Provincie Noord-Brabant

Visie PNB managed SOC-dienstverlening

Datum : 25 maart 2024
Casenummer : C2329203

Inhoudsopgave

1 Achtergrond en context

Provincie Noord-Brabant (hierna: PNB) is voornemens de dienstverlening voor managed SOC uit te besteden aan een ervaren externe gespecialiseerde dienstverlener. Voor u ligt de visie van PNB op de dienstverlening op het gebied van managed SOC.
Dit document is geschreven om de deelnemers aan de aanbesteding inzicht te geven in de gedachtegang van PNB en wat zij zoekt in de te leveren dienstverlening en dienstverlener.

1.1 Provincie Noord-Brabant

De provincie 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: De provincie 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 de provincie Noord-Brabant de realisatie van een aantal van onze belangrijke grote projecten.
SLIM: De provincie 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 de provincie 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 de provincie investeert in Brabant om ook in de toekomst die toppositie te kunnen behouden. Want dankzij die toppositie is Brabant een prachtige provincie om in te wonen en te werken.

Kernwaarden
De provincie stáát voor Brabant als kleurrijke, ondernemende en sociale provincie. In het verlengde van deze richtinggevende 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 de provincie interne en externe belangen en brengt deze samen. Ze kijkt van buiten naar binnen, werkt samen met partners en stimuleert onderlinge samenwerking.
- Doortastend
  De provincie 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. De provincie 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: de provincie 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 de provincie bereiken door samen, slagvaardig en slim te werk te gaan.

Meer informatie over de provincie is te vinden op **www.brabant.nl**.

1.2 Highlights IT-visie

PNB is een organisatie die constant in beweging is. Deze beweging wordt gevoed vanuit haar visie en ambitie (zie hoofdstuk 1.1), gestuurd door markt- en maatschappelijke ontwikkelingen, beïnvloed door politieke besluiten en geholpen door technische vernieuwingen.

Deze veranderingen hebben een sterke invloed op de manier waarop PNB kijkt naar ICT en hoe zij e.e.a. vertaalt naar doelstellingen, een bijpassende strategie en het organisatie- en governancemodel. Zoals hierboven al genoemd wordt de PNB ICT-strategie mede bepaald door ontwikkelingen in de ICT-markt. Voor de komende jaren zien wij met name de volgende ontwikkelingen als beleidsbepalend:

- Steeds snellere verSaaSing van het applicatielandschap
- Adoptie van de publieke cloud
- Focus op datagedreven werken
- Sterke stijging cybercriminaliteit en daarmee samenhangende noodzakelijke verhoging van de cyberweerbaarheid en aandacht voor privacy
- Toename hybride werken: any place any time any where
- Verbetering verduurzaming technologie
- “Alles as-a-Service” inclusief “betalen naar gebruik”
- Professionalisering van bring your own werkplekken

PNB heeft de afgelopen jaren een snelle ontwikkeling doorgaan. Werken onder architectuur is geïnitieerd. Dit wordt ondersteund door een lopende implementatie van Blue Dolphin met het doel inzicht te bewaren en snel te kunnen schakelen bij nieuwe projecten. Voor de belangrijkste dienstengebieden zijn visie en beleidsdocumenten opgesteld. Denk hierbij aan de *Cloud Visie* en *Cloud Governance,* inclusief *Financial Goverance*, 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 tooling de belangrijkste threats 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 is PNB gestart met een *Competence Center (CC)*. Door middel van onboarding en consultancy richt het zich nu nog met name op de beweging naar de public en private cloud. Ook wordt door het CC de visie op de werkplek en de visie op het netwerk verder uitgewerkt. Daarnaast wordt er druk ontwikkeld richting een security roadmap.
Het PNB-doel is om voor alle dienstengebieden een duidelijke roadmap te hebben waarin we zowel Life Cycle Management als toekomstige technologische ontwikkelingen zijn vastgelegd zodat ze ook in de uitvoeringsagenda meegenomen worden.

Samen met de IT-leveranciers wil PNB deze roadmaps verder ontwikkelen. Met het doel een omgeving te creëren die gebaseerd is op blijvend betrouwbare diensten.
PNB is ambitieus en er is zeker nog veel te doen. Vooral op het gebied van het ondersteunen van data integratie en van de koppelingen naar de leveranciers zal binnen de ICT-organisatie een verdere professionalisering worden doorgevoerd waar het gaat om de project- en beheeraanpak.

Naast de interne en ICT-marktontwikkelingen houdt PNB ook rekening met andere belangrijke factoren, waarvan, voor ICT, wellicht een van de belangrijkste is te vinden in de maatschappelijk ontwikkeling: tekort aan gekwalificeerd personeel. De provincie is een aantrekkelijke werkgever. Op het gebied van ICT zien we dat de zeer ervaren ICT-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, zijn eigen specialisten in dienst te nemen.

De snelle ontwikkelingen, het gebrek aan interne specialisten en de overgang naar SaaS, cloud, overige as-a-service diensten en de groei van outsourcing van IT-diensten overtuigt PNB om de transitie naar een regie-organisatie door te zetten. En gelijktijdig zo veel als mogelijk haar standaard ICT-dienstverlening uit te besteden aan gespecialiseerde marktpartijen. Partijen die bij uitstek geschikt zijn om diensten die voor de provincie als gespecialiseerd worden gezien, toch als standaard dienst te leveren.

Dit maakt dat ICT PNB zich kan richten op datgene waar ze werkelijk waarde toevoegt aan “de business”.

Dit zal het ICT-landschap en daarmee de provincie 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 ICT;
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 service integratie en contract- en leveranciersmanagement.

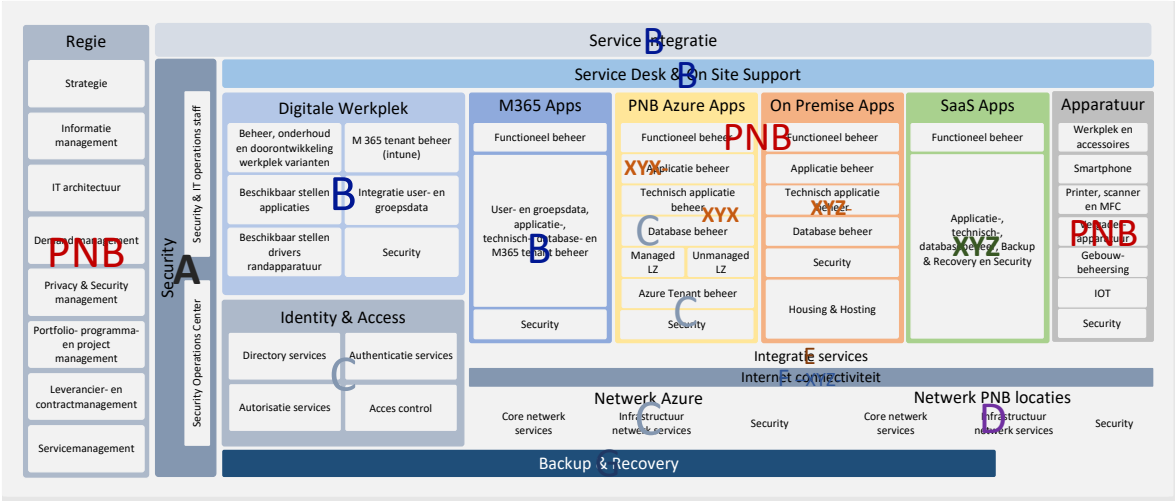
De invoering van de nieuwe structuur van de regieorganisatie is gestart in 2023 en het project loopt door tot eind 2024. Het project zal daardoor parallel lopen aan de aanbesteding.

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 leveranciers geleverd worden. Over de regievoering en samenwerking geeft hoofdstuk 6 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:



Kavel	Beschrijving
Regie	Betreft het organiseren van een soepele, integrale ICT-dienstverlening, waarbij onderdelen van de dienstverlening geleverd worden door verschillende interne oplosgroepen en externe

	dienstverleners. Regie is zowel gericht op het managen van de vraag naar dienstverlening (demand) als op de levering van dienstverlening (supply). Regie omvat daarvoor activiteiten op zowel strategisch, tactisch als operationeel niveau. PNB blijft dit kavel zelf uitvoeren.
Kavel A Security (Managed SOC-dienstverlening)	Betreft het leveren, onderhouden en doorontwikkelen van een security operations center voor Managed Detection and Respons. Het ontwikkelen en beheren (change en run) van securityactiviteiten samen met de verschillende dienstverleners uit de andere kavels en de aansluiting van IT-beveiligings- en IT-operations teams (of binnen één team) zodat alle diensten veilig zijn en blijven. PNB besteedt dit kavel uit. Opmerking: de oorspronkelijke benaming voor dit kavel is voor de onderhavige aanbesteding aangepast naar Managed SOC-Dienstverlening.
Kavel B Digitale Werkplek & M365 Apps & Service integratie & IT ServiceDesk & On-Site Support	Betreft de volgende onderdelen: – Digitale werkplek: het digitaal werkplekconcept met onderliggende infrastructuur en platformen waarmee de productiviteit van medewerkers wordt geoptimaliseerd en efficiënte samenwerking op een veilige manier tussen medewerkers en afdelingen wordt gefaciliteerd. – M365 Apps: het op een veilige manier aan gebruikers beschikbaar stellen van M365 applicaties vanuit de M365 tenant aan de PNB-medewerker op de digitale werkplek, het borgen van de veiligheid, beschikbaarheid en continuïteit van de toegang tot deze applicaties, het voeren van noodzakelijk onderhoud en het ondersteunen van de PNB-medewerker op het gebied van functionele vragen. – Service integratie: het integraal coördineren van externe leveranciers en interne oplosgroepen die onderling afhankelijke onderdelen van de dienstverlening leveren, zodat deze dienstverlening door de klant als één geheel ervaren wordt. Service integratie is voornamelijk gericht op het (operationeel) aansturen van leveranciers (de supply kant) zodat de end to end dienstverlening aan de klanteisen voldoet. – IT Servicedesk & On Site Support: het aanspreekpunt voor alle eindgebruikers bij vragen of problemen en ze handelt deze vervolgens in samenwerking met verschillende dienstverleners af. Onsite support levert ondersteuning op locatie aan eindgebruikers PNB besteedt dit kavel uit met uitzondering van het functioneel beheer. NB: De SI-rol wordt eerst intern versterkt om de volwassenheid van de regieorganisatie direct te verhogen en om een goed beeld te vormen van de rol die later uitbesteed moet gaan worden. De IT Service Desk & On Site Support wordt in eerste instantie losgeweekt van het Servicepunt en ondergebracht bij de regieorganisatie. Dit om de kwaliteit van de dienstverlening direct te verhogen. Waarna deze dienstverlening ook ondergebracht kan worden bij de dienstverlener van dit kavel.
Kavel C PNB Azure Apps & Identity & Access & Netwerk Azure	Betreft de volgende onderdelen: – PNB Azure Apps: Het op een veilige manier aan gebruikers beschikbaar stellen van applicaties vanuit de Azure (niet-M365) tenant aan de PNB-medewerker via een van de Digitale werkplekken, het borgen van de veiligheid, beschikbaarheid en continuïteit van de toegang tot deze applicaties, het voeren van noodzakelijk onderhoud en het ondersteunen van de PNB-medewerker op het gebied van functionele vragen, het aanbieden en beheren van de managed landingszones en aanbieden van unmanaged landing zones. Het applicatiegedeelte van PNB Azure Apps wordt door verschillende (reeds gecontracteerde) dienstverleners uitgevoerd, voor die PNB Azure Apps waar PNB niet zelf het Azure operations-deel binnen Azure kan ondersteunen verwacht PNB van de dienstverlener dat hij deze kan ondersteunen. – Identity & Access: Alle processen binnen PNB gericht op het beheren van gebruikers en toegangsrechten binnen de netwerkomgeving. Inclusief het centraal valideren van de identiteit van gebruikers en het inregelen van de toegang van die gebruikers tot bedrijfsgegevens en applicaties. – Netwerk Azure: De netwerkservices in Azure die verschillende netwerkmogelijkheden bieden die samen of afzonderlijk kunnen worden gebruikt. Deze zijn onderverdeeld in infrastructuur en netwerkservices. PNB besteedt dit kavel uit exclusief het functioneel beheer.
Kavel D Netwerk PNB Locaties	De netwerkservices op diverse locaties die verschillende netwerkmogelijkheden bieden die samen of afzonderlijk kunnen worden gebruikt. Deze zijn onderverdeeld in infrastructuur en core netwerkservices. PNB besteedt dit kavel uit.
Kavel E Integratie services	Het platform inclusief dienstverlening waarop mogelijk wordt gemaakt dat systemen en applicaties met elkaar communiceren door middel van zoveel als mogelijk moderne integratie (API's). Hierdoor is de integratie services het spil in het applicatielandschap. PNB besteedt dit kavel uit.
Kavel F Internet connectiviteit	Het op een veilige manier aan gebruikers toegang bieden tot (externe) diensten via een Internet connectie. PNB besteedt dit kavel uit.
Kavel G	Het op een veilige manier maken en opslaan van kopieën van PNB-data en terughalen/terugzetten van een deel van of de gehele kopie naar een eerder punt in tijd op basis van een selfservice

Backup & Recovery	model. Overige kavels zullen zich moeten conformeren aan het back-up beleid van PNB en hun deel in het back-up proces moeten waarborgen. PNB besteedt dit kavel uit.
Apps PNB locaties en remote Apps	Betreft het op een veilige manier aan gebruikers beschikbaar stellen van PNB-locaties applicaties vanuit het provinciehuis DC of remote applicaties vanuit Equinix aan de PNB-medewerker via de Digitale werkplek, het borgen van de veiligheid, beschikbaarheid en continuïteit van de toegang tot deze applicaties, het voeren van noodzakelijk onderhoud en het ondersteunen van de PNB-medewerker op het gebied van functionele vragen. PNB besteedt dit kavel uit met uitzondering van het functioneel beheer. Het beheer van de applicaties zelf ligt bij derde partijen.
SaaS Apps	Betreft het op een veilige manier aan gebruikers toegang bieden tot extern, via Internet, aangeboden SaaS-applicaties via een van de drie digitale PNB-werkplekconcepten, het borgen van de veiligheid, beschikbaarheid en continuïteit van de toegang tot deze applicaties en het ondersteunen bij technische servicedesk vragen. PNB besteedt dit kavel uit.

2 Doelstellingen en scope

2.1 Doelstellingen

De aanbesteding en het navolgende project hebben, op basis van de visie, doelstellingen, strategie, kwaliteitseisen en verwachtingen in dit document, als doel:

1. Het contracteren van één dienstverlener die, op basis van de SOC-dienstverlening, er samen met PNB voor zorg draagt dat PNB een afdoende niveau van security bescherming en compliance heeft waarmee PNB in staat wordt gesteld om aantoonbaar de bedrijfsprocessen uit te voeren binnen haar risicobereidheid.
2. Een succesvolle onboarding van de dienstverlener van de bestaande situatie zonder onderbreking van de dienstverlening.
3. Het inrichten van de security operations dienstverlening conform de overeengekomen service levels.
4. Het continu doorontwikkelen (zoals logging, use cases, etc.) van een toekomstbestendige SOC-dienstverlening en inrichting onderliggende tooling.
5. De basis leggen voor een samenwerkingsverband waarin wederzijds waarde bestaat in het werken aan kwaliteit, continue verbeteringen en innovatie. Transparantie is het uitgangspunt van de samenwerking.

2.2 Scope

De scope omvat het volgende:

1. De overgang naar en inbedding van de managed SOC-dienstverlener inclusief overname huidige dienstverlening.
2. Het uitvoeren en onderhouden van SOC-dienstverlening en het functioneel beheren van de in scope van de dienst zijnde security applicaties.
3. In samenwerking met PNB het doorontwikkelen van de SOC-dienstverlening.

1. De overgang naar en inbedding van de managed SOC-dienstverlener inclusief overname huidige dienstverlening.

De volgende producten, diensten of activiteiten behoren in ieder geval tot de scope:

1. Opstellen en afstemmen van het plan van aanpak voor de onboarding met PNB.
2. Overnemen van het beheer van de huidige draaiende PNB security tooling en de daarbij behorende processen inclusief opzet en uitvoering van communicatie naar alle oplosgroepen en externe leveranciers.
3. Inrichten SOC-dienstverlening tot overdracht naar beheer.
4. Quick wins implementeren op het gebied van SOC- en onboardingsprocessen.
5. Realiseren van de benodigde koppelingen voor triage en bewaken van de voortgang van de afhandeling van de incidenten inclusief processen, dashboards en rapportages.

2. Het uitvoeren en onderhouden van de SOC-dienstverlening en het functioneel beheren van de in scope van de dienst zijnde security applicaties.

De volgende producten, diensten of activiteiten behoren in ieder geval tot de scope:

1. Leveren van reactief, proactief en perfectief functioneel beheer van de SOC-dienstverlening.
2. Het reageren op security meldingen, het afhandelen daarvan in samenwerking met PNB en/of partners binnen de SOC-dienstverlening (waarbinnen het incident is vastgesteld) dan wel samenwerken met PNB en/of partners buiten de SOC-dienstverlening indien die gelieerd is aan de dienstverlening en het begeleiden van het incident management proces.
3. Opstellen, up-to-date houden en beschikbaar stellen van de documentatie van alle onderdelen van de SOC-dienstverlening en hieronder vallende componenten.
4. Het continu integreren van de SOC-dienstverlening met nieuwe PNB partners en/of leveranciers en deze onboarden of offboarden.
5. Verantwoording nemen voor triage en het bewaken van de voortgang tot het moment van oplossing conform SLA.

3. In samenwerking met PNB het doorontwikkelen van de SOC-dienstverlening.

De volgende producten, diensten of activiteiten behoren in ieder geval tot de scope:

1. Doorontwikkelen zodat bestaande en toekomstige use cases onderhouden worden en dat nieuwe technologieën (bijvoorbeeld IoT/OT) aangesloten kunnen worden op de SOC-dienstverlening inclusief bijbehorende uses cases.
2. Compliance rapportages opstellen en acties daarop nemen op afwijkingen met een security risico.
3. Het samen met PNB opstellen van de roadmap security dienstverlening en deze samen met PNB ten uitvoer brengen.

2.3 Optioneel in scope van de opdracht[1]

1. Participatie in BCM test processen
2. Invulling geven aan uitvoeren van jaarlijkse pentest(en)

[1] 1 Optioneel in scope betekent dat gedurende de contractperiode deze onderdelen mogelijk onderdeel kunnen worden van de opdracht. Optionele onderdelen in scope zijn nu geen verplicht onderdeel van de opdracht.

3 Visie op architectuur

3.1 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)[2] 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.

3.2 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.

[2] 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.

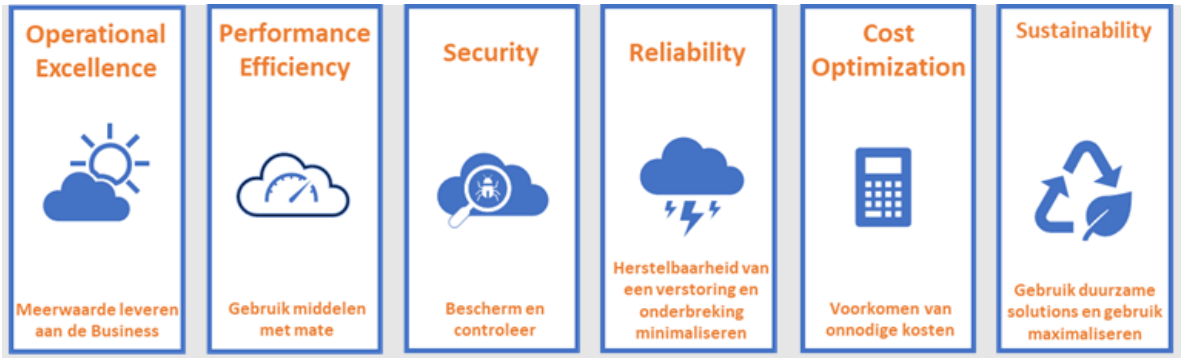
De Application en Presentation services bieden het merkbare en zichtbare: een desktop, applicaties, portals, e-mail, et cetera. Deze worden beheerd en bestuurd door de onderliggende “onzichtbare” infrastructuur, platform en datacenter services. Over alle lagen heen zijn de security en managementservices 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

3.3 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.



3.4 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.

4 Visie op de informatiebeveiliging en privacy

4.1 Informatiebeveiliging

Het uitgangspunt van PNB betreffende informatiebeveiliging wordt als volgt omschreven: Het treffen en het continue onderhouden van een samenhangend geheel van het beheren van de processen tot en met de maatregelen om de betrouwbaarheid van de informatievoorziening van PNB aantoonbaar (ISO 27001 en de baseline informatiebeveiliging Overheid (BIO)) te kunnen waarborgen. Kernpunten hierbij zijn beschikbaarheid, integriteit en vertrouwelijkheid van de informatie waar de Provincie Noord-Brabant verantwoordelijk voor is.

- 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 kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Dit geldt voor alle processen van PNB zodat de informatievoorziening gedurende de hele levenscyclus van informatiesystemen wordt geborgd, ongeacht de toegepaste technologie en het karakter van de informatie. Informatiebeveiliging binnen PNB beperkt zich dus niet alleen tot de ICT-omgeving. Het heeft betrekking op alle medewerkers, burgers, gasten, bezoekers en externe relaties van de provincie.

4.2 PNB visie

PNB is voor een correcte uitvoering van haar taken in sterke mate afhankelijk van een goed functionerende informatievoorziening. Het uitvallen van informatiesystemen of het door onbevoegden kennisnemen, wijzigen en/of verwijderen van informatie kunnen verstrekkende gevolgen hebben voor:

- De maatschappelijke doelstellingen van PNB
- Het imago van PNB
- De uitvoering van processen en financiën van PNB

Op deze wijze geeft de provincie invulling aan de relevante landelijke en Europese wet- en regelgeving op het gebied van informatiebeveiliging zoals onder meer:

1. NEN-ISO 27001
   De NEN-ISO 27001 is de internationale standaard voor het implementeren en borgen van informatiebeveiliging binnen een organisatie. Het NEN-ISO 27001 certificaat is het bewijs dat de betreffende organisatie de nodige voorzorgsmaatregelen heeft genomen om haar informatie op een adequate wijze te beschermen tegen ongeautoriseerde toegang en of bewerking. De norm staat voor een procesmatige aanpak voor het vaststellen, implementeren, uitvoeren, bewaken, onderhouden en verbeteren van informatiebeveiliging op basis van een Information Security Management System.

2. Baseline Informatiebeveiliging Overheid
   De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen) en is vanaf 1 januari 2019 van kracht om de veiligheid op het gebied van informatiebeveiliging binnen de overheid verder te vergroten. Waar in het verleden iedere overheids-laag zijn eigen baseline had is er met gezamenlijke inspanning één baseline voor de gehele overheid ontwikkeld de Baseline Informatiebeveiliging Overheid (BIO). De BIO heeft alle bestaande baselines informatieveiligheid voor het Rijk, de Gemeenten, waterschappen en Provincies vervangen. Hierdoor is er één gezamenlijk normenkader voor informatiebeveiliging ontstaan binnen de gehele overheid, welke gebaseerd is op de NEN-EN-ISO/IEC 27001:2017 en de NEN-EN-ISO/IEC 27002:2017.

3. NIS2 Richtlijn
   De NIS2-richtlijn oftewel de Network and Information Security directive, is de opvolger van de huidige NIS-richtlijn. De nieuwe NIS2 richtlijn is inmiddels vastgesteld door de Europese Unie en bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten verder te verbeteren. De NIS2 vergroot de reikwijdte van de voorgaande richtlijn door meer sectoren te omvatten. Daarnaast stelt de richtlijn veel strengere beveiligingseisen en meldingsvereisten voor incidenten. Op dit moment wordt de NIS2 naar de Nederlandse wetgeving vertaald.

4.3 Randvoorwaarden ketenpartners:

Informatiebeveiliging stopt niet bij de provinciale organisatie maar maakt in de huidige tijd ook steeds meer deel uit van de bedrijfsvoering van ketenpartners waar door de provincie diensten afgenomen worden. Om deze reden hanteren we daarbij dan ook de volgende uitgangpunten.

1. Dienstverlener is ISO 27001 gecertificeerd en conformeert zich aan de BIO voor additionele eisen voor de procesmatige inrichting van de informatiebeveiliging en is gecertificeerd met een verklaring van Toepasselijkheid (VvT) voor de volledige scope van de te leveren dienstverlening;
2. Dienstverlener conformeert zich aan de Baseline Informatiebeveiliging Overheid (BIO) op niveau BBN2 voor de volledige scope van geleverde dienstverlening;
3. Dienstverlener zegt toe zich vanaf ingangsdatum aan de toekomstige NIS2 wetgeving voor de volledige scope van geleverde dienstverlening te conformeren.

4.4 Privacy

De provincie is gegevensverwerker in de zin van de AVG. Dat betekent dat zij voor de uitvoering van haar taken als provincie en als werkgever gegevens verzamelt en verwerkt. Een adequate bescherming van deze persoonsgegevens is uitermate belangrijk. Burgers, medewerkers in organisaties en medewerkers van de provincie zelf hebben recht op een maximale bescherming van hun persoonlijke informatie.
PNB voldoet dan ook aan de actuele wetgeving en voorschriften vertaald in de AVG. Dat betekent dat belanghebbenden van de provincie 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 de provincie waarbij zij persoonsgegevens bewerken. En waarvoor ze een verwerkersovereenkomst hebben getekend.

5 Visie op managed SOC-dienstverlening

5.1 Inleiding

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 kavels, 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.

Het kiezen van de juiste partner is essentieel. 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.

Als provinciale overheidsinstelling staan wij voor de uitdaging om onze ICT-omgeving te optimaliseren en te moderniseren, met als uiteindelijk doel: de levering van excellente dienstverlening aan onze interne organisatie, inwoners, bedrijven en partners. PNB is op zoek naar versnelling van levering en de wendbaarheid van de ICT-omgeving. Heldere afspraken over producten, diensten en kwaliteitsniveaus helpen daarbij. Doorlooptijden moeten naadloos passen in de werkwijzen van PNB. Het aanvragen en verkrijgen van (nieuwe) producten of diensten moet laagdrempelig zijn en de PNB-gebruikers ervaren hierbij uitstekende ondersteuning.

Het voorgaande wordt vastgelegd in diverse documenten die beknopt en helder moeten zijn voor alle betrokken partijen, zoals:

- Een dienstbeschrijving
- Een Service Level Agreement (SLA) op hoofdlijnen
- Een Dossier van Afspraken (DAP) met detailafspraken en KPI's waarmee we de kwaliteit van de geleverde dienst meten en hoe daarop gerapporteerd wordt

5.2 ITIL

Om gestructureerd en procesmatig werken te ondersteunen werkt de PNB momenteel aan de implementatie van een aantal ITIL-processen, gebaseerd op ITIL-versie 3. We verwachten van de leveranciers dat zij ook hun supportprocessen conform ITIL hebben ingericht en dat ze aansluiten op de processen van de PNB. Ten aanzien van het beheren en onderhouden van het SOC-omgeving verwacht PNB dat de dienstverlener alles doet om verstoringen te voorkomen en mochten ze zich alsnog voordoet, er alles aan doet om ze zo snel mogelijk weer op te lossen. De ITSM-tooling van PNB ondersteunt hierbij en is voor de leverancier om op aan te sluiten (API). In onderstaande tabel zijn de operationele supportprocessen opgenomen die door PNB al zijn beschreven en ook al zijn geïmplementeerd of op dit moment worden geïmplementeerd.

Operationele processen	
Proces	**Beschrijving**
Incident Management	Het proces is gericht op het zo snel mogelijk oplossen van verstoringen en de communicatie naar de medewerkers. Hier is een primaire rol voor de IT-servicedesk weggelegd in de samenwerking met andere oplospartijen en dienstverleners. Zo is de IT-servicedesk 8x5x365 verantwoordelijk voor registratie, dispatch en monitoring. Een deel van de omgeving is missie-kritisch. Deze onderdelen dienen derhalve 24x7x365 beschikbaar te zijn. Op termijn gaat om die reden de dienstverlening naar 24x7x365, in

	nauwe samenwerking met de dienstverleners. De rol van de Incident Manager wordt op termijn bij de IT-servicedesk belegd.
Problem Management	Het proces is gericht op (proactief) wegnemen van fouten in de IT-omgeving. De dienstverleners zijn hiervoor binnen hun eigen domein van dienstverlening verantwoordelijk. De dienstverleners zoeken daarin uiteraard nadrukkelijk met elkaar de samenwerking op. Binnen de PNB is een Problem Manager als procesbeheerder aanwezig en zal met een counterpart van de dienstverlener in contact staan over openstaande Problems.
Change Management	Releases en changes met impact op de IT-infrastructuur worden besproken en afgestemd in het CAB van de PNB, met de Change Manager van de PNB, andere betrokken partijen en dienstverleners. Iedere dienstverlener is verantwoordelijk voor de uitvoer van de eigen changes in samenwerking met andere dienstverleners.
Service asset and configuration management	Het registeren en updaten van assets is de verantwoordelijkheid van de leveranciers van de diensten. Het eigendom van de CMDB ligt bij PNB. Dienstverleners zijn tenminste verantwoordelijk voor het invoeren, actualiseren en correct, tijdig en volledig bijhouden van de CMDB voor de hardware- en software en services voor zover die hen raakt. Dit wordt gedaan in de ITSM-tooling instance van PNB (single source of truth). De dienstverlener heeft een uitvoerende (invoeren/uitgeven/muteren) rol in het CMDB-proces en communiceert hierover met de Configuratie Manager van de PNB.

Naast bovenstaande processen heeft PNB nog een aantal processen geïdentificeerd die op termijn moeten worden geïmplementeerd:

- Service Level Management
- Service Validation and Testing

Deze processen zijn nog niet uitgewerkt. Hieronder een beknopte omschrijving wat PNB hiermee wil bereiken.

Operationele processen	
Proces	**Beschrijving**
Service Level Management	Het proces wordt gebruikt om IT-service levels overeen te komen, te monitoren en te reviewen. Met dit proces wordt geborgd dat de IT-provider en de business begrijpen en overeenkomen welke servicelevels geleverd gaan worden. We beschrijven niet alleen wat we overeenkomen met de leverancier maar vertalen dit naar de interne stakeholders van PNB, denk aan OnsLoket, de vakgroepen en de eindgebruikers. De benodigde rol voor dit proces is: Service Level Manager. Bij PNB is dit een bestaande rol die momenteel wordt ingevuld door de Service Delivery Managers.
Service Validation and Testing	Het proces omvat het verminderen van de risico's en onzekerheden die nieuwe of gewijzigde producten en diensten in de live-omgeving introduceren. Ook wordt getoetst of deze producten en diensten voldoen aan de design specs of ze aansluiten bij de business behoefte. Dit wordt bereikt door passende testen te plannen en uit te voeren. De benodigde rol voor dit proces is: Test Manager. Bij de PNB is dit een bestaande rol die momenteel wordt ingevuld door de Testcoördinator in nauwe samenwerking met het Change Management proces.

5.3 Managed SOC-dienst

Uitgangspunt: *PNB wenst op aantoonbare wijze op het afgesproken niveau in control te zijn. De reikwijdte hierbij is de gehele informatievoorziening*.

Ambitie en doelen:

1. Op aantoonbare wijze:
    a. De operationele uitvoering van de SOC-processen levert afdoende auditbewijs op dat BIO-compliance is aangetoond.
    b. De cyber risico's worden aantoonbaar gemitigeerd op het overeengekomen niveau.
2. Een doorlopende compliance: in lijn met het PNB IT-security beleid.

3. Op het afgesproken niveau: alle relevante interne en externe stakeholders kunnen middels dashboards de compliance met de relevante BIO-controls monitoren conform de BIV-classificatie van de onderliggende componenten en de op basis hiervan geselecteerde controls.
4. De IT-infrastructuur en het applicatielandschap: De scope van de bovenstaande uitgangspunten omvat alle PNB informatie verwerkende partijen, zowel intern als extern. En de afdekking van alle voor PNB relevant geachte use cases voor de gehele omgeving, ook geborgd voor nieuwe ontwikkelingen.

5.4 Inbedden van en overgang naar managed SOC-dienstverlener

PNB ziet het inbedden in eerste instantie als een AS-IS migratie. PNB voorziet een inbedding c.q. overgang van u als managed SOC-dienstverlener naar de gewenste situatie zonder noemenswaardige verstoringen en met minimaal dezelfde tevredenheid bij de PNB-gebruikers, de regieorganisatie en de CISO. Ook de overname van het beheer van de reeds geïmplementeerde SIEM[3] applicaties en de bijbehorende processen, verloopt geruisloos. Aan het einde van de periode van inbedding heeft u de startsituatie zoals zal worden weergegeven in de gunningsdocumentatie (hiervoor is een getekende NDA vereist) en in Bijlage 4 Beschrijving huidige situatie gerealiseerd. Dat wil zeggen dat u de betreffende applicaties in uw dienstverlening heeft opgenomen en ze voor uw dienstverlening heeft geoptimaliseerd, ze beheert en onderhoudt, de leveranciers en oplosgroepen heeft ge-onboard en u heeft de huidige use cases en de SOC-dienstverlening in place en de bijbehorende logbronnen gekoppeld/in beheer genomen.
PNB gaat ervan uit dat vanaf het moment dat de inbedding start de high priority alerts worden opgepakt en opgevolgd door opdrachtnemer. De benodigde koppelingen voor triage en bewaken van de voortgang m.b.t. de afhandeling van de incidenten zijn gerealiseerd.
Quick wins op het gebied van SOC- en onboardingsprocessen worden waar mogelijk geïmplementeerd.

5.4.1 Verwachtingen

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

1. Gedegen plan van aanpak van de succesvolle inbedding en overgang

PNB verwacht een gedegen en beproefd plan van aanpak dat invulling geeft aan de succesvolle inbedding, overgang van de huidige (gedeeltelijke) invulling van de gevraagde SOC-dienstverlening en u als managed SOC-dienstverlener en dat minimaal omvat:

- De doelstellingen, scope, diensten en resultaten beschreven in hoofdstuk 2.
- Een duidelijke governance in het plan van aanpak op operationeel, tactisch en strategisch niveau, met onder andere een stuurgroep.
- Hoe u zich verdiept in de cultuur en processen van PNB.
- Een 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;
    - Gezamenlijke begrippen;
    - Acceptatiecriteria;
    - Verificatie/validatie (inclusief afwijkingenproces van de aannames gedaan bij de inschrijving);
    - Vastgestelde deliverables en diensten met heldere en realistische acceptatiecriteria en testen met daarin onder anderen, maar niet gelimiteerd tot:
        - De te bereiken quick wins in de dienstverlening (bijvoorbeeld op het gebied van use cases, hardening, compliance autorisatie inrichting en monitoring van de eigen activiteiten van beheerders, SOC-analisten, etc.).
        - Inrichtings- en koppelingseisen met en in bestaande ITSM tooling en processen van PNB, of specificaties van requirements hiervoor.

[3] SIEM bestaat onder andere uit Darktrace, Sentinel en Nessus

    - De wijze van onboarden van de reeds bestaande PNB security tooling (Darktrace, Sentinel & Nessus, logforwarders) in de dienstverlening.
    - Rapportages en dashboard inrichting.
- Een aanpak en vooraf vastgestelde methodiek (bijvoorbeeld Prince2) gebaseerd op beheersing van doorlooptijd, kwaliteit, budget en risico's.
- Een afbakening in rollen en verantwoordelijkheden en een intensieve samenwerking tussen de organisatie van opdrachtnemer, het PNB-team, de latende partij en andere betrokken dienstverleners. Opdrachtnemer maakt duidelijkheid wanneer welke en hoeveel inzet wordt verwacht.
- Een realistische, transparante planning.
- Actief kwaliteits-, risico- en incidentmanagement inclusief (risico)mitigerende maatregelen voor PNB en andere betrokken. Dit zijn zowel risico's die binnen als buiten de directe invloedsfeer van dienstverlener liggen.

2. Transitie van de huidige situatie tot einde van de inbeddingfase c.q. start FMO

PNB opteert voor een geleidelijke, geplande overgang en niet voor een big-bang scenario. Dat geldt zowel voor de inrichting van de security-tooling als voor het onboarden van de betrokken leveranciers. PNB zal opdrachtnemer voorzien van alle noodzakelijke gegevens van de leveranciers zodat opdrachtnemer daarmee verdere afspraken kan maken.
PNB verwacht dat opdrachtnemer zelf de regie heeft over het onboardingsproces met de betrokken leveranciers. PNB verwacht tevens dat opdrachtnemer direct na het afronden van de due diligence de operationeel regievoering over de uitvoerende partijen en andere betrokken dienstverleners start.
Opdrachtnemer borgt dat de defence in depth inrichting bewaard blijft tijdens het inbeddingsproces. Bijvoorbeeld doordat de authenticatie activiteiten aan de kant van de opdrachtnemer actief beschermd dienen te zijn middels het defence in depth principe. Opdrachtnemer toont op basis van het plan van aanpak en eerdere ervaringen aan dat het uitvoeren van het proces van inrichting, zowel technisch als operationeel als voor wat betreft besturing succesvol en gecontroleerd wordt uitgevoerd.

3. Herinrichting Sentinel

PNB verwacht dat opdrachtnemer naast het continueren van de huidige omgeving z.s.m. start met de herinrichting van Sentinel conform de standaarden van opdrachtnemer. Dit betekent (ver)bouwen met de winkel open. Hierbij zal opdrachtnemer rekening houden met de uitgangspunten van en de dynamiek binnen de provincie. Dit vergt dat opdrachtnemer de opdrachtgever (en vv) snel beter leert kennen.
PNB gaat er van uit dat het herinrichten van Sentinel niet leidt tot een (tijdelijk) lager beveiligingsniveau.

4. Additionele verbeteringen tijdens de migratie

Om doorlooptijd en risico's te beperken hanteert PNB het uitgangspunt van een, in principe, AS-IS migratie voor de onboarding. Hiervan kan in overleg met PNB worden afgeweken indien er tijdens de migratie verbeteringen mogelijk zijn die veel waarde toevoegen of de inbedding sterk vereenvoudigen en die kunnen worden geïmplementeerd zonder negatieve impact op de doorlooptijd, continuïteit en/of kwaliteit. PNB verwacht hierbij dat opdrachtnemer het "laag hangend fruit" duidt, welke toegevoegde waarde dit voor PNB heeft, wat de impact hiervan is en wat nodig is voor een succesvolle implementatie.

5. Exit / retransitie afspraken

De provincie hecht veel waarde aan een voor alle betrokken partijen goede, duidelijke en realistische exit- of retransitie bij het beëindigen van de dienstverlening. Hierbij staat als hoofddoelstelling voor de provincie: de maximalisatie van continuïteit en beschikbaarheid van de functionaliteit tijdens een retransitie. Hiertoe stelt opdrachtnemer in de inbeddingsfase een exit- of retransitieplan op dat wordt overlegd aan en besproken met PNB. Het doel van het retransitieplan is de vastlegging van de wijze waarop de eindigende dienstverlening wordt overgedragen aan een verkrijgende dienstverlener of aan de provincie.
Het is belangrijk dat het retransitieplan gedurende de contractperiode wordt onderhouden. Jaarlijks beoordeelt de SOC-dienstverlener minimaal één keer of en in welke mate het plan moet worden aangepast. Ook bij, in de ogen van of de SOC-dienstverlener of PNB, grotere wijzigingen of projecten wordt vastgesteld of de wijziging impact heeft op het retransitieplan. Is dat het geval dan wordt dit meegenomen als onderdeel van de change. Hiermee blijft het retransitieplan continu up-to-date, zowel inhoudelijk als qua financiën. Jaarlijks wordt het plan samen met PNB geëvalueerd op actualiteit. Tussentijds kan de provincie een audit op het plan laten uitvoeren al dan niet door een derde partij.

Opdrachtnemer stelt in de inbeddingsfase een exit- of retransitieplan op waarbij minimaal wordt ingegaan op:

a) voorwaarden en uitgangspunten
b) overdracht van kennis
c) middelen
d) planning
e) transitie-organisatie en resources
f) documentatie
g) het afvoeren en vernietigen van (vertrouwelijke) informatie
h) informatiebeveiliging en privacy
i) financiële aspecten en juridische aspecten
j) verantwoordelijkheden en bevoegdheden
k) escalaties en klachten
l) IP (Intellectual Property).

Tijdens de exitperiode werkt opdrachtnemer in alle facetten volledig mee om een zorgeloze retransitie te bereiken met alle betrokkenen.

5.5 Het uitvoeren en onderhouden van SOC-dienstverlening en het functioneel beheren van de in scope van de dienst zijnde security applicaties.

5.5.1 Uitvoeren en onderhouden van SOC-dienstverlening

PNB heeft de wettelijke verplichting om volledig in control te zijn v.w.b. informatiebeveiliging en privacy. Dit betekent dat hij zijn omgeving secure en compliant moet houden en in staat is met de continu gefinetunede omgeving alerts binnen gestelde tijdslijnen te beoordelen en incidenten binnen vastgestelde KPI's op de juiste manier af te handelen. Dat vraagt om een stabiele hoogwaardige en zo veel mogelijk standaard SOC-dienstverlening die structureel wordt getest, ge-audit en verbeterd. PNB heeft de ambitie om minimaal op BBN-niveau 2 BIO-compliant zijn, wat eist dat ook de SOC-dienstverlener op hetzelfde niveau acteert. Een proactieve aansluiting van de SOC-dienstverlening op de ontwikkelingen en behoeften van de PNB-organisatie dient te worden gerealiseerd.

Opdrachtnemer richt zich primair op het leveren van de SOC-dienstverlening. Hij reageert op security en non-compliancy meldingen en handelt deze af in samenwerking met PNB en/of PNB leveranciers en oplosgroepen.
Zowel binnen PNB als bij haar dienstverleners wordt gewerkt met professionals met van toepassing zijnde kennis, ervaring en mandaat om het gewenste niveau de dienstverlening te realiseren, zodat PNB aan haar verplichtingen voldoet. PNB ervaart daarbij een professionele, snelle en stabiele dienstverlening. Support is excellent door transparante en efficiënte processen en PNB ervaart zorgvuldige, betrokken en kundige ondersteuning door de opdrachtnemer.
De dienstverlening is voorspelbaar, de opdrachtnemer is proactief, neemt het initiatief en adviseert PNB gevraagd en ongevraagd m.b.t. mogelijke verbeteringen, nieuwe functionaliteit en op noodzakelijke ingrepen.

De managed SOC-dienstverlener is verantwoordelijk voor de regievoering over de security en compliance keten. En daarmee dus voor het signaleren en registreren van security incidenten, de triage, het melden van het incident bij de betrokken leverancier of leveranciers, het monitoren van en actief sturen op de melding tot het moment dat die is opgelost, e.e.a. conform SLA. Hierbij is er een direct communicatiekanaal tussen de SOC-dienstverlener die hiervoor door PNB is gemandateerd en de applicatie- of kavelleverancier. PNB wordt hierbij volgens de afspraken geïnformeerd door de SOC- dienstverlener.

PNB zit in de transitie naar een regie-organisatie. Dit geldt ook voor de SOC-dienstverlening. PNB heeft dan ook geen operationele security specialisten in dienst, bijvoorbeeld voor het opstellen van runbooks en het functioneel beheer van haar SIEM-tooling (Darktrace, Sentinel, Tenable Nessus). Dit functioneel beheer wordt ingevuld door de te contracteren managed SOC-dienstverlener, die ook het wijzigingen van bestaande en het implementeren van nieuwe playbooks en use cases voor zijn rekening neemt. PNB zelf is uiteraard actief betrokken bij het opstellen van de use cases. Het voorstel voor basis inrichting use cases en event handling, de implementatie en de uitvoering is onderdeel van de SOC-dienstverlening.

Er vindt structureel near realtime uitwisseling van gegevens plaats tussen de ITSM-tool van PNB en die van de dienstverlener. Daarnaast levert de SOC-dienstverlener periodiek rapportages op conform de gemaakte afspraken. Daarnaast fungeert PNB als uiterste escalatiekanaal.
De managed SOC-dienstverlener is verantwoordelijk voor de juiste en tijdige ontvangst en verwerking van alle logbronnen en de onboarding binnen de security-tooling en processen van de bestaande en nieuwe applicaties en diensten en leveranciers (functioneel; technisch is niet in scope).
De managed SOC-dienstverlener draagt zorg voor periodieke scanning en rapportage ter controle van het compliance niveau. De bevindingen worden als non-compliances gemanaged. De managed SOC-dienstverlener draagt zorg voor periodieke rapportage en real time dashboarding op gebied van compliance en security threats.
Opstellen, up-to-date houden en beschikbaar stellen van de documentatie van alle onderdelen van de SOC-dienstverlening en hieronder vallende componenten.

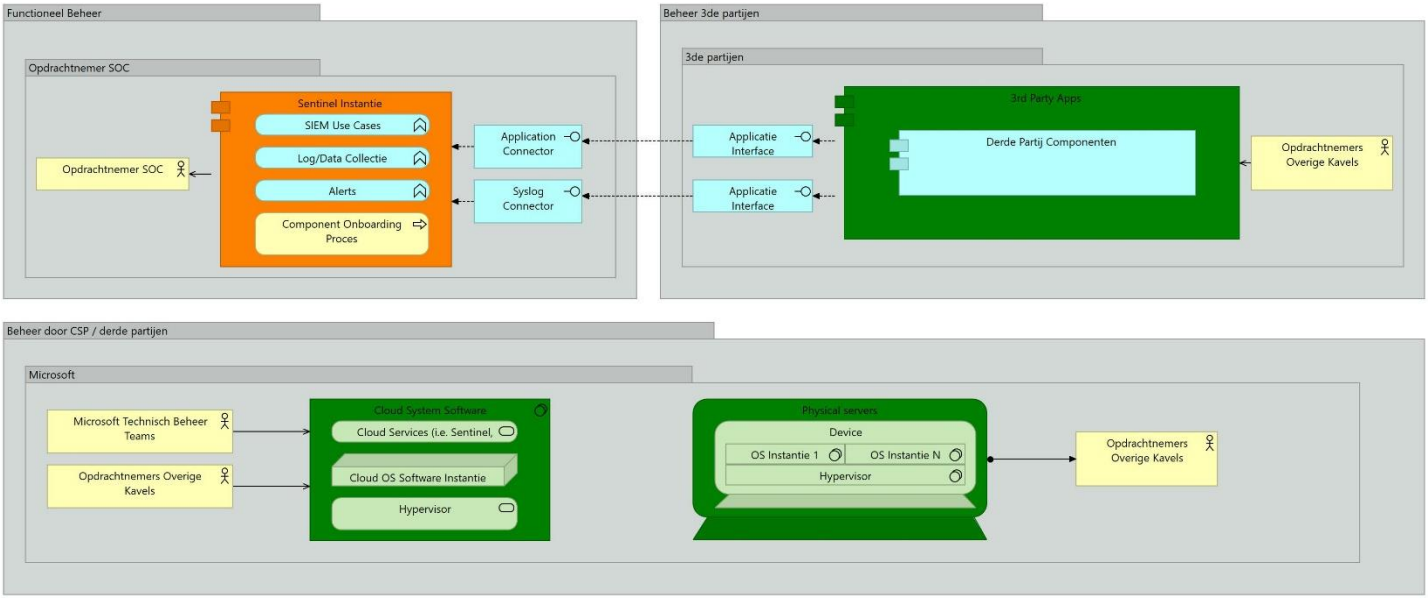
5.5.2 Functioneel beheer security applicaties

Opdrachtnemer voert functioneel applicatiebeheer over Sentinel en Nessus en hij borgt en beheert de koppeling van Sentinel naar Darktrace en Nessus. Voor de betreffende producten onderhoudt opdrachtnemer de use cases en bouwt hij nieuwe use casus op basis van de input vanuit PNB. Hij waarborgt dat de Sentinel-omgeving de juiste hygiëne en omvang (kosten efficiency) heeft noodzakelijk voor de dienstverlening. Opdrachtnemer voert trendanalyses uit op basis waarvan hij PNB adviseert. PNB doet zelf cost management op de Azure-omgeving en zal in overleg met de dienstverlener het kosten niveau besturen.

Onderdeel van de dienstverlening zijn het onderhoud aan en het life cycle management van de connectoren van de logbronnen net als het implementeren van nieuwe connectoren.
Onderdeel van de dienstverlening is het opstellen van de aansluitvoorwaarden voor leveranciers c.q. kavels.

5.5.2.1 Demarcatie functioneel en technisch beheer

In het kader van de SOC-dienstverlening is sprake van een demarcatie in de taakverdeling tussen functioneel en technisch beheer. De SOC-dienstverlener wordt geacht alle functionele beheertaken uit te voeren. Het technisch onderhoud op de onderliggende softwarecomponenten, waaronder met name Sentinel, zal worden ingevuld door Microsoft. De instantie specifieke configuratie alsook de implementatie van use cases, configuratie van connectoren ten behoeve van log en datacollectie, afhandeling van alarmen en de onboarding van componenten zijn voor rekening van opdrachtnemer. De configuratie en inrichting van componenten van derde partijen binnen de applicaties en infrastructuur van deze derde partijen is voor rekening van de derde partijen. E.e.a. hieronder grafisch weergegeven.



5.5.3 Managed SOC-dienstverlening elementen

Ten minste de volgende onderliggende SOC-diensten vallen binnen de scope van de uitvraag:

1. Security Incident Monitoring (afhandeling van security incidenten en voortgangsbewaking hierop).
2. SIEM Onderhoud & OnBoarding Log bronnen (het onderhouden van de betreffende tooling en alle aansluitingen t.b.v. logbronnen en intelligence aanlevering).
3. Security Alerts configuraties fine-tuning & management van alle aangesloten SIEM bronnen (verfijning van de inrichting ter reductie van false positive meldingen).
4. SIEM use-case ontwikkeling, fine-tuning & management (uitbreiding en optimalisatie van bestaande SIEM use cases).
5. Log & Retention Management (het beheer van informatiestromen (intelligence), log en incident informatie).
6. Centraal beheer van alle logs en incidenten (inclusief integratie met ticketing systemen incidenten / koppeling met IAM componenten voor autoresponse, het beheer van koppelvlakken met o.a. ticketing systemen, change management, CMDB en IAM-systemen).
7. Compliance. Controle vindt plaats op compliance met BIO en hardening gerelateerde instellingen. Het escalatiepad is PNB.

3.3.1. Verbijzondering

Onderdeel van de incident response dienstverlening:

1. Security Incident Resolution (het binnen de overeengekomen KPI oplossen en coördineren).
2. Incident Response Investigation: L1 (triage), L2 lijn (analyse) en L3 lijn (business impact en oplossing, joint responsibility met PNB).
3. Forensische Incident afhandeling waar nodig.
4. Security Orchestration, Automation and Response (SOAR).

Onderdeel van het vulnerability Management:

1. Vulnerability Scanning / Assessment (prioriteren en impact bepaling)
2. Vulnerability Remediation (voortgangsbewaking en bijsturing)
3. Vulnerability Governance (operationele procesbewaking/rapportage)

Onderdeel van threat intelligence:

1. Threat Feeds/Advisories (inrichten en bewaken van relevante Threat Intelligence en Advisory feeds, injecteren van IOC's hieruit in de SOC-processen).
2. Contextualiseren van geopolitieke ontwikkelingen in cyberveiligheidsbeeld (adviseren omtrent cyber actoren en hun TTP's alsmede doorvertaling naar Mitre Attack Patterns die daarvoor moeten worden ingericht als use cases in de bescherming voor de relevante componenten).
3. Threat Detection Services
4. Insider Threat Detection (UEBA)
5. Deceptie (zoals Honeypots/Fake (Birdie) accounts) management

Onderdeel van anomaly detection:

1. Threat Hunting (gericht zoeken naar vreemde zaken die indicatief kunnen zijn voor lopende besmettingen en hacks)
2. Attack surface management (externe vulnerability scanning vanaf Internet of fysieke aanvallen op Wifi en fysieke middelen met een IT-component)
3. Anti-Phishing Services (bewaking van email activiteiten)
4. Statistische en AI Use Cases (Analyse van log data)

Overige security services:

1. Red Teaming (controleren en verbeteren van de werking van de SOC-procedures en use cases)
2. OT Security Monitoring (bijvoorbeeld gladheidssensoren, VRI's, gemalen, etc.)

5.5.4 Uitgangspunten SOC-dienstverlening

Van toepassing zijnde uitgangspunten voor de managed SOC-dienst zijn o.a.:

1. De managed SOC-dienstverlener bepaalt (binnen de gegeven kwaliteitsnormen) in overleg met PNB op welke wijze de tooling wordt ge-onboard voor de dienstverlening
2. De managed SOC-dienstverlener communiceert zelfstandig met alle betrokken partijen waar het gaat over incidenten, afstemming opvolging, verdere verslaglegging, etc.
3. De managed SOC-dienstverlener faciliteert PNB voor het benodigde real time inzicht in de lopende processen voor monitoring door de PNB
4. De managed SOC-dienstverlener bouwt en onderhoudt de benodigde dashboards en rapportages voor verantwoording en sturing

5.5.5 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van de SOC-dienstverlening en het beheer van de security applicaties het volgende:

1. Dienstverlening op basis van service levels

Opdrachtnemer geeft na contracteren en tijdens de inbedding invulling aan de scope (hoofdstuk 2) en bovenstaande visie voor het uitvoeren en onderhouden van de SOC-dienstverlening en het functioneel beheer van de security applicaties.

Om de hierboven en in hoofdstuk 5 beschreven visie te bereiken verwacht PNB beheer en support op basis van servicelevels, heldere rapportages en communicatie daarover. Van dienstverlener wordt verwacht zich te verdiepen in de bedrijfsprocessen van PNB. Hierdoor wordt begrepen wat de impact van security verstoringen is op de PNB-bedrijfsvoering en operationele impact op de omgeving. De dienstverlening wordt vastgelegd in een Service Level Agreement (SLA) en het Dossier van Afspraken (DAP) waarin minimaal aan bod komen:

a. Beknopte en heldere dienstbeschrijving
b. Governance inclusief escalatie matrix: wie communiceert wanneer met wie en waarover
c. Afspraken over incidenten en zowel standaard als niet-standaard changes met doorlooptijden
d. Onbetwistbare en zoveel als mogelijk real-time rapportage over de afgesproken KPI's
e. Afspraken voor Incident Management zoals het proactief melden en oplossen van security incidenten op basis van (event) monitoring
f. De verantwoordelijk van de SOC-dienstverlener voor de regievoering over de security en compliance keten. En daarmee dus voor het signaleren en registreren van security incidenten, de triage, het melden van het incident bij de betrokken leverancier of leveranciers, het monitoren van en actief sturen op de melding tot het moment dat die is opgelost. Hierbij is er een direct communicatiekanaal tussen de SOC-dienstverlener die hiervoor door PNB is gemandateerd en de applicatie- of kavelleverancier
g. Monitoring en alerting 24*7 voor P1 situaties
h. KPI's gericht op het juist, tijdig, accuraat registreren en opvolgen van bedreigingen

2. Processen en werkwijze SOC-dienstverlening

Voor PNB is het belangrijk om goed inzicht te hebben in hoe de SOC-dienstverlener haar dienstverlening vorm geeft en invult. PNB wil graag op de hoogte zijn van ontwikkelingen, met name waar er is sprake is van afwijkingen. In de dienst en hoe de andere leveranciers reageren. Dit geeft inzicht in hoe de verhoudingen zijn tussen de opdrachtnemer en de betrokken partijen maar het kan ook input geven voor het geplande overleg tussen PNB en de betreffende leverancier. Hiervoor geeft opdrachtnemer duidelijkheid over hoe hij PNB informeert over en inzicht geeft in security incidenten en de opvolging daarvan tot en met het moment dat het incident is verholpen en afgesloten. Is opvolging conform de overeengekomen servicelevels ingevuld? Stelt opdrachtnemer eisen stellen aan PNB in dit proces of heeft ze bepaalde verwachtingen om haar diensten goed uit te kunnen voeren wil PNB hier graag inzicht in hebben.
PNB gaat er van uit dat een ervaren SOC-dienstverlener een uitgekristalliseerde en standaard aanpak heeft ingeval de servicelevels niet worden gehaald. Graag wil de provincie inzicht in deze standaard aanpak rekening houdend met een diversiteit aan incident niveaus (bijvoorbeeld: high, medium, low).
PNB wil graag inzicht in hoe en waarover opdrachtnemer de provincie rapporteert m.b.t. security incidenten. Het is voor PNB erg belangrijk goed en tijdig te worden geïnformeerd zodat tijdig kan worden ingegrepen of besluiten worden genomen. Geef aan hoe u de provincie gedurende de contractperiode structureel en tijdig informeert over nieuwe relevante ontwikkelingen en functionaliteit.

3. Detectie en respons

PNB verwacht van de opdrachtnemer dat deze een volwassen niveau van detectie implementeert en onderhoudt, dat wil zeggen: kwalitatief afdoende om de huidige dreigingen te detecteren en tijdig af te kunnen handelen. Hierbij rekening houdend met up to date intelligence informatie van zowel interne als externe bronnen. E.e.a. passend bij de actoren die middels rapportages van relevante partijen zoals NCSC en AIVD van toepassing worden geacht op de overheid.
PNB verwacht van opdrachtnemer dat hij een standaard en bewezen aanpak heeft m.b.t. het detecteren en identificeren van security-afwijkingen. Inzicht in de aanpak en het proces en de effectiviteit is relevant voor PNB. Net als hoe de SOC-dienstverlener de ingezette detectielogica up to date en relevant houdt en hoe afwijkende activiteiten worden gedetecteerd.
Respons en classificatie wordt met vastgelegd in een set business rules:

- Kritische events: er wordt automatisch direct ingegrepen volgens afspraak. Vervolgens wordt dit in het reguliere proces afgehandeld als security incident;
- Waarschuwingen: ze worden verzameld, gerapporteerd en ter beoordeling aan PNB voorgelegd en besproken in het periodiek overleg. Op basis van de beoordeling wordt ingegrepen of classificatie aangepast;
- Informal: worden geaggregeerd en gerapporteerd voor trendanalyse.

4. Functioneel applicatiebeheer

PNB verwacht dat opdrachtnemer waarborgt dat de Sentinel omgeving de juiste hygiëne en omvang (kosten efficiency) heeft noodzakelijk voor de dienstverlening. Opdrachtnemer voert trendanalyses uit op basis waarvan hij PNB adviseert. Voor PNB is het zeer relevant goed inzicht te hebben in het proces dat opdrachtnemer hieraan ten grondslag heeft liggen en waar resultaten uit de analyses worden ingezet in de dienstverlening en de processen, ook binnen en met de provincie, te verbeteren. Helderheid bijvoorbeeld over op welke wijze opdrachtnemer PNB meeneemt in de trends en ontwikkelingen m.b.t. kostenefficiency en kwaliteitsverbetering en op welke terreinen opdrachtnemer PNB adviseert zijn van toegevoegde waarde. Ook wil de provincie een beeld hebben op welke wijze opdrachtnemer invulling geeft aan life cycle management op de connectoren van de bestaande logbronnen net als op die van de nieuwe connectoren.

5.6 Optimalisatie en doorontwikkeling SOC-dienstverlening

Na afronding van de inbeddingsperiode en met de start van de future mode of operations (FMO) is het voor PNB belangrijk dat de dienst verder wordt geoptimaliseerd en het aantal benodigde resources voor invulling van de use cases verder wordt gereduceerd doordat opdrachtnemer binnen de omgeving van PNB in staat is de ontwikkeling en implementatie van de use cases steeds slimmer in te vullen. Dit moet leiden tot het reduceren van de complexiteit en afhankelijkheden naast dat het leidt tot het verlagen van de kosten.
Waar PNB verantwoordelijk is voor het aanleveren van de use cases, is opdrachtnemer samen met PNB verantwoordelijk voor het verder ontwikkelen van de use cases. Opdrachtnemer implementeert ze.
Opdrachtnemer is, in overleg met PNB, tevens actief in het optimaliseren van het incidentproces. Hij heeft dan ook niet alleen aantoonbaar veel kennis en ervaring op het gebied van use cases en van incidentproces optimalisatie, maar ook in het samenwerken met opdrachtgever m.b.t. het initiëren en uitwerken daarvan.

5.6.1 Verwachtingen

Om de hierboven beschreven visie te bereiken verwacht PNB ten aanzien van de SOC-dienstverlening en het beheer van de security applicaties het volgende:

1. Blijvend up to date

PNB heeft een sterke behoefte aan continue doorontwikkeling en innovatie op het SOC/SIEM-platform. Van de dienstverlener wordt verwacht dat hij in staat is in deze behoefte te voorzien op een manier die aansluit bij de behoefte van PNB. Hiervoor brengt de dienstverlener specialistische kennis en ervaring in, leert ze de opdrachtgever snel kennen en stemt ze de doorontwikkeling op regelmatige basis af met de provincie.
Naast de ontwikkeling van de toepassingen op het SOC/SIEM-platform is ook de ontwikkeling van het platform zelf van essentieel belang. PNB wil dat altijd op actuele versies van het SOC/SIEM-platform gewerkt wordt. PNB verwacht van de dienstverlener dat hij dit borgt en dat hij vroegtijdig impact en doorlooptijd van updates en upgrades inbrengt. En dat, onderbouwd, wordt aangegeven wanneer hiervan moet worden afgeweken.
Daarbij streeft PNB naar een stabiele en veilige omgeving die steeds efficiënter en kosteneffectiever uit te voeren en te regisseren is. Belangrijk is te weten hoe opdrachtnemer dit invult. Inzicht in het standaard proces

van opdrachtnemer is essentieel. Hierbij wil PNB dat die aanpak aantoonbaar een positief effect heeft op efficiency en effectiviteit.

2. Use cases

Het PNB IT- en applicatielandschap is continu aan verandering onderhevig. Dit vraagt van de managed SOC-dienstverlener o.a. het ontwikkelen en implementeren van nieuwe use cases voor toekomstige projecten (toekomstige projecten zijn buiten scope van deze aanbesteding). PNB gaat ervan uit dat de SOC-dienstverlener proactief potentiële use cases herkent en die de provincie voorlegt als optioneel te ontwikkelen en implementeren. PNB wil graag inzicht hoe u dit in de praktijk doet en op welke wijze u dit voorlegt aan PNB.
PNB verwacht van SOC-dienstverlener dat hij op verzoek van de provincie specifieke use cases bouwt voor die aangemerkte applicaties waarin bedrijfskritische informatie wordt verwerkt. Daarbij is PNB benieuwd wat uw verwachtingen en eisen zijn t.a.v. de dienstenleveranciers en PNB om invulling te kunnen geven aan een efficiënt werkend use case proces.
De provincie wil graag inzicht in hoe het proces in zijn werk gaat in het creëren van een specifiek use case en welke technologieën hierbij worden gebruikt. Waarbij het relevant is of use cases automatisch of handmatig ontwikkeld worden of beiden.
Concrete use case: Is opdrachtnemer in de doorontwikkeling in staat intelligence feeds te gebruiken om de security posture van het PNB landschap te bewaken v.w.b. vulnerablities, misconfiguraties, etc? En hoe doet u dit in de praktijk?

3. Security community

Ontwikkelingen in de IT gaan erg snel. Ontwikkelingen op het gebied van cyber security zo mogelijk nog sneller. Dit heeft effect op het SOC, de onderliggende security tooling, maar ook op het gebied van kennis en expertise en niet in de laatste plaats hoe in de keten wordt samengewerkt om bedreigen te voorkomen en wanneer ze zich voordoen: met een minimale impact zo snel mogelijk ter herstellen. Dit vraagt van de SOC-dienstverlener dat hij mee gaat in deze ontwikkelingen en waar mogelijk daarin voorop loopt. Naar het idee van PNB kan dit moeilijk worden waargemaakt indien de SOC-dienstverlener zich geïsoleerd van de rest van de security community wil ontwikkelen. De provincie verwacht dan ook van opdrachtnemer dat hij midden in die security community staat. Dat hij deelneemt in relevant overlegstructuren, sterke contacten heeft met relevante overheidsorganisaties, producenten en andere relevante nationale en internationale partijen.
Voor PNB is het belangrijk om te kunnen constateren dat de SOC-dienstverlener zijn kennis en expertise op het onderwerp van de aanbesteding actief onderhoudt en verder uitbouwt. De provincie wil graag weten bij welke overlegorganen, al dan niet geïnitieerd door de overheid, u een actieve rol heeft c.q. een bijdrage levert, hoe dit u helpt in de doorontwikkeling van uw dienstverlening en wat dit concreet voor PNB betekent. Ook wil PNB graag weten hoe u de opgehaalde kennis en expertise inzet bij de provincie zodat het concreet bijdraagt aan een veiliger PNB.

6 Visie op de regie en samenwerking

6.1 Regiemodel

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

1. Efficiënte en doelgerichte regie en service integratie (SIAM)
Als onderdeel van de regievoering vult PNB de service integratie rol in voor de verschillende dienstenketens. Wanneer PNB op termijn voldoende inzicht en ervaring op dit vakgebied heeft opgebouwd, zal ook de SI-rol uitbesteed worden, bijvoorbeeld aan de lead supplier.
De service integrator heeft de end-to-end verantwoordelijkheid voor de dienstverlening aan de PNB-organisatie op het gebied van service- en performance management, rapportage, governance en continual service improvement (CSI). De service integrator geeft hiervoor sturing aan de activiteiten de bij verschillende oplosgroepen worden uitgevoerd, zowel binnen als buiten de PNB-organisatie.

2. PNB richt zich op het WAAROM en WAT, dienstverleners op het HOE
Zoals ook al even aangegeven in het vorige hoofdstuk richt PNB 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 hoofdstuk 3). Daarnaast wordt een optimale architectuur-aansluiting verwacht tussen de functionele oplossing van de dienstverlener en de architectuur zoals gehanteerd door de provincie. 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 de provincie, waar de operationele regie binnen de keten van de kavel, inclusief de koppeling naar de aanpalende kavels, 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.

6.2 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 hier concreet invulling aan geven door toepassing van het Joint Added Value (JAV) model. Uitgangspunt hierbij is dat de PNB de leverancier ‘op de winkel kan laten passen’ zonder dat de kassa geteld moet worden.

6.3 JAV versus partnership

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 te doorlopen fasen passend moeten worden ingevuld. 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.

Fase 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 leveranciers

waarbij tevens wordt gezocht naar een optimale cultural- en strategic fit. Dit is een belangrijke randvoorwaarde voor een goede samenwerking.
Fase 2: partijen leveren een heldere, gedragen en duidelijke set afspraken. Hiermee wil PNB ongecontroleerde escalaties vermijden en perspectief bieden om de vruchten te plukken van gedane investeringen. Heldere (financiële) kaders, dienstbeschrijvingen en service levels zijn opgesteld en er is een duidelijke gedragen rolverdeling. Openheid en transparantie ten opzichte van elkaar is essentieel.
Fase 3: hierin 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.

Het selecteren van de juiste partner is essentieel, waarbij PNB verwacht dat de SOC-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.

6.3.1 Verwachtingen

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

1. Bijdrage aan de samenwerking

PNB verwacht dat de dienstverlener actief bijdraagt aan de samenwerking en het JAV model adopteert. In de samenwerking speelt gedrag een belangrijk rol. PNB is van mening dat door deze samenwerking de diensten aan afnemers van de managed SOC-dienstverlening en de uiteindelijk de PNB-collega's mede succesvol wordt doordat de SOC-dienstverlener:

a. In één keer goed en conform verwachting levert;
b. Samenwerking met partners in het ecosysteem 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 opdrachtnemer 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.

2. Ketenregie

PNB verwacht dat opdrachtnemer zorg draagt voor de operationele regievoering over de security en compliance keten. Hierbij heeft de SOC-dienstverlener een duidelijk beeld van en ervaring met hoe de ketenregie optimaal wordt ingevuld, waarbij het proces stevig geborgd is en waarin hij alle actoren in de keten op een zodanige wijze onboard en meeneemt dat zij exact weten wat te doen zodra de dienstverlener een security incident meldt, maar ze tevens bereid zijn de SOC-dienstverlener tijdig en volledig te informeren over de status van het incident. De rolverdeling en verwachtingen over en weer zijn voor alle betrokken partijen helder en de communicatie- en escalatielijnen duidelijk. De eisen die hij stelt aan de bestaande en nieuwe te onboarden leveranciers zijn duidelijk en gedeeld met de partijen en met PNB.

3. Koppeling ITSM-tool

Voor een optimale samenwerking tussen opdrachtgever en opdrachtnemer 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 kavels heen mogelijk maken. Dit maakt tevens dat PNB eigenaar kan zijn van een up to date CMDB. Het config managementproces is onderdeel van de koppeling. Een continu up to date CMDB vraagt een (near) realtime koppeling gebaseerd op API's.
De SOC-dienstverlener verzorgt de API-koppeling vanuit zijn organisatie en onderhoudt deze koppeling tijdens de contractlooptijd. PNB verzorgd de API-koppeling aan zijn kant.

7 Eisen - knock out -

Dit hoofdstuk benoemt, op basis van de in de vorige hoofdstukken beschreven visie en verwachtingen, de eisen die PNB stelt aan de opdracht.

Taal	
#	**Eis**
TAL-E01	Opdrachtnemer garandeert dat gedurende de uitvoering van de opdracht door alle werknemers en ingezette derden welke zorg dragen voor de uitvoering van de opdracht in de contacten met PNB, de Nederlandse of Engelse taal in woord en geschrift zal worden gebruikt. Tevens verklaart dienstverlener dat bij de uitvoering van de opdracht alle documenten, rapportages in de Nederlandse taal zijn opgesteld.
Documentatie	
#	**Eis**
DOC-E01	De dienstverlening dient in zijn geheel beschreven en voor PNB te allen tijde beschikbaar te zijn (voorbeelden, maar niet limitatief: handleidingen, beschrijvingen, designs).
DOC-E02	PNB is eigenaar van alle beschrijvingen zoals bedoeld in DOC-E01.
Algemeen	
#	**Eis**
ALG-E01	Opdrachtnemer verklaart expliciet dat hij voldoet aan alle in de inschrijvingsleidraad en daarbij behorende bijlage(n) genoemde voorwaarden en eisen die aan de opdracht zijn gesteld.
ALG-E02	Opdrachtnemer conformeert zich aan geldende en toekomstige van toepassing zijnde wet- en regelgeving.
ALG-E03	Opdrachtnemer conformeert zich aan het voor de scope van de opdracht relevante PNB-beleid.
ALG-E04	Opdrachtnemer conformeert zich aan de marktstandaarden en de standaarden voorgeschreven door het Forum voor Standaardisatie.
Informatiebeveiliging	
#	**Eis**
INB-E01	PNB eist dat opdrachtnemer zich conformeert aan de onderstaande richtlijnen en normenkader en wet- en regelgevingen die PNB hanteert voor beveiliging van IT-systemen: 1. De BIO minimaal BBN2 voor de implementatierichtlijnen en maatregelen 2. De NIS2
INB-E02	Opdrachtnemer is ISO27001 gecertificeerd voor de voor de scope van de aangeboden dienstverlening.
INB-E03	Opdrachtnemer ondersteunt alerts komende uit een OT/IoT/ICS-SIEM.
INB-E04	Bij gunning volgt een BIO-audit door een door PNB aangewezen auditor waaraan opdrachtnemer medewerking verleent.
INB-E05	Alle communicatie binnen de aangeboden dienstverlening vindt plaats over versleutelde verbindingen.
INB-E06	De data is versleuteld opgeslagen. Data is tijdens transport versleuteld.
INB-E07	Authenticatie moet voldoen aan Entra ID.
INB-E08	Op elke inlogmogelijkheid is Multi Factor Authentication (MFA) van toepassing.
INB-E09	PNB krijgt de beschikking over alle nieuwe functionaliteit die de SOC-dienstverlener biedt.
INB-E10	Opdrachtnemer laat als onderdeel van de dienstverlening jaarlijks een pentest uitvoeren op de kritische onderdelen binnen de dienst door een onafhankelijke partij. Bevindingen worden proactief en risico gedreven geprioriteerd en opgelost.
Privacy	
#	**Eis**
PRI-E01	Bij een eventuele gunning van de opdracht conformeert opdrachtnemer zich aan en gaat akkoord met de PNB verwerkersovereenkomst. Na gunning maken dienstverlener en aanbestedende dienst deze gezamenlijk af en deze wordt door beide partijen ondertekend.
PRI-E02	Opdrachtnemer handelt conform de Algemene Verordening Gegevensbescherming (AVG). Alle gegevens door provincie Noord-Brabant aan opdrachtnemer ter beschikking gesteld of door de onder de overeenkomst verrichte werkzaamheden aan opdrachtnemer bekend geworden, zullen anders dan op een door de Nederlandse Wet en regelgeving toegelaten wijze, niet aan derden worden verstrekt.
PRI-E03	Persoonsgegevens dienen standaard afgeschermd te zijn en mogen niet standaard openbaar zichtbaar zijn.
PRI-E04	Incidenten met betrekking tot privacy worden geregistreerd en periodiek gerapporteerd aan de PNB. Afhankelijk van de grootte, aard en de impact van het incident wordt er een escalatie pad gevolgd waarin PNB tijdig en zo volledig als nodig wordt betrokken.

PRI-E05	Data dient binnen de EER te worden bewerkt en opgeslagen.
SOC-dienstverlening	
#	**Eis**
DIV-E01	De dienstverlening bestaat minimaal uit de beheeronderdelen zoals beschreven in hoofdstuk 2.2 en hoofdstuk 5 van dit document.
DIV-E02	De inrichting en levering van de dienst is conform de maatregelen die van toepassingen zijn zoals deze zijn gesteld in de Baseline Informatiebeveiliging Overheid afgekort BIO.
DIV-E03	De provincie Noord-Brabant is ten allen tijden gerechtigd om een audit te laten uitvoeren door een externe auditor over de geleverde dienst. Bevindingen komende uit de audit worden door opdrachtnemer opgelost op zijn kosten.
DIV-E04	De toegekende toegangsrechten van alle voor of bij PNB in te zetten medewerkers en derden namens opdrachtnemer, worden bij de beëindiging van hun dienstverband, contract of overeenkomst direct verwijderd. Bij wijziging van de functie of rol worden de toegangsrechten direct aangepast.
DIV-E05	Voordat een account definitief wordt verwijderd dient dit te worden voorgelegd aan de PNB. Daarbij dient de leverancier een check te doen op de bevoegdheden van het te verwijderen account. Mocht blijken dat door het verwijderen van het betreffende account er 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.
DIV-E06	Opdrachtnemer heeft aantoonbare kennis, expertise en uitgebreide praktische en actuele ervaring met Darktrace, Sentinel en Nessus.
DIV-E07	Opdrachtnemer levert zijn dienst overeenkomstig de overeengekomen SLA.
DIV-E08	Opdrachtnemer borgt dat er voldoende personele bezetting is om reguliere werkzaamheden binnen de afgesproken termijnen op te kunnen leveren.
DIV-E09	Optimalisatie van excessief veel resource gebruikende use case implementaties is onderdeel van de dienstverlening en geborgd in het reguliere proces.
DIV-E10	Opdrachtnemer borgt dat er voldoende personele bezetting is om tijdens incidenten de afgesproken ondersteuning te kunnen leveren.
DIV-E11	De managed SOC-dienstverlening is 7/24 uur.
DIV-E12	Directe ondersteuning 24/7 bij een groot incident.
DIV-E13	De dienst biedt de mogelijkheid om ransomware verdediging op de endpoints aan te zetten in preventie modus, zodat dienst wordt geblokkeerd, indien ransomware wordt gedetecteerd.
DIV-E14	De dienst dient bij herkenning van een aaneengesloten reeks van malafide handelingen, op endpoint-/serverniveau, de uitvoerende dienst automatisch te blokkeren.
DIV-E15	Agents dienen (op de endpoints) detectie en automatische respons uit te kunnen voeren, zonder dat hier menselijke interactie voor vereist is.
DIV-E16	De dienst biedt de mogelijkheid om alerts af te geven aan de hand van 'out-of-the-box' en zelf gemaakte use-cases.
DIV-E17	De dienst biedt de mogelijkheid om vanuit de frontend machines te isoleren van het netwerk in het geval van een kritisch beveiligingsincident.
DIV-E18	De dienst dient gekoppeld te kunnen worden aan externe Threat Intelligence Providers, ten behoeve van de verzameling van open source Threat Intelligence.
DIV-E19	Via Machine Learning jobs moet het mogelijk zijn om anomalieën in de logging te detecteren.
DIV-E20	Opdrachtnemer levert op eerste verzoek van PNB de benodigde data ten behoeve van forensische onderzoeken in geval van incidenten.
DIV-E21	De geboden dienst moet verdeeld over meerdere fysieke locaties kunnen functioneren.
DIV-E22	De dienst/opdrachtnemer bewaart logs en alerts minimaal 1 jaar.
DIV-E23	De dienst is uitbreidbaar met nieuwe intelligence feeds.
DIV-E24	Opdrachtnemer communiceert rechtstreeks met diverse SaaS, PaaS en IaaS dienstverleners van PNB om snel en efficiënt incidenten af te laten handelen. PNB wordt hierbij continu geïnformeerd over de voortgang.
DIV-E25	De selectie van de use cases in de SIEM worden geprioriteerd op basis van een risicoanalyse en intelligence feeds omtrent relevante dreigingsactoren.
DIV-E26	Opdrachtnemer werkt op basis van een door PNB goedgekeurde autorisatiematrix.
DIV-E27	Opdrachtnemer voert, op basis van een goedgekeurde autorisatie matrix, een periodieke controle uit op de ingerichte autorisaties inclusief rapportages en opvolging van non compliances.
DIV-E28	De geboden dienst moet in Azure Sentinel als 1ste lijns managed service ondersteunen.
DIV-E29	De omgeving gebruikt voor de dienstverlening door de opdrachtnemer is gehardend conform minimaal best practices van de producent/fabrikant en opdrachtnemer borgt dat die hardend blijft.
DIV-E30	De door opdrachtnemer gebruikte omgeving voor de dienstverlening dient periodiek gecontroleerd te worden op compliance met hardening guidelines.

DIV-E31	Opdrachtnemer levert structureel en periodiek rapportages met betrekking tot lopende en afgehandelde incidenten met als minimale parameters tijdsduur, lopend en afhandelingstermijnen en binnen SLA of niet in percentages.
DIV-E32	Opdrachtnemer heeft een vastgesteld continuïteitsplan waarin is opgenomen hoe, in geval van calamiteiten, de getroffen ICT-dienst of het getroffen informatiesysteem weer zo snel mogelijk operationeel wordt. Dit plan wordt regelmatig beoordeeld en getest.
DIV-E33	Nieuwe componenten die worden aangesloten als log source worden automatisch met de voor die categorie bepaalde use cases gemonitord.
DIV-E34	Opdrachtnemer zorgt voor een, naar het oordeel van PNB, duidelijk beschreven aansluitproces c.q. -eisen voor externe leveranciers.
Samenwerking	
#	**Eis**
SIS-E01	De samenwerking geeft minimaal invulling aan de verwachtingen zoals beschreven in van dit document.
SIS-E02	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)
SIS-E03	Opdrachtnemer biedt ten behoeve van IT-meldingen en -vragen een deskundige servicedesk aan, dat wil zeggen 'een tweedelijnsondersteuning', die als aanspreekpunt rechtstreeks in contact staat met Ons Loket van de PNB.
SIS-E04	Afspraken m.b.t. samenwerking zijn minimaal vastgelegd in het DAP. Wijzigingen in het DAP worden onderling afgestemd en akkoord bevonden.
SIS-E05	In geval van calamiteiten of crisis is de directie van opdrachtnemer rechtstreeks toegankelijk voor het management van PNB.
SIS-E06	Opdrachtnemer daagt PNB meerdere malen per jaar uit na te denken over innovatieve functionaliteit bij de SOC-dienstverlening. Hierbij draagt dienstverlener concrete voorstellen aan die bijdragen aan het bereiken van de doelen en ambitie van PNB en waarvan het resultaat leidt tot een duidelijke meerwaarde voor beide organisaties.
Exit / Retransitie	
#	**Eis**
EXI-E01	Om het gemeenschappelijk belang en de verantwoordelijkheden te benadrukken en het streven naar een effectieve samenwerking tussen de provincie, verkrijgende leverancier en de latende leverancier te bekrachtigen, verklaren de provincie en opdrachtnemer de Gedragscode Retransitie van 15 mei 2014 versie 1.2 van Sourcing Nederland van toepassing.
EXI-E02	De dienstverlener stelt uiterlijk binnen 6 maanden na gunning een uitgewerkt retransitieplan op. Het retransitieplan behoeft goedkeuring van PNB.
EXI-E03	Het voorgestelde retransitieplan gaat minimaal in op de voorwaarden en uitgangspunten, overdracht van kennis, middelen, planning, transitie organisatie en resources, afvoeren van vertrouwelijke informatie, informatiebeveiliging, financiële aspecten, juridische aspecten, verantwoordelijkheden en bevoegdheden, escalaties en klachten, vernietiging van informatie, afspraken m.b.t. IP (Intellectual property), de actieve medewerking van dienstverlener aan de exit.
EXI-E04	Opdrachtnemer past tenminste eenmaal per jaar, of zo veel vaker als PNB daar in redelijkheid om verzoekt, het retransitieplan aan op de dan bestaande situatie.
EXI-E05	Opdrachtnemer 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.
EXI-E06	Opdrachtnemer 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 zoveel mogelijk tussen de partijen vrij overdraagbaar is en gebruikt mag worden.
Inkoop en contract	
#	**Eis**
INK-E01	ARBIT-2022 voorwaarden zijn van toepassing met uitzondering van de gehele “Bijzondere bepalingen koop” en voor wat betreft “Bijzondere bepalingen opdrachten” de artikelen 57, 58, 59 en 60, 80, 81.
INK-E02	PNB betaalt slechts voor actieve en daadwerkelijke geleverde en door PNB geaccepteerde diensten.
INK-E03	PNB kan marktconformiteit van prijzen en tarieven extern laten toetsen en vaststellen door middel van een benchmark.

Prijzen en tarieven	
#	**Eis**
PRT-E01	De door de inschrijver aangeboden prijzen en tarieven zijn in Euro (€), all-in, inclusief overige belastingen en/of heffingen, en exclusief BTW.
PRT-E02	Eventuele valutawijzigingen zijn voor rekening van de inschrijver.
Architectuur	
#	**Eis**
ARC-E01	Opdrachtnemer sluit haar dienstverlening aan de op architectuur van PNB en voldoet aan de door PNB gestelde aansluitvoorwaarden en architectuurprincipes.