beheerpartij 1	W2K19	
VMBH03	Beheerserver beheerpartij 1	W2K19	
VMBH04	Beheerserver beheerpartij 1	W2K19	
VMCA01	ODH Certificate services	W2K19	
VMCLEARPASS03	Network Access Protection	Linux Redhat Aruba	OS updates buiten scope
VMCLEARPASS04	Network Access Protection	Linux Redhat Aruba	OS updates buiten scope
VMDC06	ADDS Domain controller	W2K22	
VMDC07	ADDS Domain controller	W2K22	
VMEX21	Exchange Hybrid Server	W2K19	
VMFileCap01	Filesharing server (productie)	Linux Debian 11	OS updates buiten scope
VMFileCap02	Filesharing server (acceptatie)	Linux Debian 11	OS updates buiten scope
VMFORTI01	Beheerserver voor Fortigate	W2K19	
VMNCENTRAL02	Monitoring server	W2K19	
VMNDES02	Server voor werkplekuitrol	W2K22	
VMPS04	Printserver	W2K19	
VMPS05	Printserver	W2K19	
p-data-shir-001	Azure Data Factory SHIR	W2K19	
p-core-rap7cons01	Rapid7 vulnerability mgmt	W2K19	

Enkele servers staan op de nominatie om te worden uitgefaseerd. Dit zijn de VMNDES02, de VMEX21 en de VMNCentral02. Ook verwacht ODH van de nieuwe beheerpartij een alternatieve oplossing voor de beheerservers. 4 beheerservers voor het beheer van de ODH-omgeving zijn naar mening van ODH buitenproportioneel.

De OS-updates van de Linux VM's worden verzorgd door de leveranciers van de betreffende services.

Als onderdeel van deze lift and shift is de hub/spoke VNET-architectuur is gemigreerd naar Azure vWAN. Daarbij is tevens een Azure Firewall ingericht die de rol van de on-premises firewall heeft overgenomen (zie hoofdstuk 1.1). Ook zijn de Network Security Groups uitgebreid met diverse regels.

Bij de lift and shift is de traditionele on-premises DMZ-architectuur losgelaten. In plaats daarvan zijn de via internet ontsloten services (FileCap filesharing) achter een Azure (WAF v2) Application Gateway geplaatst.

De on-premises S2S VPN's die zijn verbonden met enkele SaaS-leveranciers zijn verhuisd naar Azure en ingericht als VPN-sites binnen Azure VWAN. Ook de AlwaysOn VPN client op de ODH laptops is gemigreerd naar een P2S User VPN Connection in Azure VWAN. Deze connectie maakt gebruik van de Azure VPN client uit de Microsoft Store.

De ODH Azure omgeving is (globaal) opgebouwd volgens de Azure landing zone architectuur van Microsoft. Daarbij is een platform landing zone ingericht die de "ODH cloud basisvoorzieningen" wordt genoemd. Deze landing zone fungeert als virtueel ODH datacenter dat de gemeenschappelijke beheer- en basisvoorzieningen levert die door alle workloads (kunnen) worden gebruikt. Hieronder vallen de Management Groups, Azure vWAN (inclusief VPN sites), Application Gateway, Azure Key Vault, Log Analytics Workspaces, Storage accounts, Microsoft Defender for cloud, Azure Policy, Azure Advisor en Azure Monitor.

Tijdens de (initiële) implementatie van de ODH Azure omgeving is geen gebruik gemaakt van het Azure cloud adoption framework van Microsoft of een ander framework. Mede als gevolg daarvan zijn er aandachtsgebieden op gebied van organisatie, processen en de technische inrichting die verbeterd kunnen worden. 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. Verbeteringen zullen via niet-standaard changes en/of mini-projecten worden afgehandeld (en vergoed).

1.7 Azure workloads (beheerdomein 7 in het diagram)

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 wordt een Azure VM ingezet voor de Self Hosted Integration Runtime van Azure Data Factory. Voor het presenteren van de BI-rapportages wordt gebruikt gemaakt van PowerBI online. Azure Data Factory wordt ook gebruikt voor diverse data-integraties (ETL) tussen 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. Binnenkort wordt hier een Azure webservice aan toegevoegd voor het webbased aanbieden van intern ontwikkelde geo-applicaties/kaarten.

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 de BI- en geobeheerders van ODH.

1.8 SAAS Platform Services (beheerdomein 8 in het diagram)

In dit domein vallen de platformservices die op basis van SaaS worden afgenomen. ODH maakt gebruik van de cloud Enterprise Service Bus "Opentunnel" van Enable-U. Deze oplossing 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). Zowel het technisch als het functioneel beheer van deze service valt buiten de scope van de opdracht (maar is vanwege de belangrijke rol in het ODH-landschap toch ingetekend in het diagram.

De Opentunnel oplossing dekt (in combinatie met de ETL-integraties in Azure Data Factory) het overgrote deel van de huidige integratiebehoeften van ODH af. Toch is in de architectuur van ODH een additioneel IPAAS (Integration Platform as a Service) component ingetekend, dat in de toekomst wellicht moet gaan voorzien in nieuwe behoeften op gebied van applicatie-integratie/messaging en gegevensuitwisseling via API-services. De kans is groot dat dit onderwerp op tafel komt gedurende de looptijd van het nieuwe beheercontract en als project/wijzigingsverzoek wordt belegd bij de nieuwe beheerpartij.

Tot slot valt ook de ODH Azure Devops omgeving (organisatie) in dit domein. ODH maakt gebruik van Azure DevOps voor diverse KANBAN en SCRUM boards en activiteiten. Daarnaast bevat de DevOps omgeving de initiële inrichting (repositories en pipelines) voor de geautomatiseerde deployment (CI/CD) van de ODH Azure resources. Deze

repositories en pipelines zijn de laatste jaren echter niet meer onderhouden en ook de tijdens de lift and shift toegevoegde resources (VWAN, Application Gateway, etc.) zijn niet via CI/CD geïmplementeerd. ODH wil met de nieuwe beheerpartij in gesprek of het infrastructure as code principe voor ODH nog van toegevoegde is en wat de consequenties (configuratiebeheer / desired state) zijn van het eventueel loslaten daarvan.

1.9 IT Management en Operations (beheerdomein 9 in het diagram)

De verschillende beheerdomeinen in het diagram worden momenteel als losse silo's van elkaar beheerd door meerdere beheerpartijen. Daarbij wordt een breed palet aan tools en processen gebruikt. Hierdoor ontbreekt integraal inzicht in de beheerstatus van de omgeving als geheel. Er zijn geen integrale (monitoring) tools, dashboards of rapportages die eenvoudig inzicht geven van de actuele status van de omgeving.

Op zich is het beheer van de losse onderdelen redelijk onder controle, maar het wordt bijvoorbeeld lastig als eindgebruikers klagen over de beschikbaarheid of prestaties van (primaire) SaaS-applicaties. Het is in de huidige opzet volkomen duidelijk dat de SaaS-leveranciers verantwoordelijk zijn voor de beschikbaarheid en prestaties van hun applicaties, maar hoe stel je als ODH (snel) vast dat het probleem daar wel of niet ligt? Het kan zomaar een probleem zijn met de internetverbinding, het lokale (wifi) netwerk, de configuratie van de ODH laptops of een combinatie van deze factoren.

Er zijn momenteel geen voorzieningen (ketenmonitoring) en integrale processen (incident management, problem management) die het effectief oplossen van (keten)problemen zoals hierboven genoemd ondersteunen. Gevolg is dat het oplossen van problemen regelmatig langer duurt dan voor de business acceptabel is. Ook worden problemen regelmatig als eerste door de business gemeld, terwijl ze achteraf gezien met adequate monitoring proactief voorkomen hadden kunnen worden.

ODH is nadrukkelijk op zoek naar een beheerpartij die oplossingen biedt voor dit soort vraagstukken en ODH de voorzieningen biedt om het integraal beheer en de regie daarop effectief in te richten. Aangezien het huidige beheer as-is wordt overgenomen, verwacht ODH niet vanaf dag 1 een pasklare oplossing. ODH verwacht echter wel dat de nieuwe beheerpartij met verbetervoorstellen komt om het integraal beheer en de ketenmonitoring stap voor stap (via changes en/of projecten) te optimaliseren.

ODH gebruikt Topdesk als het centrale service management systeem. De belangrijkste ITIL processen (incident, problem, change) zijn hierin ingericht. De toekomstige beheerpartij dient te werken met dit systeem. Een aandachtspunt hierbij vormt de aansluiting/integratie van de beheerprocessen van ODH met die van de nieuwe beheerpartij en die van andere externe leveranciers.

Het blijkt in de praktijk soms lastig om de ODH ITIL-processen goed te integreren met die van de leveranciers. Gevolg hiervan is dat de doorlooptijden van changes vaak onnodig lang zijn en dat niet altijd de juiste stakeholders betrokken zijn bij impactanalyses of de uitvoering van changes. Het gebruik van cloud services heeft de potentie om de time-to-market van nieuwe services en diensten sterk te bekorten, maar de "traditioneel" ingerichte ITIL-processen van ODH (en haar leveranciers) werken nog te vaak als rem hierop.

Een tweede aandachtspunt betreft de manier van werken binnen de processen. Uiteraard is het belangrijk om volgens de afgesproken processen te werken, maar dit moet geen doel op zich zijn en daardoor verzanden in (te) formele communicatielijnen. ODH hecht grote waarde aan interactiviteit en proactiviteit in de samenwerking met haar leveranciers en dat geldt zeker ook voor de samenwerking binnen de service management processen. Het face-to-face afstemmen van onduidelijkheden of andere zaken (met name in de changemanagement processen) verloopt vele malen sneller/effectiever via telefoon of Teams dan via indirecte status-updates in Topdesk. Topdesk is zeker belangrijk voor het borgen van de processen en het vastleggen van de gemaakte afspraken, maar moet niet (altijd) het enige en primaire communicatiemiddel zijn.

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

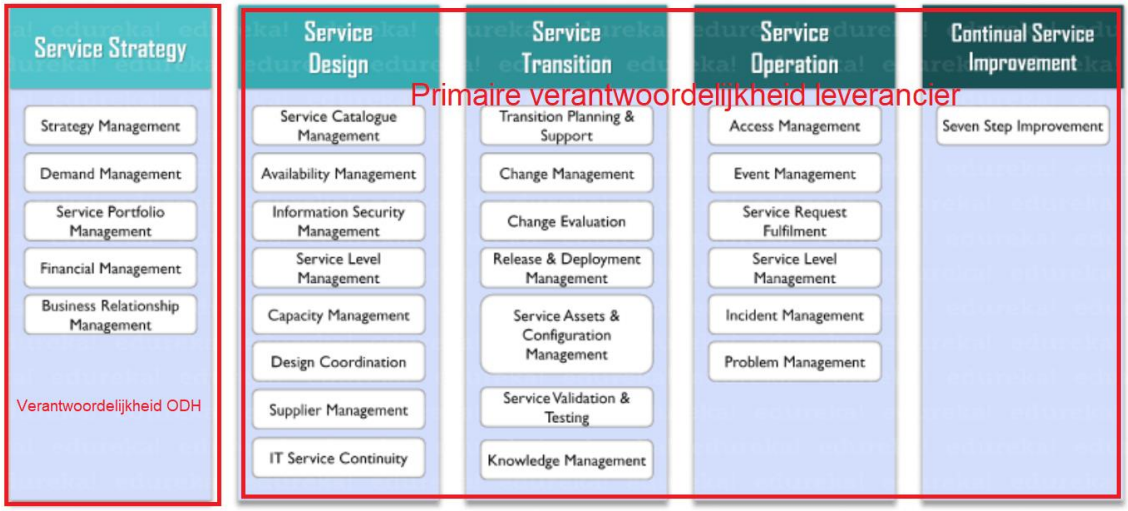
1) Service desk voor de ODH Azure cloudomgeving (basisvoorzieningen en workloads) door beheerpartij 2;
2) Service desk voor alle overige beheerdomeinen door beheerpartij 1;
3) Service desk voor het beheer van de on-premises firewall en VPN-configuraties door beheerpartij 3;
4) On site support door beheerpartij 1.

Daarnaast wordt regelmatig gebruik gemaakt van de service desks en supportkanalen van de leveranciers van de diverse SaaS diensten en applicaties. Deze dienstverlening wordt echter niet geleverd aan c.q. gebruikt door eindgebruikers.

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 echter essentieel dat in de nieuwe beheersituatie alle servicedesk 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 meldingen/wijzigingen waarbij meerdere leveranciers betrokken zijn. Van de nieuwe beheerpartij wordt verwacht dat zij binnen de incident- en problem management processen namens ODH als intermediair optreedt van en naar de verschillende leveranciers. ODH is en blijft zelf verantwoordelijk voor het contract- en service delivery management met al haar leveranciers.

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. Diverse andere processen moeten nog nader worden uitgewerkt.

Het is nu niet altijd duidelijk 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 het nieuwe beheercontract. 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 dat ODH wel de controle en regie behoudt en kan (bij)sturen op de uitvoering van de processen.

ODH hanteert momenteel de onderstaande incidentcategorieën en bijbehorende oplostijden:

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 streef-/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. Indien een RCA resulteert in een voorstel voor een structurele oplossing, dan wordt de structurele oplossing geïmplementeerd via het change management proces (indien nodig via spoed-changes).

Hieronder volgt een overzicht van het aantal meldingen (incidenten) en wijzigingen in 2022:

Globaal overzicht meldingen 2022 (niet genormaliseerd, wat betekent dat 1 grote verstoring al snel tot 50 à 100 incidentmeldingen geleid kan hebben):

Totaal aantal meldingen	: **5598**
Waarvan storingen	: 2845
Waarvan (gebruikers)vragen	: 2393
Waarvan standaardverzoeken	: 275
Waarvan security gerelateerd	: 69
Waarvan behoeften	: 16

Verdeling meldingen behandelgroepen 2022:

Afgehandeld door ODH (Functioneel beheer): 3050
Afgehandeld door externe beheerpartij(en) : **2548**

Verdeling meldingen prioriteiten storingsmeldingen (2845):

Prio 1 (service down)	: 10
Prio-2 (spoed)	: 13
Prio-3 (normaal)	: 2817
Geen prio toegekend	: 5

In het eerste half jaar van 2023 is het aantal incidentmeldingen met ca. 20% gedaald. De meeste meldingen in 2023 hadden betrekkingen op verstoringen die onbedoeld zijn veroorzaakt door changes en projectwerkzaamheden, zowel intern als door de externe beheerpartij(en). Door strakkere change management procedures en risico-analyses heeft ODH tot doel om ook in de tweede helft van 2023 het aantal incidentmeldingen met nog eens 20% te laten dalen.

Top 3 prio-1 verstoringen:

1. Fileshare (N-schijf) niet benaderbaar
2. AlwaysON VPN (thuiswerken) niet beschikbaar
3. Aanmelden op DMS (Alfresco) niet mogelijk

Typering overige meldingen en storingen:

- Wachtwoord resets
- Problemen met starten applicaties
- TimeTell: verzoeken tot aanpassen/wijzigen projectcodes
- Toekennen rechten op folders/mailboxen, etc.
- Uitgifte/inname/herstel laptops en telefoons (on-site support)

Wijzigingsverzoeken

Aantal wijzigingsverzoeken aangemeld in 2022 per (sub)categorie

Categorie	Subcategorie	Aantal en percentage	
Applicaties	AFAS Contractbeheer	7	3,15%
Applicaties	AFAS HRM	1	0,45%
Applicaties	AFAS Profit	55	24,77%
Applicaties	Alfresco	6	2,70%
Applicaties	Awaretrain	1	0,45%
Applicaties	BI	4	1,80%
Applicaties	Bodem Informatie Online	5	2,25%
Applicaties	EHerkenning	5	2,25%
Applicaties	Filecap	2	0,90%
Applicaties	I-Navigator	2	0,90%
Applicaties	IBABS	1	0,45%
Applicaties	IBIS	6	2,70%
Applicaties	InsightVM	1	0,45%
Applicaties	Kadaster	3	1,35%
Applicaties	LRSO	1	0,45%
Applicaties	Landelijk Grondwaterregister	1	0,45%
Applicaties	Myforms	2	0,90%
Applicaties	ODH website	1	0,45%
Applicaties	ODHINA	1	0,45%
Applicaties	Open.mail	1	0,45%
Applicaties	QGIS	4	1,80%
Applicaties	RAP	1	0,45%
Applicaties	Smart Privacy Analizer (SPA)	5	2,25%
Applicaties	Streetsmart - Cyclomedia	1	0,45%
Applicaties	TOPdesk	71	31,98%
Applicaties	Timetell Professional (BK)	8	3,60%
Applicaties	VIA	6	2,70%
Applicaties	Webformulieren	19	8,56%
Applicaties	WinHavik	1	0,45%
	Totaal Applicaties	**222**	**13,14%**

Basis IT	Account	425	68,88%
Basis IT	Bestandbeheer	109	17,67%
Basis IT	Internet	10	1,62%
Basis IT	Netwerk	19	3,08%
Basis IT	Office 365	13	2,11%
Basis IT	Server	23	3,73%
Basis IT	Software distributie	18	2,92%

Totaal Basis IT	**617**	**36,53%**

IT Werkplek	Docking station	3	23,08%
IT Werkplek	Laptop	2	15,38%
IT Werkplek	Muis	3	23,08%
IT Werkplek	Toetsenbord	5	38,46%
Totaal IT Werkplek		**13**	**0,77%**

Mail & Agenda	Mail (BK)	137	100%
Totaal Mail & Agenda		**137**	**8,11%**

OpenWave	Dataverbetering	632	92,40%
OpenWave	Koppeling DMS	1	0,15%
OpenWave	Overige	3	0,44%
OpenWave	Procesopbouw	1	0,15%
OpenWave	Sjablonen	44	6,43%
OpenWave	Versie Update	3	0,44%
Totaal OpenWave		**684**	**40,50%**

Telefonie	Mobiele telefoon	16	100%
Totaal Telefonie		**16**	**0,95%**

Totaal wijzigingen aangemeld in 2022	**1689**

1.10 Informatiebeveiliging en managed security operations (beheerdomein 10 in het diagram)

ODH heeft een interne Information Security Officer (ISO) die toeziet op het correct en volledig toepassen van het informatiebeveiligingsbeleid van ODH. De ISO stemt regelmatig af met de externe beheerpartijen over de actuele informatiebeveiligingsstatus van het ODH ICT-landschap. Het (door)ontwikkelen en implementeren van het ODH informatiebeveiligingsbeleid is een continu proces. Op sommige gebieden is het beleid nog niet volledig uitgewerkt. Dit ontslaat de beheerpartij(en) niet van hun plicht om de informatiebeveiliging conform algemeen geldende best practices toe te passen. Ook op dit vlak verwacht ODH een proactieve houding in de aanpak van beveiligingsincidenten en -maatregelen.

ODH beschikt over een eigen vulnerability management (scanning) oplossing van Rapid 7. Deze wordt ingezet naast de tools/oplossingen van de externe beheerpartij(en). Doel hiervan is om onafhankelijk van de beheerpartij(en) de beveiligingsstatus van de omgeving te kunnen vaststellen.

Door de scheiding van de beheerdomeinen en het beheer daarvan door meerdere partijen, processen en tools, is er geen integraal inzicht in de beveiligingsstatus van de ODH-omgeving als geheel. Ook de Rapid7 oplossing van ODH kan dit integrale beeld niet leveren. Een deel van de problematiek wordt nu bijvoorbeeld veroorzaakt door het gescheiden beheer van enerzijds Microsoft 365/Azure AD door de ene partij en anderzijds het beheer van de Azure omgeving door een andere partij. 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 vallen. ODH is dan soms zelf de partij die onvolkomen/kwetsbaarheden in de beveiliging signaleert. De toekomstige beheerpartij moet dit straks volledig onder controle hebben.

1.11 Governance, regie en innovatie (beheerdomein 11 in het diagram)

Het ODH IV-team zit nog midden in de transitie om haar regierol als service-broker tussen de externe leveranciers en de interne business organisatie te versterken. Er worden goede stappen gezet op gebied van contract- en leveranciersmanagement en ook de service delivery naar de interne business organisatie wordt verder geprofessionaliseerd. Daarnaast worden op gebied van informatie(beveiligings)beleid en compliance en risk management concrete stappen gezet.

Naast heldere contracten en SLA's, hecht ODH vooral ook grote waarde aan een goede samenwerkingsrelatie op basis van wederzijds vertrouwen en open en transparante communicatie. Dit gaat veel verder dan alleen het maandelijks controleren van de KPI's uit de SLA. De nieuwe beheerpartij moet op strategisch, tactisch en operationeel niveau een volwaardige gesprekspartner (willen) zijn en bereid zijn om daar (tijd) in te investeren. Op basis van regelmatige formele en informele gesprekken en evaluaties, wordt de dienstverlening en samenwerking doorlopend geoptimaliseerd. Dit werkt twee kanten op: ODH erkent dat zij zich nog aan het ontwikkelen is als regieorganisatie en staat zeker open voor feedback vanuit de leverancier(s) om haar eigen processen te verbeteren.

Vrijwel alle (priori)tijd en energie van het ODH IV-team wordt op dit moment besteed aan het dagdagelijks (functioneel) beheer om de ODH business zo goed mogelijk (24x7) te faciliteren. Hetzelfde geldt voor de externe beheerpartijen. De focus ligt vooral op instandhouding en minder op innovatie en modernisatie. ODH gaat haar IV-team (mogelijk) intern reorganiseren om meer ruimte te creëren voor innovatie. Dit zal voor een belangrijk deel om business innovatie gaan, maar ODH ziet op vlak van IT/IV-innovatie ook een rol weggelegd voor de nieuwe beheerpartij.

Zoals eerder aangegeven bieden clouddiensten potentieel de mogelijkheid om de time-to-market te bekorten c.q. sneller te innoveren. Het gaat daarbij niet alleen om puur technische innovatie, maar ook om business innovatie. Een belangrijk thema voor de ODH business is bijvoorbeeld dat zij meer datagedreven en geogeoriënteerd wil gaan werken, Dit raakt niet alleen de bedrijfsprocessen (en cultuur), maar heeft ook consequenties voor de IV-voorzieningen. Het huidige BI-dataplatform van ODH draait weliswaar in de Azure cloud, maar is in de basis nog gebaseerd op een traditionele BI-architectuur van meer dan 10 jaar geleden. Op dat moment waren thema's als data analytics en AI nog geen gemeengoed. ODH verwacht van de beheerpartij dat zij actief bijdraagt aan en meedenkt over (voor de ODH) innovatieve thema's zoals datagedreven werken en AI en de mogelijkheden en consequenties daarvan in kaart brengt.