NEO NL
Nucleaire Energie Organisatie Nederland

HUIDIGE EN TOEKOMSTIGE SITUATIE NEO NL

Inhoud

1 Inleiding 2

2 Huidige situatie 3

2.1 Colocatiediensten 3
2.2 WAN- en LAN-diensten 3
2.3 HSM en PKI-diensten 3
2.4 SOC- en SIEM-diensten 3
2.5 Geïntegreerde IT-diensten en beheer 3
2.6 Mobiele connectiviteitsdiensten 5

3 Gewenste situatie 6

3.1 Perceel 1: Beheerde colocatiediensten 7
3.2 Perceel 2: Beheerde WAN- en LAN-diensten 8
3.3 Perceel 3: Beheerde HSM en PKI-diensten 8
3.4 Perceel 4: beheerde SOC- en SIEM-diensten 8
3.5 Perceel 5: Geïntegreerde IT-diensten en beheer 9
3.6 Perceel 6: Beheerde mobiele connectiviteitsdiensten 10

4 Migratie 11

4.1 Ontwerpfase 11
4.2 Opbouwfase 11
4.3 Migratiefase 11
4.4 Operationele fase 12

1 Inleiding

Dit document beschrijft de huidige situatie en de gewenste toekomstige situatie van werkplekomgeving voor NEO NL en de voor nu bekende diensten bij DICTU en andere leveranciers. Om te komen tot de toekomstige situatie verstrekken we een opdracht voor een volledige nieuwe opbouw van een IT-landschap voor NEO NL (Digital Foundation) door zes verschillende leveranciers voor de volgende percelen:

Perceel 1: Beheerde colocatiediensten

Perceel 2: Beheerde WAN- en LAN-diensten

Perceel 3: Beheerde HSM en PKI-diensten

Perceel 4: Beheerde SOC- en SIEM-diensten

Perceel 5: Geïntegreerde IT-diensten en beheer

Perceel 6: Beheerde mobiele connectiviteitsdiensten

Naast het opnieuw opbouwen van de gehele benodigde infrastructuur moeten de leveranciers ook de migratie van gebruikers, configuraties en data verzorgen. Hierbij moeten onder andere Microsoft Windows, Microsoft 365, Microsoft Teams en Microsoft SharePoint data worden gemigreerd zonder verlies van services of bedrijfsdata.

De leveranciers zijn gezamenlijk verantwoordelijk voor het ontwerpen, realiseren, testen, migreren en in beheer nemen van de nieuwe omgeving. NEO NL stelt eisen aan de architectuur, digitale autonomie, beveiliging en monitoring.

De nieuwe leveranciers leveren gezamenlijk de diensten en begeleiden daarbij de uitrol van nieuwe NEO NL IT-diensten. Er wordt geen bestaande infrastructuur overgenomen. Alle componenten dienen volledig nieuw en volgens de actuele best practices, de securityrichtlijnen van NEO NL en moderne beheerprincipes te worden ingericht.

2 Huidige situatie

2.1 Colocatiediensten

NEO NL heeft momenteel geen eigen datacenter of faciliteiten voor infrastructuur. Het (gehuurde) pand is hiervoor niet geschikt. De huidige dienstverlener (DICTU) heeft eigen (co)locaties voor housing om de dienst (werkplek, storage, AI-rekenkracht en dergelijke) te kunnen leveren.

2.2 WAN- en LAN-diensten

NEO NL heeft een beheerd zakelijk internetabonnement dat als dienst door KPN wordt geleverd op basis van glasvezel. Deze verbinding komt binnen in een gezamenlijke Mechanical Engine Room (MER) in de kelder van het pand. NEO NL huurt de gehele eerste verdieping in een kantoorpand van in totaal vier verdiepingen. De geleverde bandbreedte is 2Gbps. Voor de huidige 150 medewerkers is dit voldoende. Het signaal wordt via glasvezel in het pand doorgezet op basis van single mode naar de eerste verdieping waar een Power Over Ethernet (POE) switch hangt in een 19 inch rack naast een Firewall. Al het inkomende verkeer wordt geblokkeerd, al het uitgaande verkeer wordt toegelaten. Draadloos netwerk wordt afgenomen als dienst bij een externe leverancier waardoor het mogelijk is om te werken op de door DICTU geleverde en beheerde werkplekken. De verdieping is voorzien van in totaal 19 access points voor draadloos netwerk en Avaya punchblocks voor bedraad netwerk.

2.3 HSM en PKI-diensten

NEO NL heeft geen eigen HSM of PKI-diensten. Via het ministerie van Economische Zaken levert DICTU de huidige werkplekdiensten inclusief beheerde beveiligingsdiensten.

2.4 SOC- en SIEM-diensten

NEO NL neemt geen beheerde SOC- en SIEM-diensten af.

2.5 Geïntegreerde IT-diensten en beheer

Via het ministerie van Economische Zaken levert DICTU de huidige werkplekdiensten aan NEO NL. Dit betreft Service Desk (eerstelijns), tweede- en derdelijns beheerdiensten, CMDB, change en problem management. DICTU gebruikt hiervoor eigen ITSM-tooling. Er zijn onderlinge afspraken gemaakt tussen DICTU, het ministerie van Economische Zaken en NEO NL over de processen, rapportages en SLA’s.

De werkplek is een Microsoft-gebaseerde werkplek of Macbook waarbij gebruikers centraal authenticeren en gebruikmaken van een Citrix werkplek (cloudwerkplek). Microsoft 365 vormt het primaire platform voor communicatie, samenwerking en documentopslag.

De werkplekken bestaan uit laptops en kunnen op kantoor met USB-C worden aangesloten op de aanwezige 27 inch-monitoren op de werkplek en vergaderfaciliteiten in de vergaderruimten (BYOM, Bring Your Own Meeting). Omdat er geen bedraad netwerk aanwezig is wordt alleen gebruikgemaakt van het draadloze netwerk. De Windows laptops zijn voorzien van een Vodafone SIM kaart om verbinding met het internet te kunnen maken als er geen netwerk beschikbaar is. De volgende software is standaard op elke werkplek aanwezig:

- Microsoft Windows 11 of MacOS
- Microsoft 365 versie 2606 build 20131.20150 klik-en-klaar:
  - Microsoft Office (Word, Excel, PowerPoint en Outlook),
  - Microsoft Teams voor collaboration (chat, vergaderen, samenwerken e.d.)
  - Microsoft OneDrive
  - Microsoft Edge
  - SharePoint als centraal document managementsysteem
- Adobe Acrobat Reader gratis versie

Naast de standaardset aan applicaties is het mogelijk om extra applicaties aan te vragen. De volgende applicaties worden binnen NEO NL buiten de standaardset gebruikt:

- Microsoft Visio
- Microsoft Project
- Adobe Acrobat pro
- Adobe Illustrator
- DWG TrueView

Inmiddels gebruikt NEO NL al diverse op cloud gebaseerde applicaties buiten de dienstverlening van DICTU om. Het gaat in ieder geval om de volgende applicaties die bekend zijn:

- Relatics, een cloudgebaseerde applicatie voor RMS (Requirement Management System)
- ODOO, een cloudgebaseerde applicatie voor de financiële huishouding – wordt tijdelijk gebruikt en uitgefaseerd in 2027
- ValidSign, een cloudgebaseerde applicatie voor digitaal ondertekenen
- Aryo, een cloudgebaseerd documentmanagementsysteem – wordt tijdelijk gebruikt en in 2027 uitgefaseerd
- Exact (hosted)
- Omega365 (DMS) vervangt Aryo in 2027
- BizzDesign (SaaS)

We verwachten dat in 2026-2027 tien tot vijftien applicaties moeten worden geëvalueerd en mogelijk opgenomen in de nieuwe NEO NL infrastructuur en servicemanagement, zoals: SRM, Bestuursinformatiesysteem, BPM, Bizzdesign, Emply, HR onboarding tool, IMS (Mavim), AI-tooling, Common Data Foundation.

De tot nu opgebouwde data van NEO NL bestaat uit documenten die worden opgeslagen in SharePoint Online. Verder wordt Teams voor collaboration intensief gebruikt (chat, vergaderen, samenwerken, Team sites) en wordt er veel gemaild binnen de omgeving met persoonlijke (150 stuks) en functionele (30 stuks) Exchange Online mailboxen.

NEO NL heeft diverse eigen domeinnamen in beheer, of in beheer bij het ministerie van Algemene Zaken. Het e-mailadres is voor de meeste werknemers nog steeds @minezk.nl, maar er zijn uitzonderingen aangemaakt voor het mailadres @neonl.com.

Naast de werkplek heeft elke medewerker een telefoon (Apple IPhone 13 SE) voor tweefactor-authenticatie met behulp van de Microsoft Authenticator, en zijn diverse applicaties beschikbaar op de telefoon, zoals Outlook, Word en Excel.

DICTU levert ook twee beheerde multifunctionele printers die middels VPN over 4G/5G zijn ontsloten met het overheidsnetwerk. Met de rijkspas van de overheid is het mogelijk te printen (pull printing), scannen en kopiëren. Papier en toner schaft NEO NL zelf aan.

2.6 Mobiele connectiviteitsdiensten

De mobiele diensten die nu worden gebruikt vallen onder de standaarddiensten zoals die worden geleverd door DICTU. Dit betreft telefonie-abonnementen met data en het beheer ervan. Er is een vast 088-nummer beschikbaar dat wordt doorgezet naar drie mobiele telefoons die zich kunnen aanmelden en afmelden. Als na werktijd of in de weekenden wordt gebeld naar het vaste nummer hoort de beller een boodschap met een algemeen bericht.

3 Gewenste situatie

NEO NL heeft vier strategische ICT-pijlers gedefinieerd die richting geven aan de gewenste toekomstige inrichting van de ICT-omgeving en dienstverlening:

1. **Identity First-benadering (eIAM als enabler)**
   Deze pijler valt buiten de scope van deze aanbesteding, maar de beoogde werkplek gaat er wel gebruik van maken.
2. **Security by Design binnen de nucleaire context**
   Informatiebeveiliging wordt vanaf het ontwerp integraal meegenomen in de inrichting en dienstverlening. Daarbij wordt rekening gehouden met de specifieke beveiligings-, continuïteits- en compliance-eisen die voortvloeien uit de nucleaire context waarin NEO NL opereert.
3. **Een gestandaardiseerde digitale werkplek**
   NEO NL kiest voor een zoveel mogelijk uniforme digitale werkplek. De functionele en technische inrichting wordt afgestemd op verschillende gebruikssituaties en risicoprofielen, waarbij de oplossing technologieneutraal wordt vormgegeven. Standaardisatie draagt bij aan het verkleinen van het aanvalsoppervlak en vereenvoudigt het patch-, beheer- en lifecyclemanagement. Hierdoor kunnen zowel de total cost of ownership (TCO) als de belasting van de servicedesk worden beperkt. Voor medewerkers moet dit resulteren in een consistente, veilige, betrouwbare en goed presterende gebruikerservaring. Tegelijkertijd wil NEO NL afhankelijkheid van specifieke leveranciers en technologieën zoveel mogelijk voorkomen. De architectuur moet daarom zodanig worden ingericht dat een toekomstige overstap naar een andere werkplekoplossing zowel operationeel als contractueel uitvoerbaar blijft. Het gebruik van open standaarden, de overdraagbaarheid van data en configuraties en, waar passend, open source-oplossingen dragen bij aan de strategische autonomie die past bij NEO NL als vitale maatschappelijke organisatie.
4. **Governance**
   Een heldere governance moet zorgen voor adequate sturing, beheersing en besluitvorming rondom de ICT-dienstverlening. Daarbij zijn duidelijke verantwoordelijkheden, transparantie, aantoonbare beheersing en inzicht in prestaties, risico's en afhankelijkheden van belang.

Met deze aanbesteding van een nieuwe werkplekomgeving zoekt NEO NL minimaal behoud van de huidige functionele mogelijkheden, maar tegelijkertijd een duidelijke versterking van haar **IT Foundation**. De beoogde verbetering ten opzichte van de huidige dienstverlening ligt met name op het gebied van **weerbaarheid, wendbaarheid en beheersing.**

De toekomstige dienstverlening moet NEO NL in staat stellen om veranderingen sneller en gecontroleerd door te voeren, risico's beter te beheersen en de IT-omgeving duurzaam te laten meebewegen met veranderende organisatorische, technologische en maatschappelijke eisen.

De toekomstige dienstverlening dient de eventuele integratie met OT-omgevingen te kunnen faciliteren. Dit stelt ons in staat om OT-data te verwerken in systemen zoals SOC-SIEM en deze gegevens te benutten voor rapportages. Deze koppeling zien we dan graag terug in de vorm van een datadiode passend in een netwerkbeveiligingsmodel gebaseerd op de IAEA NSS 17T.

Daarnaast verwacht NEO NL van elke leverancier dat hij volledige medewerking verleent aan de SOC- en SIEM-dienstverlening, waaronder het toestaan, en waar nodig het installeren en beheren van benodigde agents op de door hem beheerde systemen.

Van de leveranciers wordt verwacht dat zij hun diensten optimaal afstemmen op de dienstverlening van de andere leveranciers. De inrichting ervan en de migratie dient te gebeuren in overeenstemming met NEO NL en de huidige dienstverlener én in samenspraak met de overige leveranciers. De betreffende assets dienen fysiek overdraagbaar te zijn en op verzoek volledig aan NEO NL te kunnen worden overgedragen.

We vinden dat goede IT niet alleen ontstaat door technologie alleen. Goede IT ontstaat wanneer klant en leverancier hun kennis, verantwoordelijkheid en mogelijkheden samenbrengen om een veilige, betrouwbare en toekomst vaste digitale omgeving te creëren. In het door ons opgestelde *Manifest samenwerking* (bijgevoegd als bijlage) beschrijven we hoe wij willen samenwerken. We hebben dit uitgewerkt in acht waarden:

1. Gezamenlijk resultaat boven eigen belang
2. Vertrouwen door transparantie
3. Waarde boven technologie
4. Veiligheid en continuïteit als fundament
5. Eenvoud en standaardisatie waar het kan
6. Professioneel tegenspel boven volgzaamheid
7. Continu verbeteren boven stilstand
8. Vrijheid en toekomstvastheid boven afhankelijkheid

We zien onze leveranciers daarom niet alleen als uitvoerders van een opdracht, maar als professionele partners met eigen expertise en verantwoordelijkheid. Wij zien onszelf evenmin alleen als opdrachtgever. Wij zijn medeverantwoordelijk voor het creëren van de voorwaarden waarin goede IT kan ontstaan.

De gewenste situatie resulteert in een toekomstbestendige, weerbare (beveiliging), wendbare en beheersbare (modulaire en verticaal en horizontale dienstenflexibiliteit) digitale foundation met minimaal gelijkblijvende functionaliteit ten opzichte van de huidige situatie, maar met een significant hoger kwaliteitsniveau.

3.1 Perceel 1: Beheerde colocatiediensten

In de eindsituatie beschikt NEO NL over een hoogwaardige, redundante en toekomstbestendige colocatie-omgeving verdeeld over twee geografisch gescheiden datacenterlocaties. Deze omgeving vormt de fysieke basis voor de IT-dienstverlening van NEO NL en voldoet aan TIER-3, EN 50600 of aantoonbaar vergelijkbare eisen.

Per locatie beschikt NEO NL over een afgeschermde private cage met voldoende rackcapaciteit en uitbreidingsmogelijkheden gedurende de looptijd van de overeenkomst. Daarnaast is voldoende capaciteit beschikbaar op het gebied van stroom en koeling om toekomstige groei, waaronder de inzet van dedicated AI-hardware, te ondersteunen.

Binnen iedere locatie is daarnaast een separaat afsluitbaar rack beschikbaar waarvan NEO NL zelf het toegangsbeheer doet. De omgeving is 24x7 operationeel ondersteund en biedt faciliteiten voor storingsafhandeling en remote hands.

De datacenterlocaties bieden connectiviteit met meerdere onafhankelijke carriers via beheerde cross-connects, zodat redundante en flexibele netwerkverbindingen mogelijk zijn.

3.2 Perceel 2: Beheerde WAN- en LAN-diensten

Bij oplevering is een zero trust-netwerkarchitectuur met network access control (NAC) ingedeeld in meerdere securityzones beschikbaar. De kantooromgeving voor LAN en Wifi-7 infrastructuur is in beheer en ingeregeld met zonering en policy's. Ook zijn de kantoren van NEO NL redundant via WAN ontsloten en later uit te breiden met de toekomstige bouwlocaties van de kerncentrales op basis van versleutelde verbindingen en een redundante internetaansluiting met L7 firewall-voorzieningen.

Daarbij is DHCP/IPAM geïntegreerd met de securityzones en wordt gebruikgemaakt van de PKI-infrastructuur uit perceel 3.

3.3 Perceel 3: Beheerde HSM en PKI-diensten

In de gewenste situatie beschikt NEO NL over een hoog beschikbare, veilige en toekomstvaste cryptografische infrastructuur binnen de eigen datacenters. Deze infrastructuur vormt de centrale basis voor cryptografische diensten binnen NEO NL en ondersteunt de gewenste digitale weerbaarheid en autonomie.

De omgeving bestaat uit een public key infrastructure (PKI) met een root certificate authority, ondersteund door redundant uitgevoerde en gecertificeerde hardware security modules (HSM's). De infrastructuur is geïntegreerd met het IT-netwerk en de beveiligingsvoorzieningen van NEO NL en biedt een gecontroleerde omgeving voor het genereren, opslaan, gebruiken en beheren van cryptografische sleutels en certificaten.

De oplossing is zodanig ingericht dat continuïteit, beschikbaarheid en veiligheid zijn geborgd en dat technologische ontwikkelingen, waaronder post-quantum cryptography, in de toekomst kunnen worden ondersteund. De gebruikte componenten worden gedurende hun volledige levenscyclus beheerd en voldoen aan de daarvoor geldende beveiligings- en certificeringseisen.

3.4 Perceel 4: beheerde SOC- en SIEM-diensten

NEO NL beschikt over een geïntegreerde en continu bewaakte securitymonitoringomgeving die 24x7 inzicht geeft in dreigingen, afwijkingen en security-incidenten. Deze omgeving vormt een essentieel onderdeel van de security posture en digitale weerbaarheid van NEO NL.

De omgeving bestaat uit een beheerd Security Operations Center (SOC) met SIEM-functionaliteit, ingericht volgens de relevante richtlijnen uit IAEA Nuclear Security Series No. 17.

Logbronnen uit de verschillende securityzones en andere percelen zijn centraal aangesloten via beheerde log ingestion pipelines en connectors. Binnen alle relevante securityzones zijn detectiesensoren aanwezig die zijn geïntegreerd met het SIEM-platform. Detectieregels, correlaties, dashboards en alarmen zijn zodanig ingericht dat dreigingen tijdig kunnen worden herkend en opgevolgd.

NEO NL beschikt daarnaast over structurele incident response- en digitale forensics-capaciteit, waarmee securityincidenten binnen afgesproken responsetijden kunnen worden onderzocht, beheerst en afgehandeld. Monitoring, incidentafhandeling en auditing zijn aantoonbaar ingericht en sluiten aan op de geldende beveiligings- en compliance-eisen.

Aanvullend is een doorlopend security awareness- en simulated-phishingprogramma ingericht, gericht op het verhogen en aantoonbaar ontwikkelen van het beveiligingsbewustzijn en de weerbaarheid van medewerkers.

3.5 Perceel 5: Geïntegreerde IT-diensten en beheer

NEO NL zoekt naar een werkplekomgeving waarvan de verwachting is dat de werkplekomgeving volledig parallel naast de huidige werkplek omgeving zal moeten worden opgebouwd om service dips te voorkomen en continuïteit wordt geborgd (de winkel blijft open). De huidige data inclusief rechten en gebruikers moeten eveneens worden gemigreerd.

We voorzien dat er een nieuw werkplekomgeving wordt ingericht die wordt gekoppeld aan onze eigen eIAM omgeving (hiervoor loopt een apart traject dat eerder wordt opgeleverd). De tenant is minimaal voorzien van de volgende functionaliteiten: mail, collaboration inclusief videovergaderingen, chat, content en filemanagement, kantoorapplicaties, printing, werkplekbeheer en policy enforcement applicaties ingericht, conditional access met multifactorauthenticatie en antivirus mogelijkheid.

De werkplekken zijn voorzien van een modern en marktconform operating systeem, dat automatisch kan worden uitgerold en centraal beheerd. Daarnaast wordt een mobiele telefoon geleverd met een modern en marktconform operating systeem dat ook centraal wordt beheerd. Softwaredistributie voor de werkplek en telefoon wordt gedaan door middel van door de leverancier gemaakte packages waarbij de werkplek wordt gehardened in overleg met NEO NL. Updates en patching van onder andere packages, software en operating system worden automatisch uitgevoerd en het compliancebeleid van NEO NL wordt gehandhaafd. Upgrades van software worden in overleg uitgevoerd.

Het pand van NEO NL wordt door de leverancier voorzien van tenminste twee beheerde en aangestuurde multifunctionele printers en een beheerde en aangestuurde al aanwezige A0-plotter (HP T1600 PSdr)) op basis van pull printing.

De leverancier voert een volledige migratie uit van de bestaande werkplekomgeving zoals gebruikersaccounts, groepen, rechten, (functionele) mailboxen, SharePoint-data en Teamskanalen met instellingen. De migratie zelf dient plaats te vinden met minimale verstoring en gebruikers moeten zonder dataverlies kunnen doorwerken.

(Enterprise) Servicemanagement en SIAM
De leverancier van perceel 5 levert naast de werkplek- en infrastructuurdiensten het geïntegreerde servicemanagement voor NEO NL en vervult de rol van ‘lead supplier as service-integrator’ voor de verschillende IT-leveranciers. Deze rol start tijdens de implementatie en omvat de inrichting en coördinatie van de servicemanagementprocessen en de samenwerking tussen de leveranciers.

De leverancier levert hiervoor onder andere:

- een skilled servicedesk en onsite ondersteuning;
- ITIL-gebaseerde servicemanagementprocessen, waaronder maar niet uitsluitend: incident-, request-, problem-, change-, configuration- en knowledge management;
- technisch (applicatie) beheer van de binnen perceel 5 geleverde werkplek-, platform- en infrastructuursoftware;
- onboarding en integratie van nieuwe IT-diensten en leveranciers;
- ketenbrede coördinatie, rapportage en continue verbetering van de dienstverlening.

Voor de ondersteuning hiervan richt de leverancier centrale ITSM-tooling in die on-premise in een datacenter van NEO NL wordt geïnstalleerd. De tooling wordt gebruikt voor de dienstverlening van NEO NL en de samenwerking met de verschillende IT-leveranciers en wordt zodanig ingericht dat deze overdraagbaar is aan NEO NL.

De servicemanagementomgeving wordt schaalbaar en uitbreidbaar ingericht. Op termijn moet het mogelijk zijn deze ook breder binnen NEO NL toe te passen volgens de principes van Enterprise Service Management, bijvoorbeeld voor HR, Finance en Facility Management. Dit maakt geen onderdeel uit van de initiële implementatie, maar de gekozen oplossing mag deze toekomstige ontwikkeling niet belemmeren.

3.6 Perceel 6: Beheerde mobiele connectiviteitsdiensten

NEO NL beschikt in de eindsituatie over een veilige, schaalbare en centraal beheerde oplossing voor mobiele telefonie en datacommunicatie voor haar medewerkers. De voorziening is ingericht om mee te groeien met de organisatie en sluit aan op de overige beveiligings- en mobiele voorzieningen van NEO NL.

De mobiele connectiviteit is gebaseerd op e-SIM-technologie en maakt gebruik van een private APN en een Zero Trust-architectuur. De voorziening is geïntegreerd met de PKI-infrastructuur en de mobiele device-diensten, waardoor veilige toegang, authenticatie en gegevensuitwisseling vanuit mobiele apparaten mogelijk is.

De beschikbaarheid, het gebruik en de beveiliging van de mobiele dienstverlening worden continu gemonitord. Relevante logging en security-informatie zijn beschikbaar voor het SOC en SIEM, zodat ook mobiele communicatie onderdeel is van de centrale securitymonitoring van NEO NL.

Abonnementen, e-SIMs en mobiele nummers worden centraal beheerd gedurende de volledige levenscyclus. NEO NL beschikt daarbij over inzicht in beschikbaarheid, verbruik, beveiliging en kwaliteit van de dienstverlening.

4 Migratie

Na selectie van de leveranciers start de transitie naar de nieuwe ICT-omgeving. Deze transitie wordt uitgevoerd volgens een gefaseerde aanpak bestaande uit vier fasen: ontwerp, opbouw, migratie en operationele fase.

4.1 Ontwerpfase

In de ontwerpfase richten de geselecteerde leveranciers gezamenlijk de nieuwe technische infrastructuur en beheeromgeving in. Iedere leverancier is verantwoordelijk voor de realisatie van zijn eigen perceel, maar werkt hierbij aantoonbaar samen met de andere leveranciers om afhankelijkheden, koppelingen en integraties correct te realiseren. Denk hierbij aan netwerkconnectiviteit richting het datacenter, beveiligingsintegraties tussen SOC/SIEM en HSM/PKI, of authenticatie- en werkplekkoppelingen.

Gedurende deze fase worden gezamenlijke architectuursessies, technische afstemming overleggen en ketentesten georganiseerd. Van leveranciers verwachten we dat zij actief deelnemen aan deze overleggen en gezamenlijk verantwoordelijkheid nemen voor een stabiele, veilige en toekomstbestendige inrichting van het totale IT-landschap. De organisatie voert hierin regie en bewaakt samenhang, planning en kwaliteit.

4.2 Opbouwfase

Na de ontwerpfase begint de opbouwfase. In deze fase wordt de nieuwe omgeving opgebouwd en ingericht voor productiegebruik en beheer. Werkplekken en benodigde infrastructuur worden volgens ontwerp opgebouwd, waarna monitoring, beheerprocessen, autorisaties, logging, beveiligingsmaatregelen en operationele procedures worden geactiveerd en getest. Ook wordt de beheerorganisatie ingericht en worden afspraken over samenwerking, escalatie en dienstverlening operationeel gemaakt.

De leveranciers werken in deze fase nauw samen om te waarborgen dat de gehele keten volgens planning wordt opgeleverd.

4.3 Migratiefase

Na inrichting van de nieuwe omgeving vindt de migratie plaats. In deze periode worden huidige diensten, data, configuraties en beheerprocessen gecontroleerd overgedragen naar de nieuwe leveranciers en het nieuwe landschap. De overgang vindt gefaseerd plaats om continuïteit van dienstverlening te waarborgen en risico’s voor de bedrijfsvoering te minimaliseren.

Per perceel zal een migratie- en overdrachtsplan opgesteld worden waarin onder meer verantwoordelijkheden, afhankelijkheden, fallback-scenario’s en acceptatiecriteria zijn opgenomen. Omdat de dienstverlening onderling sterk verbonden is, verwachten we van leveranciers dat zij hun planning en werkzaamheden afstemmen op de overige percelen. We hechten waarde aan een gezamenlijk resultaat dat boven het eigen belang gaat en vertrouwen door transparantie.

Een succesvolle migratie van bijvoorbeeld werkplekken is afhankelijk van de beschikbaarheid van netwerk-, telefonie- en andere diensten. De huidige ICT-dienstverlener (DICTU) zal de data aanleveren ten behoeve van de migratie.

Tijdens de migratie staat kennisoverdracht centraal. Leveranciers dragen actief kennis over aan de regieorganisatie en werken volgens uniforme documentatie- en beheerstandaarden. Hierdoor ontstaat niet alleen een werkende omgeving, maar ook een duurzaam beheersbaar landschap.

4.4 Operationele fase

Na afronding van de migraties start de operationele fase. In deze fase verschuift de focus van implementatie naar optimalisatie, doorontwikkeling en samenwerking binnen de gehele infrastructuur. We zien leveranciers nadrukkelijk als partners binnen één gezamenlijke dienstverlening die een actieve bijdrage leveren aan innovatie, beveiliging, procesverbetering en kwaliteitsverhoging.

We verwachten van leveranciers dat zij niet uitsluitend vanuit hun eigen perceel opereren, maar handelen vanuit ketenverantwoordelijkheid. Incidenten, wijzigingen en verbeterinitiatieven worden daarom integraal benaderd, waarbij samenwerking tussen leveranciers essentieel is om de continuïteit en kwaliteit van de dienstverlening te waarborgen.

We hechten waarde aan continue verbetering ten opzichte van stilstand. Om dit te ondersteunen, wordt een gezamenlijke governance ingericht met periodieke operationele, tactische en strategische overleggen. Hierin worden prestaties, afhankelijkheden, risico's, verbetermaatregelen en ontwikkelingen gezamenlijk besproken.

Met deze aanpak realiseert NEO NL een toekomstvast, flexibel en veilig IT-landschap waarin samenwerking, wendbaarheid en regie centraal staan.