

Visie PNB Cloud Platform Dienstverlening

Datum: 19 december 2024
Casenummer: C2338581

EIGENDOM EN VERTROUWELIJKHEID

De informatie in dit document is juridisch eigendom van en vertrouwelijk binnen Provincie Noord-Brabant. Het is niet toegestaan dit document te reproduceren, in welke vorm dan ook, mechanische of elektronisch, inclusief elektronische archiefsystemen, geheel of gedeeltelijk te uploaden en/of, al dan niet geautomatiseerd, te verwerken in of door middel van AI-tools, ongeacht het doel hiervan, zonder de schriftelijke goedkeuring van de Provincie Noord-Brabant.

Inhoudsopgave

Inhoudsopgave	2
1 Achtergrond en context.....	3
1.1 Provincie Noord-Brabant	3
1.2 PNB en IT	4
1.3 Highlights IT-organisatie.....	5
1.4 Highlights IT-sourcing strategie	5
2 Visie, doelstellingen en overall scope van de opdracht.....	6
2.1 Visie	6
2.1.1 PNB Azure Cloud.....	6
2.1.2 Azure Cloud Netwerk	8
2.1.3 PNB On-premises datacenter Den Bosch	8
2.1.4 Authenticatie en autorisatie management.....	8
2.2 Doelstellingen van de opdracht.....	9
2.3 Overall scope van de opdracht.....	9
2.4 Buiten de scope van de opdracht	9
2.5 Mogelijke aanvullende opdrachten (optioneel in scope)	9
3 Visie, scope en verwachtingen transitie.....	11
3.1 Visie	11
3.2 Scope	11
3.3 Verwachtingen	11
4 Visie, scope en verwachtingen Dienstverlening en Innovatie	13
4.1 Visie.....	13
4.2 Scope	13
4.3 Verwachtingen	15
5 Visie, scope en verwachtingen regie en samenwerking	19
5.1 Visie.....	19
5.2 Scope	20
5.3 Verwachtingen	20
6 Visie op informatiebeveiliging en privacy	22
6.1 Visie.....	22
6.2 Scope	23
6.3 Verwachtingen	23
7 Eisen.....	25
BIJLAGE: Architectuur bij PNB	31

1 Achtergrond en context

Provincie Noord-Brabant (hierna: PNB) is voornemens de dienstverlening voor het PNB Cloud Platform uit te besteden. Deze visie geeft deelnemers aan de aanbesteding inzicht in de gedachtegang van PNB en wat zij zoekt in de te leveren dienstverlening en de dienstverlener. Dit is opgedeeld in een korte beschrijving over PNB en de IT, een visie en beschrijving van het kavel, de doelstellingen en scope van deze opdracht en vervolgens per scope-onderdeel een meer gedetailleerde beschrijving van welke kwaliteitseisen gesteld worden en welke kwaliteitswensen PNB heeft. Bijlage 2 Huidige situatie geeft een uitgebreide beschrijving van de huidige situatie.

1.1 Provincie Noord-Brabant

PNB stáát voor Brabant en de Brabanders. In hun belang neemt de provinciale organisatie initiatieven om maatschappelijke vragen op te lossen. Die vragen liggen op het terrein van ruimte en wonen, natuur en milieu, water en bodem, veiligheid bestuur, economie, kennis en Talentontwikkeling, mobiliteit, energie, landbouw en voedsel, vrije tijd en erfgoed, economie, milieu, mobiliteit en vrije tijd.

Samen, slagvaardig en slim

SAMEN: PNB wil nadrukkelijker kijken of haar besluiten lokaal draagvlak hebben. Zij wil nauwer samenwerken met alle partijen in Provinciale Staten. Ze zoekt naar nieuwe manieren om ervoor te zorgen dat draagvlak onder de Brabantse bevolking nog meer de basis vormt voor haar besluiten, bijvoorbeeld via internetconsultaties en een correctief referendum.

SLAGVAARDIG: De focus ligt op doen. Als hier lokaal draagvlak voor is, versnelt PNB Noord-Brabant de realisatie van een aantal van onze belangrijke grote projecten.

SLIM: PNB zet in op technologische en sociale innovaties. Hierdoor ondersteunt zij niet alleen de Brabantse economie, zij stimuleert ook nieuwe oplossingen voor de maatschappelijke opgaven van vandaag en morgen.

Samenwerking

Dat doet PNB meestal niet alleen. Om haar ambities te halen wordt er veel samengewerkt met onder andere gemeenten, het Rijk, Europa en maatschappelijke instellingen.

Kennis en innovatie

Brabant is een Europese topregio op gebied van kennis en innovatie. Het bestuur van PNB investeert in Brabant om ook in de toekomst die topospositie te kunnen behouden. Want dankzij die topospositie is Brabant een prachtige provincie om in te wonen en te werken.

Kernwaarden

PNB stáát voor Brabant als kleurrijke, ondernemende en sociale provincie. In het verlengde van deze richtinggevendende visie zijn een aantal kernwaarden gedefinieerd. Afgesproken is dat alle activiteiten aan deze kernwaarden worden getoetst. Het betreft de volgende kernwaarden:

- **Verbindend**
Vanuit deze kernwaarde inventariseert PNB interne en externe belangen en brengt deze samen. Ze kijkt van buiten naar binnen, werkt samen met partners en stimuleert onderlinge samenwerking.
- **Doortastend**
PNB geeft invulling aan deze kernwaarde door een helder resultaat te formuleren en daarvoor te staan. Ze kiest de rol die kiest voor een maximaal resultaat, grijpt kansen en lost op.
- **Vernieuwend**
Deze kernwaarde staat voor een creatieve manier van werken. PNB staat open voor nieuwe ideeën, leert van zaken die niet goed zijn gegaan en verbetert permanent. Met haar aanpak is zij een voorbeeld voor anderen.
- **Betrouwbaar**
Ofwel: PNB zegt wat ze doet en doet wat ze zegt. Zij toont één gezicht naar buiten, is aanspreekbaar op haar woorden en daden en doet wat is afgesproken in resultaat en dienstverlening.

Dit wil PNB bereiken door samen, slagvaardig en slim te werk te gaan.

Meer informatie over PNB is te vinden op www.brabant.nl.

1.2 PNB en IT

PNB is een organisatie die constant in beweging is. Deze beweging wordt gevoed vanuit haar visie en ambitie, gestuurd door markt- en maatschappelijke ontwikkelingen, beïnvloed door politieke besluiten en geholpen door technische vernieuwingen. Deze veranderingen hebben sterke invloed op de manier waarop PNB kijkt naar IT en hoe zij e.e.a. vertaalt naar doelstellingen, een bijpassende strategie en het organisatie- en governance-model. PNB wil IT en het IT-landschap slagvaardiger, wendbaarder en veiliger maken voor al haar stakeholders.

Daarom richt PNB zich nu en de komende jaren met name op:

- Het naar de cloud brengen van het applicatie landschap.
- Data gedreven werken en het delen van data met externe samenwerkingspartners, zoals gemeenten, en burgers.
- Het verhogen van de cyberweerbaarheid met aandacht voor privacy door de sterke stijging van cybercriminaliteit.
- De toename van hybride werken: any time, any place, anywhere.
- Het verbeteren van de verduurzaming van technologie.
- “Alles as-a-Service” inclusief “betalen naar gebruik”.

PNB heeft de afgelopen jaren een snelle ontwikkeling doorgemaakt. Zo is onder andere werken onder architectuur geïnitieerd, ondersteund door de implementatie van Blue Dolphin met het doel inzicht te bewaren en snel te kunnen schakelen bij nieuwe projecten. Voor de belangrijkste dienstgebieden zijn visie en beleidsdocumenten opgesteld. Denk hierbij aan de *Cloud Visie* en *Cloud Governance*, inclusief *Financial Governance*, een *Werkplek Visie* en het backup beleid dat inmiddels grotendeels geïmplementeerd is. Daarnaast heeft PNB veel aandacht voor de inrichting van maatregelen rondom informatiebeveiliging, waar met inzet van nieuwe tooling de belangrijkste bedreigingen inmiddels worden afgedekt. Momenteel wordt hard gewerkt aan het verder vormgeven van het vervolgonderzoek, de analyse en, waar nodig, de opvolging van hieruit voortvloeiende acties.

Om klanten nog sneller te kunnen ondersteunen in hun wensen met migratie naar de cloud, is PNB gestart met een *Competence Center (CC)* wat onboarding ondersteunt en consultancy biedt.

Het PNB-doel is om voor alle dienstengebieden een duidelijke roadmap te hebben waarin zowel Life Cycle Management als toekomstige technologische ontwikkelingen zijn vastgelegd zodat deze ook in de uitvoeringsagenda meegenomen worden. Samen met de IT-dienstverleners wil PNB deze roadmaps opstellen en/of verder ontwikkelen. Met het doel blijvend betrouwbare diensten te leveren.

PNB is ambitieus en er is zeker nog veel te doen. Vooral op het gebied van het ondersteunen van data integratie, inzet van AI en van de koppelingen naar de dienstverleners en externe gebruikers. Ook zal binnen de IT-organisatie een verdere professionalisering worden doorgevoerd waar het gaat om de project- en beheeraanpak.

Naast de interne en IT-marktontwikkelingen houdt PNB ook rekening met andere factoren, waarvan, voor IT, wellicht een van de belangrijkste is te vinden in de maatschappelijk ontwikkeling: tekort aan gekwalificeerd personeel. PNB streeft ernaar om een aantrekkelijke werkgever. Op het gebied van IT zien we dat de zeer ervaren IT-specialisten de voorkeur geven aan werkgevers met continu sterk vernieuwende projecten. En hoewel PNB die ook heeft, gaat ook veel aandacht uit naar het borgen van de veiligheid en continuïteit van het IT-landschap. PNB werkt hierbij momenteel met een grote externe schil. Hierdoor hebben we juist de benodigde groep specialisten aan boord. PNB heeft de ambitie om, zodra duidelijk is welke rollen op de langere termijn nodig zijn, eigen specialisten in dienst te nemen.

De snelle ontwikkelingen, het tekort aan interne specialisten, de overgang naar cloud, SaaS en overige as-a-service diensten en de groei van outsourcing van IT-diensten heeft PNB overtuigd om de transitie naar een regieorganisatie door te zetten. En gelijktijdig zo veel als mogelijk haar standaard IT-dienstverlening uit te besteden aan gespecialiseerde marktpartijen. Partijen die bij uitstek geschikt zijn om diensten die voor PNB als gespecialiseerd worden gezien als standaard dienst te leveren. Dit maakt dat IT PNB zich kan richten op datgene waaraan ze werkelijk waarde toevoegt: “de business”.

Dit zal het IT-landschap en daarmee PNB slagvaardiger, wendbaarder en veiliger maken voor al haar stakeholders.

1.3 Highlights IT-organisatie

De huidige IT-organisatie van PNB heeft de verantwoordelijkheid voor IT-regie gecombineerd met verantwoordelijkheden op operationeel gebied. PNB wil haar IT-organisatie nog beter gaan positioneren als partner voor de business en heeft daarop haar structuur aangepast.

In de nieuwe structuur staat de regierol en de daarmee samenhangende activiteiten op het gebied van supply en demand management centraal. Activiteiten die geen relatie hebben met regie worden óf elders in de organisatie belegd, óf (op termijn) ondergebracht bij dienstverleners zodat de juiste focus gerealiseerd wordt.

De nieuwe regieorganisatie bestaat uit een vijftal onderdelen met een duidelijke focus:

1. *I-advies* vormt een belangrijke schakel tussen bedrijfsvoering en IT;
2. *Project- en programmamanagement* richt zich op de realisatie van projecten voor vernieuwing of verbetering van de dienstverlening;
3. Het *serviceteam cloud en Platformen* richt zich op de optimale inzet van de cloud- en Platform en netwerkomgeving;
4. Het *serviceteam digitale werkplek* richt zich op de werkplek en de servicedesk;
5. *Service- en contractmanagement* richt zich op servicemanagement en contract- en leveranciersmanagement evenals het licentiemanagement (SAM).

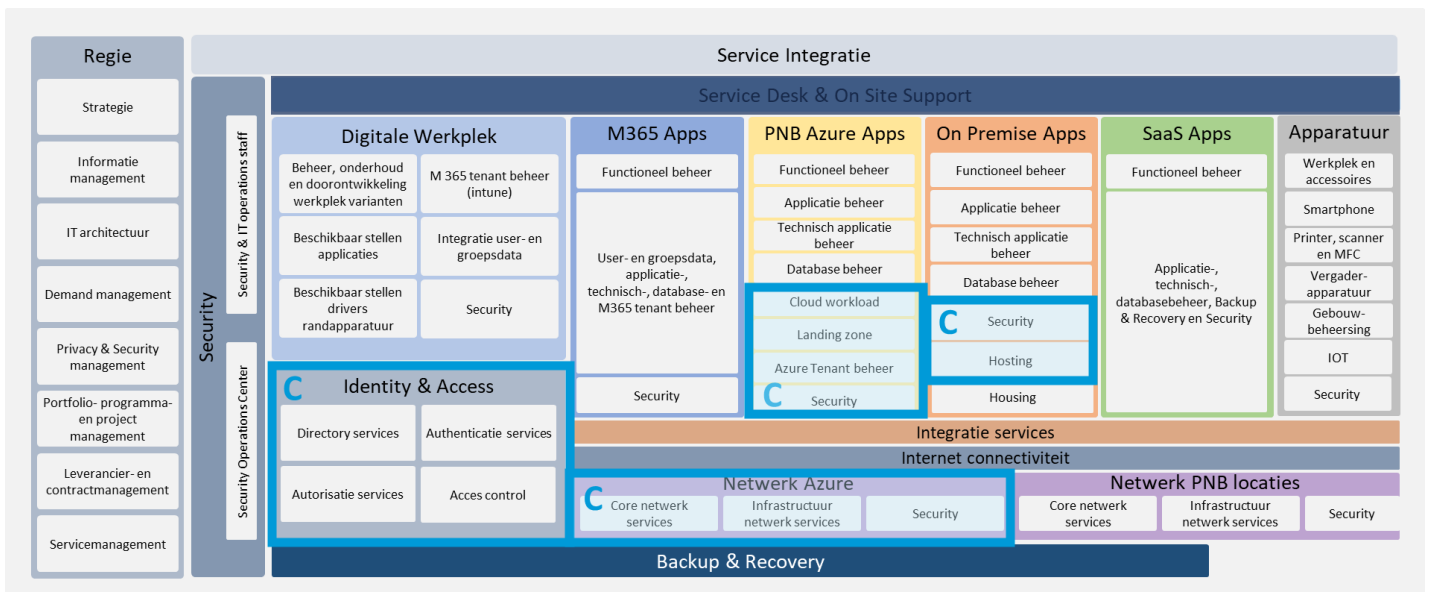
De invoering van de nieuwe structuur van de regieorganisatie is gestart in 2023 en het project loopt door tot 2025. Het project loopt parallel door aan deze aanbesteding en de transitie.

Om de bedrijfsvoering van PNB optimaal te ondersteunen is goede samenwerking cruciaal. De regieorganisatie is de verbindende schakel tussen de vraag uit de business en de diensten die door de dienstverleners geleverd worden. Over de regievoering en samenwerking geeft hoofdstuk 5 een nadere toelichting.

1.4 Highlights IT-sourcing strategie

PNB heeft in 2023 haar IT-sourcing strategie herijkt. De belangrijkste doelstelling hierbij is dat PNB maximaal overzicht, inzicht, rust en grip heeft en ze weet de “time-to-market” te verbeteren.

In de IT-sourcing strategie is, op basis van criteria, bepaald welke IT-werkzaamheden en diensten PNB zelf uitvoert en welke werkzaamheden en diensten bij specialistische dienstverleners belegd worden. Onderstaande afbeelding geeft aan welke onderdelen (kavels) PNB wil uitbesteden en welke zij zelf uitvoert:



Deze aanbesteding betreft kavel C (blauw omkaderde onderdelen), dat bestaat uit de dienstverlening met betrekking tot het PNB Cloud Platform.

2 Visie, doelstellingen en overall scope van de opdracht

2.1 Visie

PNB wil meer gebruik maken van clouddiensten in haar IT-landschap om:

- **De focus van IT-dienstverlening te verleggen naar primaire bedrijfsprocessen.** Dat betekent niet dat er géén oog is voor techniek. PNB wil ontzorgd worden op het vlak van operationele taken als onderhoud en dagelijkse monitoring van infrastructuur.
- **Gebruik te maken van de wendbaarheid en schaalbaarheid van de cloud.** Door gebruik te maken van de cloud is PNB in staat om de dienstverlening te versnellen en sneller en efficiënter nieuwe mogelijkheden te introduceren.
- **Connectiviteit te bieden naar iedereen:** Steeds meer derde partijen en overheidsinstanties hebben toegang nodig tot onze data en applicaties. Deze verschillende profielen kunnen het beste ontsloten worden via een publieke connectiviteitsstrategie. Uiteraard dient het veilig en volgens de richtlijnen van PNB gebeuren.
- **Autorisatie en authenticatie onder controle te hebben en houden.** Meerdere wet-, regelgeving en normenkaders (BIO, NIS2) eisen een autorisatieproces waarbij verantwoording afgelegd wordt over verschillende niveaus van toegang. Aan deze richtlijnen wil PNB-invulling geven door een goed gedefinieerde en geïmplementeerde Instroom-Doorstroom-Uitstroom (IDU) proces voor het managen van de identiteiten en gebruikersaccounts binnen PNB.

PNB loopt niet voorop op het gebied van werken in de cloud. PNB is vooral op zoek naar een stabiel platform. De innovatie ligt vooral op het vlak van uitwisselen van data met externe partijen en het voldoen aan de veiligheidsnormen en wetgeving van de overheid.

PNB onderkent de volgende onderdelen binnen dit kavel:

1. PNB Azure Cloud
2. Azure Cloud netwerk
3. PNB on-premises datacenter in Den Bosch
4. Authenticatie en autorisatie management

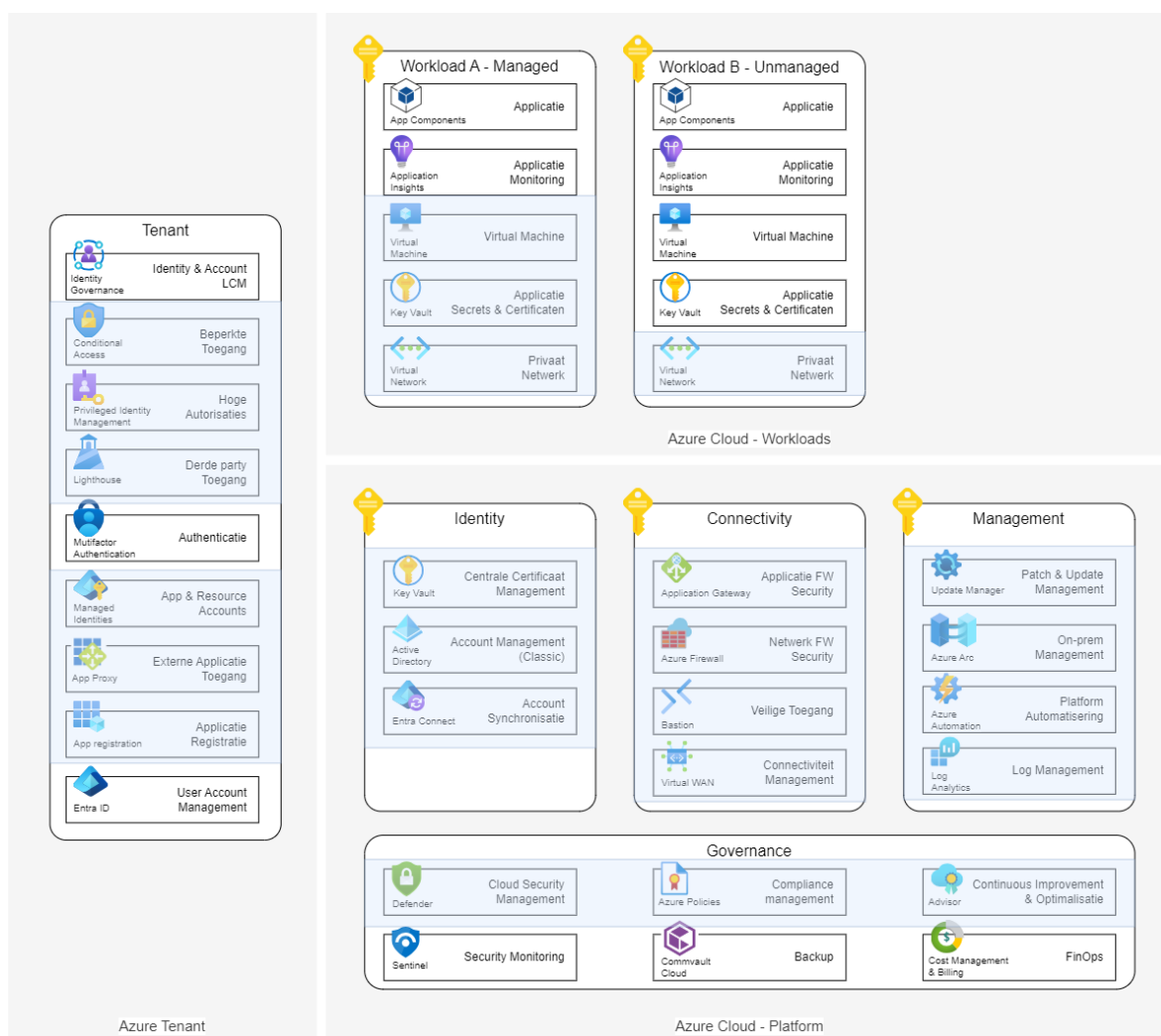
2.1.1 PNB Azure Cloud

De Azure Cloud omgeving binnen PNB is ingericht volgens het Microsoft Cloud Adoption Framework (CAF). Verder worden de vijf gebieden van de Azure Well-Architected Framework (WAF) gebruikt om de omgeving continu te verbeteren en de Microsoft best practices voor workloads dient als basis bij het uitrol van nieuwe omgevingen.

Op het platform worden workloads gehost. Deze workloads draaien elk in een landingzone. Een workload binnen PNB wordt gedefinieerd als een logische groepering van Azure resources *om een applicatie te laten draaien* voor een specifieke applicatie of omgeving. De verdeling heeft veelal met governance-afspraken te maken, zoals cost-management en toegang door derden. Een workload kan meerdere omgevingen hebben t.b.v. release management (OTAP).

De verschillende workloads zijn divers van aard. Er zijn workloads die primair bedrijfsapplicaties hosten en er zijn technische workloads ter ondersteuning van het IT-landschap (IT4IT). Traditionele applicaties die verhuisd zijn naar Azure zijn vooral IaaS gebaseerd en vormen het grootste deel van het PNB-landschap. Nieuwe workloads zijn vooral PaaS gebaseerd, zoals datawarehouse activiteiten en applicaties met koppelingen naar het Internet.

Sommige workloads worden beheerd door derde partijen of door PNB zelf. Van andere workloads wordt verwacht dat de cloud platform dienstverlener het beheer overneemt. In de toekomst wil PNB zowel landing zones af kunnen nemen van de dienstverlener zonder workload management, als landing zones inclusief workload management. Van de dienstverlener wordt verwacht dat hij het basis Azure Platform volledig in beheer heeft.



PNB is in een vroeg stadium gaan pionieren met en in Azure. Dit heeft de nodige waardevolle ervaringen opgeleverd over wat wel en niet werkt binnen PNB. Op dit moment ligt de focus op standaardisatie en optimalisatie van de eerste generatie workloads, in het bijzonder door versobering van de cloud configuraties en technieken, en optimalisatie van cost management. Ook zijn centrale diensten als connectiviteit en back-up ingericht binnen de omgeving. De Azure Cloud wordt binnen PNB het primaire Platform voor het hosten van workloads. Hierdoor zal het Platform een toenemende activiteit en optimalisatie zien in de komende jaren.

PNB kent momenteel circa 16 workloads verspreid over 33 subscriptions. De maandelijkse Azure spend is nu rond de 50.000 Euro. Er loopt een PNB-breed traject om applicaties van bestaande datacenterlocaties te migreren naar de Azure-omgeving. Het streven is dat de Azure-omgeving de primaire datacenterfunctie binnen PNB zal overnemen. Verder is het te verwachten dat de omgevingen zullen doorontwikkelen van IaaS naar PaaS. Hierdoor zal de Azure footprint toenemen, waarbij in 2025/2026 een toename van 120% van het aantal workloads wordt verwacht.

PNB gebruikt vanuit haar Azure-beleid Infrastructure-as-code om de verschillende componenten uit te rollen, hoewel dat nog niet overal gestandaardiseerd is. Azure DevOps wordt ingezet om Infrastructure-as-code (IAC) te huisvesten. Deze code is onderdeel van de workload. De code dient dus aan alle eisen van de applicatie/workload te voldoen (change management, autorisatie management, enz.).

PNB heeft een eigen Enterprise Agreement met Microsoft en zal de Azure-kosten direct zelf dragen (geen CSP). PNB voorziet dat de dienstverlener alle beheerwerkzaamheden binnen de tenant van PNB uitvoert met tooling vanuit de PNB-omgeving.

2.1.2 Azure Cloud Network

PNB kent als onderdeel van haar communicatie van en naar de verschillende workloads een uitgebreid Azure netwerk. Deze diensten in de PNB Azure Cloud zijn gebaseerd op een hub-spoke architectuur die de volgende verdeling kent:

- Core netwerkservices
- Netwerk infrastructuur en security resources

Momenteel maakt PNB nog gebruik van het Equinix datacenter en is een ExpressRoute tussen dit datacenter en Azure noodzakelijk. De overgang van het PNB-applicatielandschap van on-premise in Den Bosch en verschillende diensten in het Equinix datacenter (verwachting Q4 2025) naar de Azure cloud zorgt voor een versimpeling van de benodigde netwerkstructuur, waardoor de communicatie wordt beperkt tot communicatie binnen de cloudomgeving. Voor het restant aan on-premise communicatie zal een site-to-site connectie worden ingebouwd. Gezien de te verwachten ingangsdatum van de nieuwe overeenkomst, gaat PNB ervan uit dat de ExpressRoute nog onderdeel van de PNB-omgeving uitmaakt op moment van contracteren van de cloud platform dienstverlener. De bestaande ExpressRoute valt niet binnen de scope van deze opdracht. Het beheer van de verbinding tussen het PNB on-premises datacenter in Den Bosch en Azure wordt een gedeelde verantwoordelijkheid tussen de dienstverlener van dit kavel en netwerkbeheer in Den Bosch.

2.1.3 PNB On-premises datacenter Den Bosch

De huidige on-premises datacenters van PNB omvat drie locaties: één DC in Den Bosch (eigen bezit) en twee bij Equinix (AM3 in Amsterdam en ZW1 in Zwolle). De locatie in Den Bosch huisvest momenteel de meeste infrastructuur, waaronder de netwerk- en server hardware voor applicatiehosting en alle ondersteunende diensten. De meeste servers zijn gevirtualiseerd (VMware), er zijn ongeveer 40 host machines met centrale opslag (SAN). De Equinix datacenters worden momenteel ontmanteld en zijn niet meer in gebruik op moment van contracteren van de cloud platform dienstverlener.

Het doel van de on-premise datacenter in Den Bosch verandert in de komende 3 – 5 jaar. Alle applicatiehosting en ondersteunende diensten worden gemigreerd naar de Azure PNB Cloud. Echter blijft er infrastructuur t.b.v. locatie afhankelijke diensten (bijvoorbeeld gebouwbeheersystemen) en een netwerkinfrastructuur voor connectiviteit op locatie Den Bosch aanwezig. Alle server-, storage- en hosting-infrastructuur (niet zijnde netwerkinfrastructuur) in Den Bosch die nog niet afgebouwd zijn of gemigreerd naar cloud varianten moeten in beheer genomen worden als onderdeel van deze uitvraag.

2.1.4 Authenticatie en autorisatie management

Voor toegang tot Azure resources wordt van Microsoft Entra ID gebruik gemaakt als bron voor authenticatie en autorisatie binnen de PNB cloud omgevingen. PNB verwacht dat deze *Identity Provider* (IDP) uiteindelijk wordt gebruikt als centrale spil voor alle vormen van authenticatie en autorisatie binnen PNB, maar ook voor het reguleren van toegang door derden.

Verder is er een klassieke Active Directory on-premise in gebruik. Deze directory wordt momenteel ingezet voor authenticatie en autorisatie van gebruikers binnen applicaties zowel in de Den Bosch als in de PNB Azure Cloud.

Binnen het landschap onderkent PNB de volgende type toegang op resources:

- Interactieve toegang voor standaard gebruikers
- Interactieve toegang voor beheerders
- Niet-interactieve toegang voor applicaties en processen

Deze vormen van toegang worden binnen Azure ingevuld door Entra ID gebruikersaccounts voor type (a) en (b), Service Principals (SP) en Managed Identities (MI). Momenteel wordt het on-premise ingevuld door accounts vanuit een traditionele Active Directory. PNB verwacht dat deze accounts tijdens de migratie van de workloads uit de on-premises datacenter naar de Azure Cloud omgezet worden naar Entra ID-gebaseerde credentials.

Zoals aangegeven is de traditionele Active Directory de primaire bron voor gebruikersaccounts gebruikt. Deze accounts worden gesynchroniseerd naar Entra ID. De synchronisatie zal dan niet meer naar Entra ID gaan,

maar komt juist van Entra ID. Provisioning van eindgebruikers en functioneel beheer van autorisaties voor eindgebruikers vallen buiten scope van deze kavel. Er is binnen PNB eind 2024 een apart project gestart voor het inrichten van RBAC en autorisatiemanagement voor eindgebruikers.

Binnen de verschillende applicaties zijn meerdere vormen van authenticatie in gebruik, waaronder Service Principals met wachtwoorden (*secrets*) en Managed Identities vooral voor toegang tussen de verschillende Azure resources en certificaten. Laatstgenoemde wordt in laatstgenoemde scenario ingezet voor authenticatie, maar kan natuurlijk ook ingezet worden voor encryptie. De visie van PNB is dat deze security artefacten binnen een beheerde Azure keyvault infrastructuur ondergebracht worden, met periodieke rollering van alle secrets en tijdig lifecyclemanagement voor certificaten.

Hoge autorisaties binnen Azure worden momenteel met een Role Based Access Control (RBAC) model binnen Privileged Identity Management (PIM) vanuit Entra ID beheerd. Per workload wordt de applicatie eigenaar functioneel verantwoordelijk gesteld voor de autorisaties binnen een landing zone. De technische uitvoering van de verschillende rollen komen bij de beherende partij van de betreffende landingzone vandaan.

2.2 Doelstellingen van de opdracht

Met deze aanbesteding zoekt PNB een partner die invulling geeft aan:

1. Het overnemen van de dienstverlening van de PNB Azure Cloud, de server en opslag infrastructuur binnen het PNB on-premises datacenter in Den Bosch, het Azure netwerk en Authenticatie en Autorisatiemanagement, zonder onderbreking, van de huidige dienstverlener.
2. Het inrichten van de dienstverlening in overeenstemming met het overeengekomen samenwerkingsmodel, de processen en servicelevels.
3. Zijn verantwoordelijk voor het beheer en de continue doorontwikkeling van de PNB Azure Cloud, het PNB on-premises datacenter, het Azure netwerk en Authenticatie en Autorisatiemanagement helpt vorm te geven. Dit omvat het borgen van de beschikbaarheid, veiligheid en continuïteit van deze applicaties, inclusief de bijbehorende Azure resources zoals vm's, vnets, storage accounts, enz. Hierbij wordt het beleid uit de PNB Cloud Governance nageleefd en afgedwongen.
4. Operationele processen zoals incidentafhandeling, regulier onderhoud en monitoring van alle bestaande resources. Ondersteuning bij nieuwe workloads in de Azure Cloud omgeving van de PNB moet mogelijk zijn.
5. Het leggen van de basis van een samenwerkingsverband waarin wederzijds waarde wordt gecreëerd door het werken aan kwaliteit, continue verbeteringen en innovatie. Transparantie is het uitgangspunt van de samenwerking.

2.3 Overall scope van de opdracht

Om bovenstaande doelstellingen te bereiken, is voor deze aanbesteding een scope gedefinieerd. Op het hoogste niveau bestaat deze uit:

1. Transitie; het overnemen van de dienstverlening van de huidige dienstverlener en PNB en het inrichten van het beheer conform de geëiste en overeengekomen SLA/DAP.
2. Beheren en door ontwikkelen het PNB cloud platform.
3. Innovatie gericht op het samen, op basis van mogelijke nieuwe functionaliteit en nieuwe applicaties, doorontwikkelen van het landschap

Deze scope is verder in detail uitgewerkt in onderstaande visie-hoofdstukken: Transitie, Dienstverlening en Innovatie, Governance en Samenwerking en Informatiebeveiliging.

2.4 Buiten de scope van de opdracht

De volgende diensten vallen buiten de scope van de opdracht:

1. Eerstelijns beheer
2. Licentie- of hardware broker
3. Microsoft contract: er zal gebruik gemaakt worden van de PNB Enterprise Agreement

2.5 Mogelijke aanvullende opdrachten (optioneel in scope)

In de nabije toekomst wil PNB mogelijk de volgende extra diensten afnemen bij de cloud platform dienstverlener:

1. AVD deployment.

De inzet van AVD deployment is afhankelijk van de nog op te stellen werkplek visie en de daaraan voorafgaande marktconsultatie voor het kavel Digitale werkplek. PNB heeft op het cloud platform vier verschillende AVD's draaien. Het is op het moment van aanbesteden niet duidelijk of het logischer is deze AVD's automatisch vanuit het cloud platform te deployen (en dus binnen de cloud platform dienstverlening) i.p.v. het onder te brengen in de dienstverlening van het nog aan te besteden kavel Digitale werkplek.

Medio 2025 zal een marktconsultatie rondom het kavel Digitale werkplek plaatsvinden en zal de informatie uit de markt t.a.v. o.a. AVD deployment en de keuze in welke kavel dit het beste tot zijn recht komt, worden gemaakt. Indien de marktconsultatie en daarmee de keuze van AVD deployment leidt tot het onderbrengen in de onderhavige opdracht kan de omvang van de overeenkomst worden verhoogd met € 120.000,- per jaar. Deze extra opdracht heeft geen invloed op de overige uitvoeringsvoorwaarden die daarmee gelijk blijven aan hetgeen in deze procedure is vastgesteld. De aard van de opdracht blijft daarmee hetzelfde.

2. Microsoft Azure API management.

PNB is onlangs gestart met het definiëren van zijn integratie services behoefte. Dit is een traject dat een langere doorlooptijd kent. Definitieve besluitvorming wordt einde 2025 verwacht, waarna deze dienstverlening middels een aanbesteding wordt geoutsourcet. PNB gaat ervan uit dat 2^e helft 2026 kan worden overgegaan tot gunning, zodat deze optie, indien die wordt gelicht, voor maximaal 2 jaren zal worden gecontracteerd.

Momenteel zijn er diverse API-koppelingen in gebruik t.b.v. communicatie tussen en integratie met applicaties op het Azure cloud platform. Zonder dat deze koppelingen nu worden gemonitord en beheerd. Indien deze optie wordt gelicht zal de dienstverlener verantwoordelijk zijn voor het monitoren van de API-koppelingen en het signaleren van niet juist functionerende koppelingen.

Indien besluitvorming over integratie services wordt gemaakt nadat de transitie van de Cloud Platform aanbesteding is afgerond en de keuze leidt tot het onderbrengen van Azure API management in de onderhavige opdracht, kan de omvang van de overeenkomst voor een periode van maximaal 2 jaar worden verhoogd met maximaal € 60.000,00 per jaar. Deze extra opdracht heeft geen invloed op de overige uitvoeringsvoorwaarden die daarmee gelijk blijven aan hetgeen in deze procedure is vastgesteld. De aard van de opdracht blijft daarmee hetzelfde.

3. Innovatie

PNB heeft een sterke behoefte aan een cloud platformdienst waarop continu wordt geïnnoveerd en doorontwikkeld door de dienstverlener. Standaard wijzigingen in de dienst van de dienstverlener en standaard wijzigingen zoals die door Microsoft worden doorgevoerd (ook wel "update" genoemd) vallen in de reguliere dienstverlening en daarmee in het standaard beheertarief. Daar staat tegenover dat de grote impactvolle functionele wijzigingen die een projectmatige aanpak vereisen optioneel in scope zijn en worden gefinancierd vanuit het daarvoor geoormerkte Innovatie-budget. Onder impactvolle functionele wijzigingen wordt verstaan: Microsoft Azure diensten als onderdeel van de Azure product catalog (services) die nog niet in de PNB-omgeving zijn geïmplementeerd of nog niet door Microsoft ter beschikking zijn gesteld op het moment van contracteren en die een projectmatige aanpak vereisen voor een succesvolle implementatie. Voorbeelden: Mixed Reality en IoT.

Op voorhand is voor PNB niet te voorzien welke grote functionele wijzigingen door met name Microsoft zullen worden geannonceerd, of die überhaupt relevant en interessant zijn voor PNB, of er voldoende resources beschikbaar zijn om de innovatieprojecten uit te voeren en of er nog voldoende innovatie-budget in het betreffende jaar beschikbaar is. Gedurende de looptijd van het contract zal dienstverlener PNB informeren over potentiële innovatieprojecten en de toegevoegde waarde voor PNB. Aan de hand hiervan zal PNB besluiten of: a) het potentiële project relevant is dan wel voldoende waarde toevoegt, b) er voldoende resources zijn om het project succesvol uit te kunnen voeren, c) er voldoende budget resteert en d) er een bij de verwachtingen van PNB passend voorstel tot implementatie en uitvoering is uitgebracht.

Is aan al deze voorwaarden voldaan kan de omvang van de overeenkomst worden verhoogd door het in opdracht geven van één of meer van deze projecten voor maximaal € 350.000,- per jaar voor contractjaren 1 en 2. en voor maximaal € 100.000,- voor de daaropvolgende contractjaren. Deze extra opdracht heeft geen invloed op de overige uitvoeringsvoorwaarden die daarmee gelijk blijven aan hetgeen in deze procedure is vastgesteld. De aard van de opdracht blijft daarmee hetzelfde.

3 Visie, scope en verwachtingen transitie

3.1 Visie

PNB ziet de transitie als een stapsgewijze aanpak met als stap 1 de as-is overname van de huidige dienstverlening en de bestaande inrichting van het platform en stap 2 het inrichten van de gevraagde dienstverlening en samenwerking door de dienstverlener. Het betreft een 'brownfield' situatie waarbij de dienstverlener doorontwikkelt op basis van de bestaande inrichting.

De overname van de dienstverlening van de huidige dienstverlener moet probleemloos en zonder noemenswaardige verstoringen verlopen.

De transitieperiode start met een kickoff waarin alle direct betrokkenen van de dienstverlener, PNB en derde partijen elkaar leren kennen. Hierin wordt tevens de aanpak voor de transitie geschetst zodat iedereen een duidelijk beeld heeft van de aanpak, planning en wat van hem of haar verwacht wordt.

Technische documentatie, kennis over specifieke toepassingen en inzicht in lopende problemen en (openstaande) verbeterpunten vormen vanuit de huidige partij(en) belangrijke input voor een succesvolle transitie. Van de dienstverlener verwacht PNB dat deze voorafgaand aan de transitie een gedegen verificatie doet van het bestaande 'cloud-landschap' en vervolgens tijdens de transitie de lead neemt in het 'in control' komt over de voor de dienstverlening relevante kennis en documentatie en deze waar nodig updatet. Tevens verwacht PNB dat de dienstverlener de acties neemt om (openstaande) verbeterpunten op te lossen en dienstverlening conform SLA te kunnen garanderen als de transitie wordt afgerond.

De transitie wordt aangepakt op basis van een vooraf vastgestelde methodiek (bijvoorbeeld Prince2) met beheersing van doorlooptijd, kwaliteit, budget en risico's. Hierbij is de governance duidelijk en voor alle betrokkenen inzichtelijk wat van hen wanneer verwacht wordt.

Voor de start van de transitie is duidelijk wat de deliverables inclusief acceptatiecriteria per fase zijn. De deliverables bestaan o.a. uit projectmanagement-, technische-, dienstverlening, governance en samenwerking producten. De deliverables worden getest op basis van het beschreven testproces.

De samenwerking en het gereed zijn voor in beheername wordt in de praktijk, met alle betrokken partijen (latende, ontvangende en PNB), getest door middel van dry-runs met vooraf overeengekomen scripts en acceptatiecriteria. Pas als uit de dry-runs blijkt en alle partijen aangegeven hebben gereed te zijn voor de beheerfase vindt overdracht naar de beheerorganisatie plaats.

Decharge vindt plaats na in beheername en overeenstemming van eventuele restpunten in de in te richten stuurgroep.

3.2 Scope

Tot de scope van de transitie behoort:

1. As-is overname van het huidige beheer.
2. Inrichten van de gecontracteerde dienstverlening en verantwoordelijkheid van alle onderdelen in scope van het PNB uitgevraagde diensten
3. Optimaliseren van de dienstverlening d.m.v. automatisering.
4. Inrichten en operationaliseren van de organisatie, governance en samenwerking voor de beheer- en doorontwikkelfase.
5. Koppelen van ITSM-tooling.
6. Overnemen en actualiseren van beheer, designs en inrichtings-documentatie.

3.3 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van de transitie het volgende:

1. Gedegen aanpak

PNB verwacht een gedegen aanpak waarmee de dienstverlener invulling geeft aan:

- a) De doelstellingen en scope en resultaten van het traject;
- b) Een duidelijke aanpak met onderscheid in:
 - Fasen met bijbehorende tijdslijnen van het traject;
 - Transparante faseovergangen;

- Dechargemomenten waarbij sprake is van een zorgvuldige voorbereiding van de inbedding en overgang;
 - Voldoende aandacht voor kennismaking van PNB en haar organisatieonderdelen;
 - Acceptatiecriteria en acceptatieproces;
 - Verificatie/validatie (inclusief afwijkingenproces van de aannames gedaan bij de inschrijving);
 - Vastgestelde deliverables met heldere en realistische acceptatiecriteria
- c) De wijze waarop de bovenstaande scope onderdelen van de transitie worden gerealiseerd.
 - d) De wijze waarop dienstverlener zorgdraagt dat de kennis en ervaring die over PNB wordt opgedaan tijdens dit traject, gedurende de looptijd van het contract zowel binnen de organisatie (en de ingezette medewerkers) van de dienstverlener geborgd blijft.
 - e) Duidelijke en realistische randvoorwaarden, aannames en beperkingen waarbij dienstverlener een actieve rol neemt om samen met PNB en andere partijen invulling te geven aan een succesvolle transitie, inclusief het afwijkingenproces indien blijkt dat randvoorwaarden, aannames en beperkingen afwijken.
 - f) Een duidelijke governance in het plan van aanpak op operationeel, tactisch en strategisch niveau, met onder andere een stuurgroep.
 - g) Afhankelijkheden met andere lopende projecten en het nog op te stellen retransitieplan van de huidige dienstverlener;
 - h) Belangrijkste risico's en mitigerende maatregelen inclusief een actief kwaliteits-, risico- en issue managementproces (voor zowel risico's die binnen als buiten de directe invloedssfeer van dienstverlener liggen).

2. Optimaliseren dienstverlening

PNB verwacht dat de huidige dienstverlening wordt geoptimaliseerd alvorens over te gaan naar FMO, zodat zo veel mogelijk is geautomatiseerd zoals oa het beschikbaar stellen VM, etc, en standaard wijzigingen automatisch kunnen worden uitgevoerd conform SLA.

PNB verwacht dat de dienstverlener een overzicht deelt van de minimaal te automatiseren activiteiten/processen in de transitie periode welke onderdeel zijn van het transitiebudget. De transitieperiode is zo kort als mogelijk met een beperkte freeze-periode, waarbij kwaliteit van procesinrichting en continuïteit van de dienstverlening centraal staan.

3. Intensieve samenwerking

De wijze waarop, conform de visie in hoofdstuk 5, tijdens dit traject intensief wordt samengewerkt met een duidelijke afbakening in rollen en verantwoordelijkheden van en tussen de dienstverlener, het PNB-team, de latende partij en andere betrokken dienstverleners. Dienstverlener maakt duidelijkheid wanneer welke en hoeveel inzet wordt verwacht van eenieder.

4 Visie, scope en verwachtingen Dienstverlening en Innovatie

4.1 Visie

PNB streeft naar een wendbare en betrouwbare IT-omgeving voor haar interne organisatie, inwoners en voor externe partijen. PNB is geen vooroploper op het gebied van werken in de cloud, maar ze is vooral op zoek naar een stabiel platform. De innovatie ligt op dit moment vooral op het vlak van uitwisselen van data met externe partijen en het voldoen aan de veiligheidsnormen en wetgeving van de overheid. Heldere afspraken over producten, diensten en kwaliteitsniveaus ziet de PNB hiervoor als essentieel.

PNB zoekt daarom een dienstverlener die zich verantwoordelijk voelt voor het leveren van de stabiele PNB cloud omgeving en dit in de praktijk ook realiseert. Een partij die er alles aan doet om verstoringen te voorkomen en die ze, als zich toch verstoringen voordoen, zo spoedig mogelijk op basis van afgesproken servicelevels oplost. Een dienstverlener die bij nieuwe verzoeken of wijzigingen adequaat adviseert en snel acteert. Hierbij is het van belang dat de dienstverlener meedenkt, proactief opereert en continu de kwaliteit bewaakt. Voorbeelden van vragen die hij zich dient te stellen zijn bijvoorbeeld: 'Is deze aanvraag voor de change wel compleet?', 'Bereikt PNB wel wat zij wil bereiken?', 'Kan die nieuwe functionaliteit niet kostenefficiënter?' 'Wordt voldaan aan alle randvoorwaarden uit de Azure governance?'.

Van dienstverlener wordt verwacht zich blijvend te verdiepen in de bedrijfsprocessen van PNB, startend bij de transitie en ook doorlopend tijdens de verdere contractperiode. Hierdoor begrijpt de dienstverlener wat de impact van de dienstverlening en verstoringen is op de PNB-bedrijfsvoering en operationele impact op de omgeving.

De dienstverlening wordt nader vastgelegd in o.a. een Service Level Agreement (SLA) en in het Dossier van Afspraken en Procedures (DAP) waarin minimaal aan bod komen: duidelijke en meetbare KPI's, de governance, de roadmap en heldere rapportages. PNB wil, waar mogelijk, aansluiten bij de standaard SLA van de dienstverlener. Voor PNB specifieke afwijkingen wordt in overleg met de dienstverlener beoordeeld of deze echt noodzakelijk zijn.

De PNB cloud omgeving en daarmee de gevraagde dienstverlening is sterk in beweging door het aanbod van nieuwe mogelijkheden en integraties van oplossingen. Dat maakt het bepalen wat in/uit scope van de dienst is niet eenvoudig. Zeker is dat we als PNB zo veel mogelijk ontzorgd willen worden. Daar hoort ook bij het samen met de dienstverlener uitwerken van wat nu standaard in de dienst zit en wat gezien wordt als toekomstige (door)ontwikkelingen of impactvolle innovaties. Standaard wijzigingen in de dienst van de dienstverlener en standaard wijzigingen zoals die door bijvoorbeeld Microsoft worden doorgevoerd vallen in de reguliere dienstverlening en daarmee het standaard beheertarief. Daar staat tegenover dat de grote impactvolle (functionele) wijzigingen die een projectmatige aanpak vereisen onder innovatie vallen. Omdat op voorhand niet te voorzien is welke grote veranderingen zullen volgen en of die überhaupt relevant en interessant zijn voor PNB, heeft PNB voor de duur van de overeenkomst een innovatie-budget PNB cloud platform vastgesteld (zie selectieleidraad voor hoogte).

4.2 Scope

Tot de scope van de dienstverlening en innovatie behoort:

1. Reactief en proactief beheer en onderhoud van het PNB (cloud en on premise) platform op een zo hoog mogelijke automatiseringsgraad, inclusief het uitvoeren van service requests, changes en het uitrollen van nieuwe application landing zones en Azure resources.
2. Transparante en periodieke rapportages (bij voorkeur middels real time/near real time dashboards) over de dienstverlening gebaseerd op de SLA en KPI's, performance en capaciteit inclusief verbetervoorstellen.
3. Opstellen van roadmaps voor de Azure en on-premise omgeving, op basis van ontwikkelingen vanuit de markt en relevant voor PNB.
4. Implementeren van Microsoft ontwikkelingen die op basis van push vanuit Microsoft geleverd worden.
5. Resources en application landingzones worden binnen de PNB Azure Cloud geautomatiseerd uitgerold op basis van gestandaardiseerde sjablonen. Deze processen en componenten zijn ook onderhevig aan lifecycle management. Deze LCM werkzaamheden zijn onderdeel van de standaard dienstverlening.

6. Op verzoek van PNB in beheer nemen van nieuwe cloud workloads (ten behoeve van een applicatie). Hiervoor is een transparant kostenmodel overeengekomen.
7. Implementeren nieuwe impactvolle functionaliteit binnen het Microsoft Azure cloud gerelateerde producten (onderdeel van innovatie-budget).
8. Implementeren nieuwe impactvolle functionaliteit anders dan Microsoft t.b.v. cloud platform (onderdeel van innovatie-budget).
9. Huidige workloads vanuit on-premise naar Azure verhuizen (onderdeel van innovatie-budget).
10. Ontwerp, testen en implementeren van nieuwe applicaties binnen de dienst Azure cloud platform (onderdeel van innovatie-budget).
11. Deelnemen en actief bijdragen aan de verbetering van de (Azure) governance zodat deze voldoet aan de randvoorwaarden voor beheer vanuit de dienstverlener.
12. Aansturen van PNB en/of partners binnen het PNB cloud platform en samenwerken met PNB en/of partners buiten het PNB cloud platform zoals beschreven in hoofdstuk 5.
13. Opstellen, up-to-date houden en beschikbaar stellen van de documentatie, CMDB en architectuurdesigns (HLD / LLD) van alle onderdelen van Azure Platform en landing zones, PNB on-premise datacenter, het Azure Network en Authenticatie en Autorisatiemanagement. HLD's worden binnen PNB door de Design Authority beoordeeld en kunnen niet eerder worden uitgevoerd dan na akkoord. Indien er afwijkingen van het beleid zijn zullen deze worden voor gelegd aan de PNB architectuurboard. Implementeren en bewaken van de van toepassing zijnde security en compliancy eisen en voldoen aan eisen en aansluitvoorwaarden gesteld vanuit de SOC-dienstverlening, inclusief audit en rapportage.
14. Microsoft Premier Support for Partners, ter vervanging van het momenteel lopende Microsoft Unified Support contract.

In meer detail behoren onder andere de volgende onderdelen van het PNB Cloud Platform¹ tot de scope:

PNB Azure Cloud	• Azure tenant beheer (management groups, subscription structuur, policies, Azure governance) • Beheer en onderhoud van de centrale componenten en van Azure resources in landingzones, denk aan: - Deployment and Maintenance - Networking - Managed environment configuration - Monitoring en alerting van de Azure componenten - Provisioning - Incident Management - Change management - Problem Management - Security Management - Patch Management - Continuity Management - Reporting - Service Request Management - Managed Firewall - Asset en configuration management • Gezamenlijk opstellen van designs voor nieuwe landingszones en workloads. • Aansluiten van workloads op de bestaande backup voorziening i.o.m. PNB backup dienstverlener. • Aansluiten van logging vanuit workloads op de bestaande SIEM voorziening (Sentinel) • Cost Management, o.a.: (re-)sizing, tagging, kosteninschattingen, optimalisaties, monitoring en signaleren. • Input leveren voor changes en requests (logische architectuur, sizing inschatting o.b.v. Azure Calculator).
Azure Netwerk	• Technisch beheer en onderhoud van Azure netwerk infrastructuur (vwan, Azure FW, VPN, enz) • Het (door) ontwikkelen en verbeteren van de Azure netwerk infrastructuur • Monitoring van netwerkcomponenten

¹ Daar waar gesproken wordt over de dienst PNB cloud en platform worden minimaal alle diensten/objecten bedoeld zoals weergegeven in de tabel op pagina 13.

	• Technisch en functioneel beheer van firewall rules voor workloads (Azure FW, App Gateway), inclusief certificate management waar nodig • Technisch beheer van 3e partij toegang (VPN, Bastion, Lighthouse) • Aansluiten van logging vanuit netwerkcomponenten op de bestaande SIEM voorziening (Sentinel) • Beheren verbinding tussen het datacenter in Den Bosch en Azure
PNB on-premise datacenter	• Technisch beheer hardware platform - Servers (Dell) - Storage Area Network (SAN) inclusief opslag (disks) • Hypervisor management (VMware) • Monitoring van de infrastructuur (servers en storage) • Besturingssysteem beheer (LCM, patch en update management) • Technische ondersteuning m.b.t. infrastructuur t.b.v applicatie teams • Technische ondersteuning voor 3e partijen (bijvoorbeeld back-up dienstverlener, SOC) • Verzorgen backup in de backup omgeving van PNB in samenwerking met de door PNB gecontracteerde backupdienstverlener
Authenticatie en Autorisatie	• Technisch beheer van de PNB directory services voor zowel Active Directory als Entra ID. • Inrichten toegang, gebruikersrechten en autorisaties m.b.t. Azure resources. • Beheren van applicatieve toegang tot systemen, inclusief service principals en managed identities • Beheren van certificaten, secrets en credentials m.b.t infrastructuur (Azure en On-Premise) • Technisch en functioneel beheer PKI infrastructuur
Premier Support for Partners	• End tot end support. Volledige ondersteuning over het hele Microsoft platform, inclusief cloud, werkplek, hybride en on-premise omgeving. • Proactieve diensten. Mogelijkheid tot het afnemen van workshops en andere proactieve diensten om kennis te vergroten en adoptie te stimuleren. Dit is op verzoek en hoeft dus niet meegenomen te worden in het budget. • Ondersteuning door Microsoft bij Kritieke Situaties. Biedt de hoogste prioriteit reactietijden voor kritieke problemen, waarbij direct contact tussen PNB en Microsoft (eventueel gezamenlijk met dienstverlener) tot de mogelijkheden behoort. Hierbij gelden de standaard SLA voorwaarden van Premier Support for Partners zoals aangeboden door Microsoft: ○ Minimal business impact (Sev C): <4 business hours ○ Moderate business impact (Sev B): <2 hours ○ Critical business impact (Sev A): <1 hour ○ And critical situation support

4.3 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van de dienstverlener het volgende:

1. Adequaat beheer en ondersteuning conform overeengekomen service levels (continuïteit)

Van de dienstverlener wordt verwacht zich te verdiepen in de bedrijfsprocessen van PNB. Hierdoor begrijpt hij wat de impact van verstoringen is op PNB, haar gebruikers, inwoners en externe partijen. De dienstverlening wordt afgestemd op de mate waarin de bedrijfsvoering missie-kritisch is en wat de operationele impact is van verstoringen op de PNB-bedrijfsvoering en op de omgeving. PNB verwacht dat de dienstverlener concrete en adequate servicelevels opstelt, conform levert en PNB wil hiervoor een Service Level Agreement (SLA) afsluiten. Daarbij eist PNB dat de dienstverlener minimaal invulling geeft aan de beschreven servicelevels zoals opgenomen in de eisen omtrent de dienstverlening.

PNB verwacht daarnaast:

a) Standaardiseren van verzoeken en wijzigingen:

Dienstverlener heeft een gestandaardiseerd, in de regel geautomatiseerd, proces waarmee veel voorkomende verzoeken en wijzigingen worden uitgevoerd. Dienstverlener levert een uitputtend overzicht van deze gestandaardiseerde wijzigingen en verzoeken op. Ze zijn vast onderdeel van de inschrijfprijs c.q. het overeengekomen beheertarief en de lijst groeit continu.

b) Infrastructure as Code:

De dienstverlener hanteert, met uitzondering van specifieke situaties, een 'hands-off'-beleid door middel van *Infrastructure as Code* (IaC) met *Azure Bicep*.

Met Bicep worden de infrastructuurconfiguraties als code vastgelegd, wat zorgt voor efficiëntie en consistentie. Hierdoor kunnen gemakkelijk dezelfde configuraties toegepast worden zonder de risico's van handmatige fouten en variaties.

De dienstverlener heeft het eigen Azure platformbeheer volledig geautomatiseerd. Dit geldt bijvoorbeeld voor het automatiseren van Virtuele Machine implementaties en het uitrollen van een Application Landing Zone. De dienstverlener blijft hierin ontwikkelen en zorgt ervoor dat nieuwe policies en functionaliteiten m.b.t. het Azure platform ook conform Infrastructure as Code worden uitgerold en beheerd.

Er is een beveiligde repository en tooling voor de implementatiecode van workloads en services, en deze is toegankelijk voor het Cloud Competence Center van PNB.

Naast bovenstaande punten staat PNB open voor aanvullingen van de dienstverlener op zowel de huidige levels als suggesties voor aanvullende afspraken.

2. Proactief bewaken van kwaliteit

Naast dat de dienstverlener de continuïteit bewaakt is PNB ook op zoek naar een dienstverlener die aantoonbaar continu meedenkt en proactief is. Het zit zelfs in het DNA van de dienstverlener. Hierbij valt te denken aan:

- a) De dienstverlener voelt zich verantwoordelijk voor het PNB (cloud) platform en draagt dit proactief uit d.m.v. optimalisatievoorstellen.
- b) Wijzigingen en verzoeken worden kritisch bekeken en daar waar het beter, handiger of sneller kan, wordt dat met PNB besproken. De dienstverlener doet op een pragmatische manier een voorstel, zonder dat het tot noemenswaardige vertraging leidt. Er wordt op alle wijzigingen en verzoeken een controle gedaan op juistheid en volledigheid. Waar nodig wordt proactief informatie opgehaald door de dienstverlener.
- c) Naast de ontwikkeling van de toepassingen op de dienst is ook de ontwikkeling van de installed base c.q. het platform zelf van essentieel belang. PNB wil dat altijd op actuele versies gewerkt wordt. PNB verwacht van de dienstverlener dat hij dit borgt en dat hij vroegtijdig impact en doorlooptijd van updates en upgrades in kaart brengt en de implementatie daarvan is onderdeel van de dienst. En dat, onderbouwd, wordt aangegeven wanneer hiervan moet worden afgeweken.
- d) PNB vraagt dienstverlener inzicht te geven hoe zij gestructureerd en meerdere keren per jaar PNB informeert en uitdaagt na te denken over potentiële mogelijkheden voor het implementeren van innovatieve functionaliteit m.b.t. Azure cloud, Azure netwerk en authenticatie en autorisatiemanagement dienstverlening. En waarbij de dienstverlener concrete realistische voorstellen doet die bijdragen aan het bereiken van de doelen en de ambitie van PNB en waarvan het resultaat leidt tot een duidelijke meerwaarde voor PNB en bij voorkeur voor beide organisaties

3. Bijdragen aan de Azure Cost Management Governance

Door PNB is een Azure Cost Management Governance opgesteld binnen het Cloud Adoption Framework en conform de gestandaardiseerde FinOps principes van de FinOps Foundation een Azure Cost Management Governance opgesteld. Hoewel PNB de kosten in Azure draagt en eindverantwoordelijk is voor het cost management, verwacht PNB van de dienstverlener dat hij PNB hierin op een proactieve manier ondersteunt. Uitgangspunt hierbij is dat FinOps en/of kostenefficiënt denken, aanwezig is in de standaard werkwijze en mindset van het beheerteam.

De taken en verantwoordelijkheden voor de dienstverlener passen bij het FinOps engineering persona. Ze zijn gericht op het ontwerpen, beheren en optimaliseren van cloudinfrastructuur om kosteneffectiviteit, performance en betrouwbaarheid te bereiken, terwijl de security en compliancy worden gewaarborgd. Hier zijn de belangrijkste verantwoordelijkheden:

1. Resource monitoring en right-sizing:
 - a. Identificeren van ongebruikte of onderbenutte resources en deze opschonen of schalen om kosten te besparen.
 - b. Proactieve communicatie over onverwachte afwijkingen in gebruik van het Azure Platform en van alle workloads in beheer bij de dienstverlener.
2. Tagging:

Implementeren van de PNB taggingstrategie om resources te categoriseren en kosten toe te wijzen aan de juiste afdelingen of projecten.
3. Optimization en Advisory:

Periodiek adviseren over kostenoptimalisaties, zoals het gebruik van andere of nieuwe cloud services die kosten kunnen besparen, voor alle workloads in beheer van de dienstverlener.

4. Policy Enforcement:
Handhaven van policies om te voorkomen dat resources worden gemaakt/ingezet die niet voldoen aan de kostenbeheerstrategieën.
5. Automation:
Automatiseren van routinetaken met betrekking tot kostenbeheer, zoals het uitschakelen van niet-productieomgevingen buiten werktijden.
6. Deelname overleg:
Op uitnodiging aansluiten bij het Operationeel Cloud Cost Management Overleg van het Cloud Competence Center van PNB.

4. Aanvraagproces nieuwe workload

PNB wil de mogelijkheid hebben om ook de implementatie en het beheer van nieuwe cloud workloads bij de dienstverlener onder te brengen. Hierbij wordt dus niet alleen de Application Landing Zone door dienstverlener beheerd, maar wordt ook de workload ten behoeve van de applicatie ingericht en beheerd. PNB wil dat het aanvraagproces van een nieuwe cloud workload efficiënt is en de doorlooptijd kort. De dienstverlener zorgt er op een proactieve manier voor dat zij over alle hiervoor benodigde informatie beschikt. Hierbij worden altijd de PNB policies in acht genomen, en dienen de regie-inspanningen voor PNB zeer laag. Het gaat bij deze workloads om bijvoorbeeld VM's, een storage oplossing of een andere standaard Azure service (IaaS/PaaS). PNB verwacht inzicht in het standaardproces en de werkwijze van dienstverlener, de afhankelijkheden en de aandachtspunten m.b.t. het aanvraagproces nieuwe cloud workload.

5. Continu innoveren en doorontwikkelen op basis van impactvolle wijzigingen (ad 7 en 8 van de scope)

PNB heeft een sterke behoefte dat op de cloud platform dienst continu wordt geïnnoveerd en doorontwikkeld. Van de dienstverlener wordt verwacht dat hij in staat is in deze behoefte te voorzien op een manier die aansluit bij de verwachtingen van PNB. Hiervoor brengt de dienstverlener specialistische kennis en ervaring in, hij leert de opdrachtgever snel kennen en stemt hij de impactvolle kansen op regelmatige basis af met de provincie.

Veranderingen zijn zowel in de markt als binnen het PNB IT- en applicatielandschap continu aan de orde. Dit vraagt van de dienstverlener cloud en platform dat hij meegaat in deze ontwikkelingen en waar mogelijk en voor PNB zinvol vooroploopt. Dit doet hij onder andere door een actieve afstemming met Microsoft en belangrijke (internationale) Azure cloud communities en leveranciers. Op basis hiervan legt hij PNB actuele en stevig onderbouwde keuzes voor, onder andere in de vorm van roadmaps en designs voor toekomstige projecten. PNB wil inzicht hoe de dienstverlener dit in de praktijk op een gestructureerde manier doet, op welke wijze hij dit voorlegt aan PNB en hoe besluitvorming en uitvoering vorm gegeven wordt. Afhankelijk van het onderwerp wordt dit op tactisch of strategisch niveau toegelicht en besloten. Voor deze nieuwe ontwikkeling stelt de dienstverlener een HLD op of past het bestaande design aan op een wijze dat het door PNB kan worden getoetst aan de architectuur kaders en verwerkt kan worden in Blue Dolphin.

PNB wil inzicht hoe dienstverlener doorontwikkel- en innovatietrajecten in de praktijk aanpakt en op welke wijze hij die voorlegt aan PNB en hoe besluitvorming en uitvoering vormgegeven wordt.

6. Huidige workloads vanuit on-premise naar de Azure cloud verhuizen

De dienstverlener beschikt vanuit de techniek over ruime kennis en ervaring om PNB te begeleiden bij het verhuizen van de huidige workloads vanuit het on-premise datacenter in Den Bosch naar de Azure cloud².

PNB verwacht dat dienstverlener, in samenwerking met de applicatie leverancier, voor deze nieuwe ontwikkelingen, een HLD opstelt, of hij past het bestaande design aan op een wijze dat het door PNB kan worden verwerkt in Blue Dolphin.

² Het daadwerkelijke project ter uitvoering van het cloud native maken van applicaties zelf valt niet binnen het innovatie budget en zal niet binnen deze dienstverlening worden uitgevraagd.

7. Ontwerp, testen en implementeren van nieuwe applicaties binnen de dienst Azure cloud platform.

Naast het overzetten van bestaande on-premise geïmplementeerde applicaties naar de Azure-omgeving, zullen ook in de toekomst nieuwe applicaties door PNB worden aangeschaft. In die situatie verwacht PNB van de dienstverlener dat hij ruim voldoende kennis en ervaring heeft om PNB advies te geven t.a.v. de juiste strategie en aanpak voor het optimaal implementeren van deze applicatie. Daarnaast stelt hiervoor dienstverlener een HLD op conform de kaders en richtlijnen van PNB. De dienstverlener neemt deel aan het daarop volgend project om te komen tot een correcte implementatie van de nieuwe applicatie. Van dienstverlener wordt verwacht aan te geven hoe hij PNB op dit punt adviseert en hoe hij dit advies afstemt met betrokken partijen.

5 Visie, scope en verwachtingen regie en samenwerking

5.1 Visie

In de IT-visie en de sourcing strategie heeft PNB haar doelen en ambitie op het gebied van IT-dienstverlening vastgelegd. De kern van de sourcing strategie is dat PNB zich focust op de overall regievoering over de kavel, samenwerking en het WAAROM en WAT van de dienstverlening. Wat betekent dat de niet-strategische IT-dienstverlening wordt uitbesteed en waar dit al het geval is, blijft dit zo. De IT-dienstverleners richten zich op de inhoud, het HOE en op een optimale samenwerking met PNB. Dit moet voor PNB leiden tot een beter overzicht, inzicht, rust en grip en tot een betere 'time to market' van nieuwe of gewijzigde diensten, het vergroten van het adaptief vermogen van PNB en tot het borgen van de continuïteit van de dienstverlening en expertise.

PNB wil een regiemodel en samenwerkingsmodel implementeren, geënt op het 9-vlaks model van Maes, ITIL en JAV waarin de onderstaande elementen centraal staan:

- *Efficiënte en doelgerichte regie en service integratie (SIAM)*
Als onderdeel van de regievoering wil de PNB de service integratie rol invullen voor de verschillende dienstenketens. Wanneer PNB op termijn voldoende inzicht en ervaring op dit vakgebied heeft opgebouwd, wordt mogelijk ook de SI-rol uitbesteed.
- *PNB richt zich op het WAAROM en WAT, dienstverleners op het HOE*
PNB richt zich op het ophalen van de vraag bij de business en de functionele formulering van deze vraag, het WAT en het WAAROM hierachter. De dienstverleners richten zich op de technische- en dienstinvulling van de functionele vraag en daarmee ook op de wijze waarop dit zal plaatsvinden, het HOE. In een enkel geval leggen interne spelregels, beleid of wettelijke kaders enige beperkingen op aan bovenstaande principe. In die gevallen wil of moet PNB zelfs meekijken "onder de motorkap" van de dienstverlener, meedenken over de oplossing. Dit geldt specifiek in de volgende situaties:
 1. Architectuur. PNB kent een aantal uitgangspunten en richtlijnen t.a.v. architectuur die ook raakvlakken hebben met het HOE. Bijvoorbeeld op het gebied van aansluitvoorwaarden en architectuurprincipes of de inzet van TOGAF (zie Bijlage Architectuur bij PNB). Daarnaast wordt een optimale architectuur-aansluiting verwacht tussen de functionele oplossing van de dienstverlener en de architectuur zoals gehanteerd door PNB. Denk hierbij bijvoorbeeld aan de enterprise of referentie architectuur. Dit maakt dat PNB graag meekijkt "onder de motorkap".
 2. Security. Dit is bij uitstek een element waarbij interne regelgeving, beleid en wettelijke voorschriften steeds vaker raakvlakken hebben met en in een enkel geval voorschrijvend zijn v.w.b. het HOE. Soms gaat het over het proces, soms over richtlijnen en soms over techniek.
 3. Regie. De regie over het IT-landschap en de onderliggende dienstverleners ligt bij PNB, waar de operationele regie binnen de keten van de kavel, inclusief de koppeling naar de aanpalende kavel, het werkgebied van de dienstverlener is. Op de koppelvlakken stemmen PNB en de dienstverlener met elkaar af hoe e.e.a. optimaal wordt geïmplementeerd. Gebruik van gezamenlijke (PNB) tooling voor o.a. ITIL is hierbij een belangrijk uitgangspunt.
- *Intensieve samenwerking met dienstverleners*
PNB streeft naar een langdurige strategische samenwerking met dienstverleners, mogelijk tot wel 8 jaar bij gebleken succesvolle dienstverlening en samenwerking.
Voor het invullen van dit 'partnership' wil PNB hieraan concreet invulling geven door toepassing van het Joint Added Value (JAV) model. Uitgangspunt hierbij is dat de PNB de dienstverlener 'op de winkel kan laten passen' zonder dat de kassa geteld moet worden.

Het selecteren van de juiste partner is essentieel, waarbij PNB verwacht dat de dienstverlener verder kijkt dan alleen haar eigen belang, werkterrein of gecontracteerde dienstverlening en er een daadwerkelijk partnership gaat ontstaan. Het partnership leidt tot afgestemde belangen, innovatie en efficiëntere dienstverlening voor PNB én de dienstverlener. De samenwerking is gebaseerd op openheid, transparantie en vertrouwen en past in de visie van PNB als opgave gestuurde overheidsorganisatie.

De essentie van JAV ligt in leveren van toegevoegde waarde en de vertrouwensrelatie die de juiste context creëert om het te laten ontstaan en gedijen. Hiertoe staan acht elementen centraal die in elke van de drie onderstaande te doorlopen fasen passend moeten worden ingevuld:

1. PNB geeft invulling door een gedegen voorbereiding van de aanbesteding en evaluatie en herinrichting van de eigen regie organisatie. Al in de aanbestedingsfase gaat PNB in gesprek met dienstverleners waarbij ook wordt gezocht naar een optimale cultural- en strategic fit. Dit is een belangrijke randvoorwaarde voor een goede samenwerking.
2. Partijen stemmen met elkaar een heldere, gedragen en duidelijke set afspraken af. Hiermee wil PNB ongecontroleerde escalaties vermijden en perspectief bieden om de vruchten te plukken van gedane investeringen. Heldere (financiële) kaders, dienstbeschrijvingen en servicelevels zijn opgesteld en er is een duidelijke gedragen rolverdeling. Openheid en transparantie ten opzichte van elkaar is essentieel.
3. Gedurende de looptijd van de overeenkomst wordt met geduld en respect gewerkt aan het op- en uitbouwen en onderhouden van een goede relatie. In deze fase wordt door partijen periodiek bij tactisch overleg geëvalueerd en successen worden gevierd.

Voor een beknopte uitleg van de acht elementen en hoe PNB deze vervolgens wil invullen, verwijzen we u naar bijlage 11 Samenwerking op basis van Joined Added Value.

5.2 Scope

Tot de scope van de regie en samenwerking behoort:

1. Samenwerken (op locatie) gericht op continuïteit, stabiliteit, transparantie en betrouwbaarheid waarbij de werkwijze continu wordt geprofessionaliseerd.
2. Deelnemen en bijdragen aan de verschillende overleggen.
3. Transparantie in kosten en rapportages.

5.3 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van de regie en samenwerking het volgende:

1. Bijdrage aan de samenwerking

PNB verwacht dat een dienstverlener verder kijkt dan alleen haar eigen belang, werkterrein of gecontracteerde dienstverlening en er een daadwerkelijk partnership gaat ontstaan. Het partnership leidt tot afgestemde belangen, innovatie en efficiëntere dienstverlening voor PNB én de dienstverlener. De samenwerking is gebaseerd op openheid, transparantie en vertrouwen en past in de visie van PNB als opgave gestuurde overheidsorganisatie. De communicatielijnen zijn op alle niveaus kort. Dienstverlener en PNB weten elkaar snel te vinden. Betrokkenen hebben voldoende mandaat om snel te besluiten waar nodig. PNB verwacht dat de dienstverlener actief bijdraagt aan de samenwerking en het JAV-model adopteert. In de samenwerking spelen houding en gedrag een belangrijke rol. PNB is van mening dat door deze samenwerking de diensten aan afnemers van de dienstverlening en uiteindelijk de PNB-collega's mede succesvol wordt doordat de dienstverlener:

- a. In één keer goed en conform verwachting levert;
- b. Samenwerking met partners binnen de regie organisatie van PNB opzoekt;
- c. Een proactieve houding heeft en eigenaarschap toont om bij te dragen aan het oplossen van meldingen en afhandelen van (security) incidenten;
- d. Het principe hanteert van resolve first, discuss later;
- e. Proactief verbetervoorstellen doet over de actuele dienstverlenings- en kwaliteitsniveaus en de rapportages daarover;
- f. Gevraagd en ongevraagd adviseert en uitdaagt over lopende ontwikkelingen en meedenkt over opvolging van latente behoeften en wensen;
- g. Initiatieven realiseert, met een minimale administratieve last voor zowel PNB als dienstverlener zelf;
- h. Werkt met standaarden, maar pragmatisch is waar het nodig;
- i. Gebruik maakt van de kennis en ervaring van PNB op haar expertisegebieden (architectuur, PNB-organisatie, processen) en zich opstelt als stevige discussiepartner.
- j. Indien door dienstverlener zelf of door PNB gewenst, of wanneer de situatie daarom vraagt, activiteiten op de PNB locatie uitvoert en door dienstverlener op PNB locatie deelneemt aan de diverse (strategische, tactische en operationele) overleggen op de PNB locatie in Den Bosch.

2. Operationele regie

PNB verwacht dat dienstverlener zorgdraagt voor de operationele regievoering over de diensten die hij levert en de aansluiting op aangrenzende diensten. Hierbij heeft de dienstverlener een duidelijk beeld van en ervaring met hoe de grensvlakken optimaal wordt ingevuld. De rolverdeling en verwachtingen over en weer zijn voor alle betrokken partijen helder en de communicatie- en escalatielijnen duidelijk. Daarnaast voldoet de dienstverlener aan de aansluitvoorwaarden van de SOC dienstverlener en informeert de dienstverlener de SOC-dienstverlener tijdig en volledig over de status van security incidenten.

3. Koppeling ITSM-tool

Voor een optimale samenwerking tussen opdrachtgever en dienstverlener is een snelle goed werkende koppeling tussen beide ITSM-tools van groot belang. De wijze van koppelen moet de regie en service integratie rol van PNB over alle kavelen heen mogelijk maken en de PNB ITSM tool de single source of truth te zijn. Dit maakt tevens dat PNB-eigenaar kan zijn van een up to date CMDB. Het configuratie managementproces is naast incident, change en problem management, net als request fulfilment onderdeel van de koppeling. Een continu up to date ITSM tool vraagt een (near) realtime koppeling gebaseerd op API's.

De dienstverlener verzorgt de API-koppeling vanuit zijn organisatie en onderhoudt deze koppeling tijdens de contractlooptijd. PNB verzorgt de API-koppeling aan zijn kant.

6 Visie op informatiebeveiliging en privacy

6.1 Visie

Informatiebeveiliging en de daarmee samenhangend cybersecurity hebben de laatste jaren een grote vlucht genomen. PNB onderkent dat in alle opzichten. Informatie moet voldoen aan de BIV eisen (Beschikbaarheid, Integriteit en Vertrouwelijkheid) en informatiesystemen moeten veilig kunnen worden gebruikt. Niet alleen door provinciale medewerkers, maar ook door samenwerkende overheden, dienstverleners, burgers en bedrijven participeren in de informatievoorzieningen van PNB. Door het toepassen van kaders, wet- en regelgeving zoals bijvoorbeeld de ISO- en BIO-normeringen bouwt PNB aan een veilige omgeving op basis van de onderstaande kernwaarden.

- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid: het beschermen van informatie tegen inzage, mutatie en verwijdering. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Deze kernwaarden gelden voor alle processen van PNB zodat de informatievoorziening gedurende de hele levenscyclus van informatiesystemen is geborgd. Dit ongeacht de vorm van de technologie en het karakter van de informatie. Informatiebeveiliging binnen PNB beperkt zich dus niet alleen tot de IT-omgeving. Het heeft betrekking op alle gebruikers van de provinciale informatie.

PNB is NEN-ISO27001 gecertificeerd. De organisatie voldoet daarbovenop ook aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO is een verplicht normenkader opgelegd vanuit de Rijksoverheid en geldt voor overheidsinstanties binnen Nederland zoals bijvoorbeeld rijk, provincies, waterschappen en gemeenten. Bovendien voldoet PNB aan de Europese NIS-richtlijn en is in voorbereiding op zijn opvolger NIS2. Bovengenoemde wet-, regelgeving en normenkaders dienen gezien te worden als de pijlers van de PNB-informatiebeveiliging. Daarnaast heeft PNB ook nog te maken met andere wetgevingen en normenkaders of uitvloeisels daarvan zoals bijvoorbeeld de Archiefwet, Wet Digitale Overheid en Forum Standaardisatie.

Gecertificeerde Dienstverlening

Informatiebeveiliging stopt niet bij de provinciale organisatie. Het maakt in de huidige tijd ook steeds meer deel uit van de bedrijfsvoering van dienstverlener en ketenpartners van of voor PNB. Om deze reden stelt de PNB eisen aan de dienstverlener en de geleverde diensten die onderdeel uitmaken van de keten:

1. Dienstverleners en hun onderaannemers zijn NEN-ISO27001 gecertificeerd (of gelijkwaardig).
2. Alle dienstverlenende producten van de dienstverlener zijn NEN-ISO27001 gecertificeerd.
3. Onderaannemingen van de dienstverlener die bijdragen aan de diensten die worden verstrekt aan PNB zijn NEN-ISO27001 gecertificeerd.
4. De dienstverlener conformeert zich aan de Baseline Informatiebeveiliging Overheid (BIO) en afgeleide wetgeving en/of normenkaders over de volledige scope van geleverde dienstverlening. Na een verplichte audit worden geconstateerde afwijkingen in overleg met PNB binnen een overeengekomen periode ingevuld.
5. De dienstverlener conformeert zich vanaf de publicatie in de Staatscourant aan de toekomstige NIS2 wetgeving en de daaruit voortvloeiende cyberbeveiligingswet (CBW) voor de scope van geleverde dienstverlening.

Samenwerking met securitypartner

PNB heeft een complexe digitale omgeving en heeft daarom diverse gespecialiseerde dienstverleners gecontracteerd. Dit is ook het geval voor security en compliance. Deze dienstverlener levert naast het Security Operations Center (SOC) functioneel beheer op onderdelen zoals SIEM (Security Information and Event Management) en heeft een regievoerende rol ten aanzien van incidenten- en kwetsbaarhedenmanagement. De rol van de security dienstverlener gaat dus verder dan alleen het melden van incidenten en kwetsbaarheden. Hij fungeert als aanjager over incidenten en stelt eisen ten aanzien van security en compliance in de rol van regievoerder over de gehele IT-infrastructuur en de daarmee samenhangende dienstverleners.

Privacy

PNB is gegevensverwerker in de zin van de Algemene wet Verordening Gegevensbescherming (AVG). Dat betekent dat zij voor de uitvoering van haar taken als provincie en als werkgever persoonsgegevens verzamelt en verwerkt. Een adequate bescherming van deze persoonsgegevens is uitermate belangrijk. Burgers, personen uit samenwerkende organisaties en provinciale medewerkers hebben recht op een maximale bescherming van hun persoonsgegevens. PNB voldoet dan ook aan de actuele wetgeving en voorschriften zoals gesteld in de AVG. Dat betekent dat belanghebbenden van PNB mogen verwachten dat zij persoonsgegevens op een rechtmatige, behoorlijke en transparante manier, conform de AVG verwerkt. Dat geldt ook voor alle derde partijen die diensten leveren aan PNB waarbij zij persoonsgegevens verwerken en waarvoor verplicht ze een verwerkersovereenkomst hebben getekend.

6.2 Scope

Tot de scope van informatiebeveiliging en privacy behoort:

1. Het inrichten en onderhouden van de dienstverlening conform de geldende wet- en regelgeving en normenkaders op het gebied van informatiebeveiliging en privacy.
2. Het inrichten en onderhouden van de IT-infrastructuur conform de geldende wet- en regelgeving en normenkaders op het gebied van informatiebeveiliging en privacy en/of uitvloeisels van andere van toepassing zijnde wet- en regelgeving.
3. Het continu veilig houden van het PNB cloud platform.
4. Inrichten en uitvoeren van de dienstverlening conform de AVG-richtlijnen.
5. Een integratie, dan wel een samenwerking, met andere provinciale dienstverleners op het gebied van security, met name de SIEM/SOC-dienstverlener.

6.3 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van informatiebeveiliging en privacy het volgende:

1. Proactieve informatiebeveiliging

De dienstverlener is verantwoordelijk voor een adequate en passende inrichting en het actief onderhouden van alle securitycomponenten binnen de verschillende (gecontracteerde) omgevingen die onderdeel uitmaken van de provinciale IT-infrastructuur. Van de dienstverlener wordt verwacht dat hij volledig transparant is ten aanzien van de beveiligingsstatus en -updates van de provinciale Azure cloud, het on-premise datacenter, Azure netwerk en de authenticatie en autorisatiemanagement-inrichting. Software is altijd voldoende up-to-date en ligt in lijn met het kwetsbaarhedenmanagement zoals dat wordt voorgeschreven door PNB en de verantwoordelijke dienstverlener. Security incidenten en externe dreigingen worden vroegtijdig ontdekt, gemeld en met passende maatregelen beantwoord. Dienstverlener hanteert vastgestelde procedures voor het afhandelen van security incidenten. Expertise, autonomie, snelheid en effectiviteit zijn hierin sleutelbegrippen in tegenstelling tot het verwijzen naar administratieve procedures of contractuele afspraken.

Er wordt proactief onderzoek gedaan naar risico's en dreigingen binnen het verantwoordelijk domein van de dienstverlener. De dienstverlener mitigeert op basis van risico gebaseerde informatiebeveiliging. De dienstverlener beweegt (pro-)actief mee met de veranderende eisen vanuit PNB en/of wet- en regelgeving gedurende de looptijd van de overeenkomst. Daarnaast adviseert dienstverlener PNB proactief ten aanzien van risico's en nieuwe security en privacy gerelateerde oplossingen.

2. Security als onderdeel binnen de dienstverlening

Van de dienstverlener wordt verwacht dat hij ten aanzien van security binnen zijn dienstverlening en het kavel zorgdraagt voor het beheer en het regulier onderhoud waarbij alle securityvoorzieningen en eisen in acht worden genomen. PNB is ervan overtuigd dat dit specifieke, passende en specialistische kennis en ervaring met zich meebrengt. Deze kennis is organisatorisch geborgd en komt tot uiting in functies en rollen bij de dienstverlener zoals CISO, ISO, ISM en/of operationeel security engineers. De provincie verwacht mede dat vanuit deze verschillende rollen op reguliere basis strategische en tactische overleggen plaatsvinden tussen de provincie en de dienstverlener. Ook moet dit specialisme bijdragen aan het adequaat opvolgen en van afhandelen security incidenten of het vertalen van maatregelen uit

normenkaders en wet- en regelgeving naar functionele en/of technische oplossingen. De dienstverlener hanteert standaardprocedures en/of draaiboeken in het geval van verschillende typen security incidenten of calamiteiten.

Operationele securitymedewerkers c.q. het securityteam en/of CIRT (Cyber Incident Response Team) opereert onafhankelijk van reguliere beheerteams waarbij altijd het belang van de klant centraal staat.

3. Samenwerking met de security dienstverlener (SOC)

PNB maakt gebruik van een gespecialiseerde securitypartner die is gecontracteerd voor een overkoepelend Security Operations Center (SOC) en het beheren van het Security Information and Event Management (SIEM). Dienstverlener is verantwoordelijk voor de operationele beveiliging binnen de eigen dienstverlening (bijvoorbeeld het doorvoeren van security patches en implementeren van mitigerende maatregelen) inclusief realtime ontsluiting van logbronnen richting het SOC. Ook informatie m.b.t. systeemarchitectuur en -configuratie wordt gedeeld.

Dienstverlener zorgt ervoor dat het SIEM voldoende rechten krijgt op de benodigde assets/componenten binnen beheerde infrastructuur. De behoefte van PNB is hierin leidend. Uit de SOC-dienstverlening ontstaan security incidenten die worden opgevolgd door de dienstverlener op basis van het reguliere incidentproces en zoals is overeengekomen met PNB en de security dienstverlener.

PNB is gebaat bij een goede samenwerking tussen de dienstverlener, de SOC dienstverlener en PNB. Dit vraagt om een gezamenlijk risicomanagement met daarin een duidelijke afbakening van het eigenaarschap van te treffen maatregelen. Van de samenwerkende partijen, en dus ook van de cloud platform dienstverlener, wordt verwacht dat de dienstverlening ten aanzien van hoge prioriteit security incidenten 24x7x365 wordt ingevuld volgens de prioriteit P1 zoals vastgelegd in het SLA, inclusief bijbehorende servicelevels en afspraken, bijvoorbeeld ten aanzien van het informeren van PNB. Indien nodig werkt dienstverlener mee een te vormen Computer Security Incident Response Team (CSIRT).

4. Wet- en regelgeving

De provincie is als overheidsorganisatie gebonden aan wet- en regelgeving waar het gaat om verwerking en opslag van informatie uit verschillende taken met bijbehorende processen binnen de ambtelijke organisatie. Voor informatiebeveiliging zijn de NEN-ISO27001, BIO, NIS2 en de AVG-normenkaders en wetgeving die de inrichting van de IT-infrastructuur direct raken. Maar ook uitvloeisels van deze normenkaders of wetgeving zoals het Forum Standaardisatie of de Wet Digitale Overheid of de Archiefwet drukken hun stempel op het IT-beleid en de technische inrichting. Van de dienstverlener wordt niet alleen verwacht bekend te zijn met de verschillende wet- en regelgeving, maar dat dit ook actief onderdeel is als het gaat om onderhoud, beheer, implementatietrajecten en/of wijzigingsprocedures binnen de ICT-infrastructuur. Dienstverlener verbetert dus de cloud infrastructuur op het gebied van securityonderdelen en vertaalt maatregelen vanuit normenkaders of high level designs naar functionele en technische oplossingen verwoord in zogenaamde low level designs

Vanuit technologisch perspectief wordt gezocht naar een dienstverlener die handelt volgens security-by-design en security-by-default principes en die dergelijke principes ook kan implementeren binnen de aangeboden dienstverlening.

7 Eisen

PNB heeft de volgende overall kwaliteitseisen (knock-out criteria):

#	Eis Algemeen
1.	Dienstverlener verklaart expliciet dat hij voldoet aan alle in de selectieleidraad en daarbij behorende bijlage(n) genoemde voorwaarden en eisen die aan de opdracht zijn gesteld.
2.	Dienstverlener conformeert zich aan geldende en toekomstige van toepassing zijnde wet- en regelgeving.
3.	Dienstverlener conformeert zich aan het voor de scope van de opdracht relevante PNB-beleid.
4.	Dienstverlener conformeert zich aan de marktstandaarden en de standaarden voorgeschreven door het Forum voor Standaardisatie.
5.	Intellectual property t.a.v. data, processen en procedures, maatwerk scripting, designs, documenten, rapportages, logbronnen, IP-rechten, voor zover ze betrekking hebben op de aan opdrachtgever gecontracteerde dienstverlening, zijn en blijven eigendom van provincie Noord-Brabant.
#	Eis Inkoop en contract
1.	ARBIT-2022 voorwaarden zijn van toepassing.
2.	PNB betaalt slechts voor actieve en daadwerkelijke geleverde en door PNB geaccepteerde diensten.
3.	PNB kan marktconformiteit van prijzen en tarieven extern laten toetsen en vaststellen door middel van een benchmark. Dienstverlener verleent hieraan gevraagde bijdrage.
4.	Partijen zullen uitkomst van de benchmark bespreken en hieraan eventueel passende consequenties verbinden.
5.	Dienstverlener gaat akkoord met de conceptovereenkomst.
#	Eis Taal
1.	Dienstverlener garandeert dat gedurende de uitvoering van de opdracht door alle werknemers en ingezette derden die zorgdragen voor de uitvoering van de opdracht in de contacten met PNB, de Nederlandse taal in woord en geschrift zal worden gebruikt. Tevens verklaart dienstverlener dat bij de uitvoering van de opdracht alle documenten en rapportages in de Nederlandse taal zijn opgesteld. Een uitzondering hierop betreffen technische product handleidingen, die ook in het Engels mogen worden opgeleverd.
#	Eis Documentatie
1.	De dienstverlening dient in zijn geheel beschreven en voor PNB te allen tijde beschikbaar te zijn (voorbeelden, maar niet limitatief: handleidingen, beschrijvingen, designs).
2.	(Technische) documentatie is zo opgesteld dat de continuïteit van de dienstverlening is geborgd, PNB inzicht heeft en sturing kan geven op de geleverde diensten en dat PNB of een derde partij het beheer kan overnemen.
3.	PNB is eigenaar van alle beschrijvingen.
#	Eis prijzen en tarieven
1.	De door de inschrijver aangeboden prijzen en tarieven zijn in Euro (€), all-in, inclusief overige belastingen en/of heffingen, en exclusief BTW.
2.	Eventuele valutawijzigingen zijn voor rekening en risico van dienstverlener.
3.	De dienst wordt op een transparante manier gefactureerd, zodanig dat PNB de rekening begrijpt.
#	Eis architectuur
1.	Dienstverlener sluit haar dienstverlening aan de op architectuur van PNB en voldoet aan de door PNB gestelde aansluitvoorwaarden, architectuurprincipes en werkwijze.

PNB heeft de volgende kwaliteitseisen (knock-out criteria) ten aanzien van de Transitie:

#	Kwaliteitseis
1.	De aangeboden transitie aanpak voldoet minimaal aan de in dit document beschreven beschrijving, uitgangspunten en scope.

2.	Decharge van het traject vindt plaats nadat projectwerkzaamheden zijn uitgevoerd, eventuele restpunten zijn benoemd, gepland en overeengekomen en er een formele overdracht is naar en acceptatie door de beheerorganisatie. Decharge vindt enkel plaats na akkoord PNB.
3.	Binnen 3 maanden na de start van de transitie stelt dienstverlener een retransitie- of exitplan op conform de in de Overeenkomst gestelde eisen, waarin de wederzijdse verplichtingen uiteen worden gezet om een geruisloze overgang terug naar PNB of een opvolgende dienstverlener te faciliteren bij beëindiging van de overeenkomst. Het retransitieplan wordt gedurende de looptijd van de overeenkomst minimaal jaarlijks geactualiseerd en besproken met PNB.
4.	Om het gemeenschappelijk belang en de verantwoordelijkheden te benadrukken en het streven naar een effectieve samenwerking tussen PNB, verkrijgende dienstverlener en de latende dienstverlener te bekrachtigen, verklaren PNB en dienstverlener de Gedragscode Retransitie van 15 mei 2014 versie 1.2 van Sourcing Nederland van toepassing. Dienstverlener verklaart dat hij bij het beëindigen van de dienstverleningsovereenkomst 100% medewerking zal verlenen bij de overgang van de dan bestaande dienstverlening naar PNB en/of een derde partij. Dienstverlener borgt dat er geen blokkerende constructies in de diensten of dienstverlening worden gehanteerd die een succesvolle transitie en retransitie in de weg kunnen staan en dat data, informatie en middelen tussen de partijen vrij overdraagbaar is en gebruikt mag worden.

PNB heeft de volgende kwaliteitseisen (knock-out criteria) ten aanzien van Dienstverlening en Innovatie:

#	Kwaliteitseis
1.	De aangeboden dienstverlening en doorontwikkeling voldoet minimaal aan de in dit document beschreven beschrijving, uitgangspunten, service levels en scope.
2.	De aangeboden dienstverlening geeft volledige dekking t aan de scope van de opdracht en de uitgevraagde dienstverlening .
3.	(Technische) documentatie is zo opgesteld dat de continuïteit van de dienstverlening is geborgd, PNB inzicht heeft en sturing kan geven op de geleverde diensten en dat PNB of een derde partij het beheer kan overnemen.
4.	Bij de Inschrijving overlegt dienstverlener een uitputtende lijst van de uitvoeringsprocessen zoals die tijdens de transitiefase en voor overgang naar SLA-gebaseerd beheer (FMO fase) zijn geïmplementeerd.
5.	Dienstverlener heeft een vastgesteld continuïteitsplan waarin is opgenomen hoe, in geval van calamiteiten, de getroffen dienst en/of het getroffen informatiesysteem weer zo snel mogelijk operationeel gemaakt kan worden. Dit plan wordt minimaal jaarlijks beoordeeld en getest.
6.	Dienstverlener heeft periodiek geteste procedures voor backup en recovery van informatie en configuratie voor herinrichting en fouterstel van verwerkingen. Dienstverlener conformeert zich aan de kaders en richtlijnen van de dienstverlener die verantwoordelijk is voor het uitvoeren van de reguliere backup and recovery dienstverlening voor de provincie.
7.	PNB is te allen tijden gerechtigd om een audit uit te voeren of uit te laten uitvoeren door een externe door PNB aan te wijzen auditor over de geleverde dienst. Bevindingen komende uit de audit worden door dienstverlener opgelost op zijn kosten.
8.	De dienstverlener draagt er zorg voor dat alle data wordt verwerkt en opgeslagen binnen de Europese Economische Regio (EER). Uitzonderingen hierop zijn alleen toegestaan met expliciete toestemming van de provincie Noord-Brabant.
9.	De dienstverlener is ingericht op en gerechtigd om Microsoft Premier Support for Partners aan afnemers aan te bieden.
10.	Alle informatiesystemen ten dienste van de dienstverlener beschikken over voorzieningen voor adequate en actuele bescherming tegen ongewenste invloeden.
11.	De toegekende toegangsrechten van alle voor of bij PNB in te zetten medewerkers en derden namens dienstverlener, worden bij de beëindiging van hun dienstverband, contract of overeenkomst direct verwijderd. Bij wijziging van de functie of rol worden de toegangsrechten direct aangepast.
12.	Voordat een account definitief wordt verwijderd dient dit te worden voorgelegd aan de PNB. Daarbij doet de dienstverlener een check op de bevoegdheden van het te verwijderen account. Mocht blijken dat er door het verwijderen van het betreffende account belangrijke content en/of beheerrechten komen te vervallen die niet (automatisch) worden overgezet naar een ander bestaand account, dan moet dit kenbaar worden gemaakt aan de PNB.

12.	Dienstverlener levert structureel en periodiek rapportages bij voorkeur in een Dashboard. Hij zal minimaal rapporteren over: - Aantal, prioriteit, soort melding (tenminste Incidenten, Problems, Service requests en wijzigingen) - Prestatieoverzichten van afhandeling meldingen (duur openstaande melding, reactietijd, hersteltijd, per categorie) inclusief percentage KPI realisatie - Wijzigingenbeheer: overzicht openstaande en uitgevoerde wijzigingen inclusief KPI realisatie - Trendanalyse over laatste 6 maanden van overeengekomen KPI afspraken - Verbetermaatregelen van service levels indien deze beneden het vereiste niveau zijn of dreigen te raken. - Maandelijks inzicht en advies mbt cost management - Overzicht van geautomatiseerde processen - Per kwartaal een technology roadmap - Houdt het HLD up to date																								
13.	Zie voor minimale service levels op gebied van incident management de onderstaande tabel. De meetperiode voor de opgestelde KPI's betreft één kalendermaand. <table><tr><th>Prioriteit</th><th>Scope</th><th>Maximale Reactietijd</th><th>Maximale Hersteltijd</th><th>Status-melding</th><th>Percentage Gehaald (KPI)</th></tr><tr><td>Prioriteit 1</td><td> - Grote delen van organisatie kunnen niet werken - Incidenten met grote impact op de organisatie, waaronder bedrijfskritische applicaties - Er is sprake van acute dreiging m.b.t. de continuïteit, integriteit, aangeboden dienst (Potentieel) datalek </td><td>30 minuten</td><td>4 klokuren</td><td>elk klokuur</td><td>100% van de Incidenten binnen de norm opgelost</td></tr><tr><td>Prioriteit 2</td><td> - Niet bedrijfskritische applicaties - Meerdere gebruikers kunnen niet werken (vanaf 5) - Individuele VIP ondersteuning - Bepaalde afname functionaliteit </td><td>60 minuten</td><td>48 klokuren</td><td>iedere 4 klokuur</td><td>95% van de Incidenten binnen de norm opgelost</td></tr><tr><td>Prioriteit 3</td><td> - Standaard prioriteit - Eén of enkele gebruikers kunnen niet werken </td><td>4 klokuren</td><td>5 werkdagen</td><td>in overleg</td><td>95% van de Incidenten binnen de norm opgelost</td></tr></table>	Prioriteit	Scope	Maximale Reactietijd	Maximale Hersteltijd	Status-melding	Percentage Gehaald (KPI)	Prioriteit 1	- Grote delen van organisatie kunnen niet werken - Incidenten met grote impact op de organisatie, waaronder bedrijfskritische applicaties - Er is sprake van acute dreiging m.b.t. de continuïteit, integriteit, aangeboden dienst (Potentieel) datalek	30 minuten	4 klokuren	elk klokuur	100% van de Incidenten binnen de norm opgelost	Prioriteit 2	- Niet bedrijfskritische applicaties - Meerdere gebruikers kunnen niet werken (vanaf 5) - Individuele VIP ondersteuning - Bepaalde afname functionaliteit	60 minuten	48 klokuren	iedere 4 klokuur	95% van de Incidenten binnen de norm opgelost	Prioriteit 3	- Standaard prioriteit - Eén of enkele gebruikers kunnen niet werken	4 klokuren	5 werkdagen	in overleg	95% van de Incidenten binnen de norm opgelost
Prioriteit	Scope	Maximale Reactietijd	Maximale Hersteltijd	Status-melding	Percentage Gehaald (KPI)																				
Prioriteit 1	- Grote delen van organisatie kunnen niet werken - Incidenten met grote impact op de organisatie, waaronder bedrijfskritische applicaties - Er is sprake van acute dreiging m.b.t. de continuïteit, integriteit, aangeboden dienst (Potentieel) datalek	30 minuten	4 klokuren	elk klokuur	100% van de Incidenten binnen de norm opgelost																				
Prioriteit 2	- Niet bedrijfskritische applicaties - Meerdere gebruikers kunnen niet werken (vanaf 5) - Individuele VIP ondersteuning - Bepaalde afname functionaliteit	60 minuten	48 klokuren	iedere 4 klokuur	95% van de Incidenten binnen de norm opgelost																				
Prioriteit 3	- Standaard prioriteit - Eén of enkele gebruikers kunnen niet werken	4 klokuren	5 werkdagen	in overleg	95% van de Incidenten binnen de norm opgelost																				
14.	Dienstverlener garandeert onderstaande beschikbaarheid van de diensten: <table><tr><th>Tijdvak</th><th>Beschikbaarheid</th><th>Meetperiode</th></tr><tr><td>Servicewindow</td><td>Minimale beschikbaarheid 99,5%</td><td>1 maand</td></tr><tr><td>Onderhoudswindows</td><td>Minimale beschikbaarheid 97%</td><td>1 maand</td></tr></table>	Tijdvak	Beschikbaarheid	Meetperiode	Servicewindow	Minimale beschikbaarheid 99,5%	1 maand	Onderhoudswindows	Minimale beschikbaarheid 97%	1 maand															
Tijdvak	Beschikbaarheid	Meetperiode																							
Servicewindow	Minimale beschikbaarheid 99,5%	1 maand																							
Onderhoudswindows	Minimale beschikbaarheid 97%	1 maand																							
15.	Wijzigingsbeheer moet ervoor zorg dragen dat gewenste aanpassingen aan geleverde oplossing (software, omgeving) / dienstverlening een gestructureerde, overzichtelijke en gecontroleerde manier een weg vinden naar het productiesysteem. Zie onderstaand de minimale eisen aan het change management:																								

	Prioriteit	Norm	Tijdigheid	Juistheid	Volledigheid
	Service request	Reactietijd: 1 Werkdag Doorlooptijd: 1 Werkdag		100% in één keer correct doorgevoerd.	• 90% binnen de norm afgesloten • 100% binnen 2 * de norm afgesloten
	Standaard wijziging	Reactietijd: 1 Werkdag Doorlooptijd: 2 Werkdagen		100% in één keer correct doorgevoerd.	
	Niet standard wijziging	Reactietijd: 2 Werkdagen Doorlooptijd: 5 Werkdagen, na akkoord van CAB Indien van toepassing: een offerte binnen 5 Werkdagen*	minimaal 5 Werkdagen voor het beoogde Change-window aangekondigd bij het CAB	• in maximaal 2 keer goed-gekeurd door het CAB (tijdig, volledig, juist aangeleverd) • 90% in één keer correct doorgevoerd, in het geplande Change-window	
16.	Dienstverlener koppelt alle relevante logbronnen aan het SIEM van PNB om een permanente stroom van benodigde events te leveren aan het overkoepelend Security Operations Center (SOC) en Security Information and Event Management (SIEM).				
17.	Dienstverlener accepteert de aansluitvoorwaarden van de PNB SOC-dienstverlener en hij volgt de security events, gemeld door de SOC-dienstverlener, op conform die aansluitvoorwaarden.				

PNB heeft de volgende kwaliteitseisen (knock-out criteria) ten aanzien van Regie en Samenwerking:

#	Kwaliteitseis
1.	De samenwerking geeft minimaal invulling aan de verwachtingen zoals beschreven in dit document.
2.	Dienstverlener realiseert een near realtime koppeling tussen zijn ITSM-tool en de PNB ITSM tool door middel van een API (t.b.v. incident, problem, change en config management en request fulfilment). Indien de ITSM-tool van PNB nog niet operationeel is op het moment van contracteren, realiseert dienstverlener een tijdelijke (email)koppeling tussen zijn ITSM-tool en de servicemanagement tool van PNB.
3.	Dienstverlener borgt gedurende de contractperiode dat er een bij de PNB verwachting passende (mix kennis en ervaring) contactpersoon is als vast aanspreekpunt voor de PNB architectuur board en t.b.v. roadmapsprekken.
4.	Dienstverlener stelt voor de looptijd van de overeenkomst een vaste contactpersoon voor PNB aan voor escalatiebeheer, samenwerking en support planning.
5.	Dienstverlener is bereid projecten en complexere vraagstukken op locatie in gezamenlijkheid op te pakken.
6.	Dienstverlener biedt ten behoeve van IT-meldingen en -vragen een deskundige servicedesk aan, dat wil zeggen 'een tweedelijns ondersteuning', die als aanspreekpunt rechtstreeks in contact staat met <i>OnsLoket</i> van de PNB.
7.	Afspraken m.b.t. samenwerking zijn minimaal vastgelegd in het DAP. Wijzigingen in het DAP worden onderling afgestemd en akkoord bevonden.
8.	In geval van calamiteiten of crisis is de directie van dienstverlener rechtstreeks toegankelijk voor het management van PNB.

PNB heeft de volgende kwaliteitseisen (knock-out criteria) ten aanzien van informatiebeveiliging en privacy:

#	Kwaliteitseis informatiebeveiliging
1.	PNB eist dat dienstverlener zich minimaal conformeert aan de onderstaande richtlijnen, normenkaders, wet- en regelgevingen of uitvloeisels daarvan die PNB hanteert voor beveiliging van IT-systemen: - BIO-overheid - NIS2 / CBW - Forum Standaardisatie - Provinciale richtlijnen - AVG
2.	Dienstverlener is NEN-ISO27001 gecertificeerd voor de volledige scope van de aangeboden dienstverlening.

3.	Bij gunning volgt een BIO-audit door een door PNB aangewezen onafhankelijk auditor. Dienstverlener werkt hier volledig aan mee zonder enige beperkende maatregelen vanuit de zijde van de dienstverlener.
4.	Dienstverlener voorziet in een security dienstverlening op organisatorisch niveau en heeft de afdoende kennis en expertise als het gaat om onderhoud en beheer op alle security-onderdelen binnen het Azure cloud platform en infrastructuur in het on premise datacenter.
5.	Dienstverlener heeft de kennis- en expertise op het gebied van afhandeling van security incidenten (onderzoek, oplossing en rapportage).
6.	De dienstverlener conformeert zich aan het beleid van de door PNB gecontracteerde security dienstverlener bij de afhandeling van security incidenten inzake het verhelpen van kwetsbaarheden.
7.	Dienstverlener laat periodiek en minimaal eenmaal per jaar een penetratietest uitvoeren door een onafhankelijke partij. De provincie is betrokken bij de keuze van deze partij en ze krijgt inzage in de volledige rapportage. Bevindingen worden door de dienstverlener binnen een afgesproken tijd gemitigeerd of opgelost.
8.	Dienstverlener conformeert zich aan alle werkzaamheden voortvloeiend uit de maatregelen zoals die worden gesteld in de BIO-overheid en geeft daarnaast alle medewerking aan derde partijen die uit hoofde van PNB hiervoor werkzaamheden uitvoeren. Voorbeelden hiervan zijn penetratietesten, kwetsbaarhedenmanagement en auditing.
9.	De provincie behoudt het recht op (permanente) toegang/inzage op alle systeemonderdelen binnen de ICT-infrastructuur. Voorbeelden zijn systeemconfiguratie, logging en rapportage.
10.	Dienstverlener geeft volledige medewerking als het gaat om informatieverstrekking uit relevante logbronnen voor het Security Information and Event Management (SIEM) van PNB om een permanente stroom van benodigde eventlogging te leveren aan het overkoepelend Security Operations Center (SOC).
11.	Dienstverlener neemt in geval van een security incident of calamiteit deel aan een eventueel crisisteam.
12.	Dienstverlener stemt er in toe dat PNB haar invloed behoudt als het gaat om de toe te passen securityoplossingen en waarbij PNB altijd de laatste stem heeft.
13.	PNB bepaalt wie de eigenaar is of wordt van de securityoplossingen/-systemen.
14.	Alle informatiesystemen ten dienste van de dienstverlener beschikken over voorzieningen voor adequate en actuele bescherming tegen ongewenste invloeden.
15.	Ten aanzien van het uitoefenen van onderhoud en beheer conformeert de dienstverlener zich aan de BIO en provinciale richtlijnen waarbij beheertaken en beheerrollen worden gesegmenteerd, de toegang tot inhoudelijke data tot een minimum wordt beperkt alsook een beperking van maximale rechten per beheerrol. Dienstverlener gaat onverminderd akkoord met bijvoorbeeld realtime monitoring, verscherpte toegangsregels of andere maatregelen rondom de inzet en het gebruik van beheerrollen. Dit komt tot uiting in het toegangsbeleid van de dienstverlener t.a.v. beheertaken en beheerrollen.
16.	Er is een demarcatie tussen de bedrijfsvoering van de dienstverlener en die van de ambtelijke provinciale organisatie. Dienstverlener krijgt dan ook op geen enkele manier toegang tot inhoudelijke data van provinciale informatiesystemen als zijnde een ambtelijk medewerker van de provinciale organisatie. Met andere woorden is de dienstverlener geen onderdeel van de ambtelijke provinciale organisatie met daarin de overheidstaken van PNB en de daaruit voortvloeiende processen.
#	Kwaliteitseis informatiebeveiliging Privacy
1.	Dienstverlener conformeert zich aan en gaat akkoord met de provinciale verwerkersovereenkomst op grond van de AVG. Na gunning maken dienstverlener en aanbestedende dienst deze gezamenlijk op en deze wordt door beide partijen ondertekend.
2.	Dienstverlener handelt conform de Algemene wet Verordening Gegevensbescherming (AVG). Alle gegevens door PNB aan dienstverlener ter beschikking gesteld of door de onder de overeenkomst verrichte werkzaamheden aan dienstverlener bekend geworden, zullen anders dan op een door de Nederlandse Wet en regelgeving toegelaten wijze, niet aan derden worden verstrekt.
3.	Persoonsgegevens dienen standaard afgeschermd te zijn en mogen standaard niet openbaar zichtbaar zijn.
4.	Incidenten met betrekking tot privacy worden geregistreerd en conform de verwerkersovereenkomst gerapporteerd aan PNB. Afhankelijk van de grootte, aard en de impact van het incident wordt er een escalatiepad gevolgd waarin PNB tijdig en zo volledig als nodig wordt betrokken.

5.	Alle, en met name privacy gevoelige, data ten aanzien van de aangeboden dienstverlening wordt alleen binnen de Europese Unie (EU) verwerkt en/of opgeslagen. Taken waarbij er geen sprake is van het verwerken van privacy gevoelige data mogen buiten Europees grondgebied worden uitgevoerd, mits hiervoor expliciet toestemming is verleend door de Provincie Noord-Brabant.
----	---

BIJLAGE: Architectuur bij PNB

Architectuurniveaus

PNB onderscheidt verschillende architectuurniveaus, te weten:

- Enterprise architectuur
- Referentie architectuur
- Informatie architectuur
- Applicatie architectuur
- Solution architectuur
- Data architectuur
- Integratie architectuur
- Technische architectuur

Architectuur is een coherent geheel van principes, methoden, modellen en standaarden, die worden gebruikt voor het ontwerp en de realisatie van een bedrijfsorganisatiestructuur, business processen, informatiesystemen en infrastructuur. De organisatie-eigen Enterprise architectuur van PNB is sterk in ontwikkeling en zal de komende jaren verder worden verfijnd.

De voor dit visiedocument 2 belangrijkste architectuurniveaus zijn:

- a. De referentiearchitectuur zien we als een basisset van principes, methoden, modellen en standaarden, die voor elke provincie uitgangspunt zijn bij gemeenschappelijke ontwikkelingen. Als referentiearchitectuur hanteert PNB de Nederlandse Overheid Referentie Architectuur (NORA) waarvan de PETRA (Provinciale EnTerprise Referentie Architectuur) op aansluit. De PNB Infrastructuur Cloud Referentie Architectuur (PICRA)³ is de cloud en infrastructuur architectuur die concreter invulling geeft aan de technische architectuur vanuit NORA naar PETRA.
- a. Solution architectuur zien we als beschrijving van de gewenste oplossing van een specifiek IT-probleem, of het eindresultaat van een IT-project. Een solution-architectuur komt tot stand op basis van de referentie architectuur. Een PSA (Project Startarchitectuur) gebaseerd op de bouwblokken van de referentie architectuur geeft richting en handvatten voor projecten. De PSA is hierdoor richtinggevend en kader stellend voor de totale solution architectuur. HLD(high level)-designs vormen een deeloplossing en gezamenlijk de concrete uitwerking van de totaaloplossing van de solution architectuur. De LLD-designs zijn vervolgens de specifieke invulling van de deeloplossingen afgeleid van de HLD-designs. Gezamenlijk vormen alle designs het geheel van bouwblokken van de totaaloplossing en daarmee de doelarchitectuur.

De overige architectuurniveaus worden verderop in het proces toegelicht in een bijlage.

PNB Referentie architectuur

IT-infrastructuur binnen PNB wordt geïmplementeerd op basis van de PICRA. De PICRA is een gelaagd model die van onder naar boven wordt doorlopen. De gelaagde vorm maakt het mogelijk om per laag een onderwerp af te bakenen. Elke volgende laag maakt gebruik van begrippen uit de onderliggende laag en dus in voorgaande teksten, wat tot een logische en gefundeerde opbouw leidt.

In de fase waarin low level designs (LLD) tot in detail worden uitgewerkt, wordt gebruik gemaakt van Bouwblokken om per onderdeel een low level design op te leveren.

Het bestaat uit de volgende lagen (layers) en bouwblokken:

- Datacenter layer: Housing
- Core Infra layer: Compute, Storage, Network
- Supporting Infra layer: Backup, Security, Operations Management, etc.
- Middleware layer, Dbases, Integration, etc.
- Applications services: Collaboration, Business applications, etc.
- Presentation services: Client-platform, Web-based, user experience, etc.

³ De PNB Infrastructuur Cloud Referentie Architectuur (PICRA) is gelijk aan de C2RA, Cloud and Clear Referentie Architectuur en mag gebruikt en toegepast worden in afspraak met de auteur en eigenaar Cloud and Clear IT Consultancy.

- Compliance & Control layer: Confidentiality, Availability, Integrity, Scalability etc.
- Governance & Management layer: Architecture, ITSM, Project Management, etc.

De Application en Presentation services bieden het merkbare en zichtbare: een desktop, applicaties, portals, e-mail, et cetera. Deze worden beheerd en bestuurd door de onderliggende “onzichtbare” infrastructuur, platform en datacenter services. Over alle lagen heen zijn de security en managementservices ingericht, die onder meer de betrouwbaarheid en integriteit bieden, en daarnaast de gereedschappen en voorwaarden leveren om de SLA's waar te maken.

Met deze architectuur wordt voorzien in een volledig gelaagde, betrouwbare en veilige ICT-infrastructuur. Uitbreidingen op het gebied van applicatiediensten kunnen eenvoudig worden geïmplementeerd, omdat de onderliggende platformdiensten zorgdragen voor zaken als back-up, monitoring, patch management, et cetera.

PICRA heeft als uitgangspunt te werken met referentie architecturen van leveranciers om op basis hiervan de best bewezen oplossingen te implementeren. Hiermee worden onderstaande doelstellingen behaald:

- Snelheid, door sneller infrastructuur te bouwen en te implementeren
- Eenvoud, door de best practices als richtlijn te gebruiken voor het ontwerpen van oplossingen
- Efficiënt, door sneller time-to-value met een hoger ROI te creëren
- Optimalisatie, door uitvoerig geteste workload afstemming met applicaties en hypervisors

PICRA Framework pilaren

De onderstaande pijlers van PICRA-Framework begeleiden en zijn richtinggevend bij het ontwerpen volgens PICRA van Cloud en Infrastructuur vanuit zes verschillende perspectieven.



Architectuur principes

De belangrijkste architectuur principes van de PICRA zijn:

1. PNB werkt in de architectuuraanpak pragmatisch, niet bureaucratisch;
2. Architectuur wordt uitgedrukt in principes, modellen, standaarden en richtlijnen;
3. Architectuur zorgt voor kosten-efficiënte oplossingen, waarbij kwaliteit voorop staat;
4. Voorkom onnodig complexiteit en volg principe KISS (Keep It Smart Simple);
5. PNB-beleid geeft sturing aan de architectuur;
6. Er wordt gewerkt met houdbare en duurzame oplossingen en diensten, waarbij o.a. ook de volwassenheid en levensvatbaarheid van het product en de leveranciers worden beoordeeld;
7. Lean principes worden gevolgd: lever alles dat nodig is, lever niets wat niet gevraagd is;
8. Automate everything. Beperk handmatige acties in de run door bij het ontwerp zoveel mogelijk te scripten en automatiseren
9. Everything as Code. De IT-infrastructuur wordt in code configuraties vastgelegd en vanuit centrale repositories gedeployed.
10. Composable & Loosely coupled. Door functie en dienst te scheiden is het eenvoudig om deze los van elkaar aan te passen en te verbeteren.
11. Digital first & first time right. Door processen zo ver mogelijk te automatiseren vinden menselijke interventies alleen plaats waar deze hoge waarde in de keten leveren. Door processen en techniek goed in te richten is de privacy van gegevens geborgd en zijn DPIA's en informatieverzoeken uit te voeren.

12. Security and Privacy by design. Door processen en techniek goed in te richten en verantwoordelijkheden in rollen te borgen, is de gehele bedrijfsvoering robuust en wordt controleerbare kwaliteit geleverd.
13. Marktstandaarden. Gebaseerd op best practices en proven technology. De geboden oplossing en de daarin gebruikte componenten bestaat volledig uit industrie standaarden en bewezen technologieën.
14. Reliable design. Ontwerp met de gestelde kaders en eisen in het achterhoofd en toon aan dat het ontwerp hieraan voldoet.
15. Standaard gaat voor maatwerk. Maatwerk leidt tot inflexibiliteit van de IT-omgeving als geheel. Door maatwerk kunnen vernieuwingen niet eenvoudig worden doorgevoerd of zelfs worden tegengehouden.
16. Bewezen oplossingen. Kies een standaard bouwblok/oplossing (klant-, leverancier- of marktstandaard) in plaats van zelfbouw.
17. Just enough, just in time. Ontwikkel samen die architectuur-componenten waaraan nu behoefte is om verder de realisatie vorm te kunnen geven.
18. TOGAF. Dit model wordt gehanteerd bij het ontwikkelen van de architectuur.
19. Onze architectuur wordt vastgelegd in Blue Dolphin en onderhouden door de landschapseigenaren.