



BIJLAGE A SPECIFICATIE VAN DE OPDRACHT

Europese aanbesteding

“SAP Managed Platform”

Versie : 1.0
Kenmerk : IUC25-003
Datum : 01-07-2025

INHOUDSOPGAVE

Hoofdstuk 1. Inleiding.....	4
Hoofdstuk 2. Functionals	5
Aansluitvoorwaarden	8
Hoofdstuk 3. IV kaders	12
3.1 Beveiligingseisen	12
Hoofdstuk 4. Integriteit	18
4.1. Business Etiquette	18
Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI).....	19
5.1. Algemeen.....	19
5.2. Milieu	19
5.3. Klimaat.....	19
5.4. Circulariteit (inclusief Biobased).....	19
5.5. Ketenvaartwoordelijkheid (ISV)	20
5.6. Social return	21
5.7. Diversiteit en inclusie	22
5.8. Duurzaamheidsbijdrage Inschrijver	22
Hoofdstuk 6. Juridische kaders.....	24
Hoofdstuk 7. Prijsstelling	25
7.1. Algemene eisen ten aanzien van Prijzen.....	25
7.2. Toelichting Prijscomponenten in Bijlage VIII "Prijzenformulier"	25
7.3. Specifieke eisen ten aanzien van Prijzen	27
7.4. Indexering Prijs	27
Hoofdstuk 8. Documentatie.....	29
8.1. Documentatie.....	29
Hoofdstuk 9. Voorbereiding- en Realisatiefase	30
9.1. Voorbereiding	30
9.2. Implementatie	32
9.3. Documentatie.....	32

Hoofdstuk 10. Operationele fase	33
10.1. Onderhoud en Support.....	33
10.2. Documentatie.....	43
10.3. Factureren en bestellen	43
10.4. Kaders voor (re)transitie	44

Hoofdstuk 1. Inleiding

Dit document beschrijft de eisen en wensen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding IUC25-003. Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

Hoofdstuk 2. Functionals

2.1 Functionele Eisen

Taal

GUE 1.	De Inschrijving en alle overige informatie inclusief communicatie dient volledig in de Nederlandse taal te geschieden.
--------	--

Generiek

GUE 2.	De Oplossing dient voor de Opdrachtgever verifieerbaar SAP gecertificeerd te zijn voor productief gebruik van de HANA database 2.0 SPS7 (en hoger), voor Suite on HANA, BW on HANA, BW for HANA en S/4HANA. De relevante onderdelen van de Oplossing dienen op de "Certified and supported SAP HANA hardware directory" voor te komen.
--------	--

GUE 3.	De back-up faciliteiten en alle andere delen van de Oplossing dienen op de relevante SAP lijsten voor gecertificeerde HANA Oplossingen voor te komen.
--------	---

GUE 4.	De Oplossing dient te voldoen aan de voorschriften zoals SAP stelt in best practices en configuration guides van stack onderdelen, SAP notes en SAP wiki's
--------	--

GUE 5.	Het platform dient geschikt te zijn voor deployment van Edge Integration Cell van software leverancier SAP op een hiervoor gecertificeerd Container Application Platform. Dit Container Application Platform moet draaien op de Oplossing.
--------	--

GUE 6.	Daarnaast dient de Oplossing ook geschikt te zijn voor deployment van Tricentis op Windows VM's
--------	---

GUE 7.	De Inschrijver levert als onderdeel van de Oplossing de licenties voor het Suse Linux OS, Windows OS en voor het Kubernetes open source system die onderdeel zijn van de VM's. De gekozen versies van Suse Linux OS, Kubernetes en Windows worden gebruikt voor alle virtuele Hosts van de Oplossing.
--------	--

GUE 8.	De Inschrijver levert de Oplossing als één integraal werkende dienst.
--------	---

GUE 9.	De Oplossing dient geplaatst te worden in een Datacenter van de Opdrachtgever. De Opdrachtgever beschikt over twee logische Datacenters gelegen in twee verschillende steden (Apeldoorn en Groningen). Voor beide locaties geldt dat sprake is van een twin Datacenter (dus twee in Apeldoorn en twee in Groningen). Dat houdt in dat er per plaats 1 logisch Datacenter is dat over twee, fysiek en geografisch, gescheiden Datacenters is verdeeld. De definitieve keuze voor een Datacenter wordt later bepaald.
--------	--

GUE 10.	De hoeveelheid memory die ter beschikking staat voor een Scale-up HANA Systeem op 1 server is minimaal 3 TB.
---------	--

GUE 11.	Bij aanvang van de Overeenkomst is alle Infrastructuur (hardware) binnen de Oplossing (fabrieks)nieuw en zijn alle servers (voor de workload van Opdrachtgever) binnen de Oplossing identiek.
---------	---

UE.1	In navloging van GUE 11: Bij een mogelijke verlenging van de Overeenkomst geldt dat alle hardware (servers en infrastructuur) binnen de Oplossing (fabrieks)nieuw en identiek zijn.
GUE 12.	De Oplossing dient dusdanig gedimensioneerd te zijn dat het SAP landschap hierop kan worden gedeployed, met inachtneming van de minimale sizing Gegevens in paragraaf 2.4.2 van het Beschrijvend Document. Dit geldt voor zowel CPU capaciteit als memory, de sizing van het netwerk binnen de SAP POD, de storage en de Backup & Restore Oplossing (B&R Oplossing).
GUE 13.	De storage capaciteit is te verdelen over de twin Datacenters. De in paragraaf 2.4.2 van het Beschrijvend Document genoemde capaciteit dient daadwerkelijk netto toegekend te kunnen worden aan de servers, en is dus exclusief redundantie als gevolg van RAID technieken, synchronisatie etc.
UE.2	Bij de dimensionering van de Infrastructuur moet rekening worden gehouden met het feit dat de Opdrachtgever productie - en beheer systemen bij elkaar in de ene locatie van het twin Datacenter gaat deployen, en de SOTA en secundaire HANA Systemen in de andere locatie.
GUE 14.	Binnen de Oplossing is het mogelijk om vanuit de SAP-applicatie op de hypervisor laag te kunnen kijken zoals bedoeld in o.a. SAP note “1606643 - Linux VMware vSphere host monitoring interface” en “2266266 - Key Monitoring Metrics for SAP on VMware vSphere (version 5.5 u3 and higher)”.
GUE 15.	Inschrijver levert bij Inschrijving een gedetailleerde technische beschrijving en ontwerp van de Oplossing.

W1	Technisch ontwerp Beschrijf voor welke onderwerpen en op welke manier de Inschrijver implementeert op basis van bovenstaande GUE 15. Vraag Lever een compleet ontwerp van de Oplossing aan, waarin minimaal de volgende onderdelen zijn opgenomen: • Een overzicht van alle in de Oplossing aanwezige fysieke en gevirtualiseerde componenten, inclusief type aanduiding en specificaties. Geef aan welke componenten bedoeld zijn voor het hosten van Sap databases en applicaties en welke componenten bedoeld zijn voor additionele services zoals AD, NTP, DNS, Monitoring, Log en Auditing. • Een beschrijving en schematische tekening van de netwerk topologie van de gehele Oplossing met daarin de verschillende netwerkcomponenten benoemd. • Een beschrijving en schematische tekening van het server & storage ontwerp. • Een beschrijving en schematische tekening van de backup oplossing. • Een beschrijving en schematische tekening van de datasluis oplossing. • Een beschrijving van de security maatregelen in de infrastructuur inclusief de realisatie van de toegang van beheerders van Inschrijver en opdrachtgever. • Een beschrijving van de inrichting van het beheer van de managed infrastructuur. • Een beschrijving van de schaalbaarheid van de oplossing. Verwachting De Opdrachtgever verwacht van het antwoord van de Inschrijver dat:
-----------	---

	• De beantwoording ingaat op alle hierboven genoemde aspecten. • Volledig is met een beschrijving van het ontwerp waaruit blijkt welke keuzes u heeft gemaakt met betrekking tot de ingezette techniek. • Concreet: onderbouwd waarom deze keuze(s) gemaakt zijn • Relevant is: reeds bij een andere opdrachtgever gerealiseerd, verifieerbaar en in de Gunningstest aantoonbaar etc. • Toegevoegde waarde: overtuigende beschrijving van de voordelen voor Opdrachtgever, Beoordeling: Deze wens wordt beoordeeld op basis van de mate waarin het antwoord voldoet aan de verwachtingen van de Aanbestedende dienst. Het maximale aantal punten dat behaald kan worden voor deze wens is 60 punten. <table border="1"> <tr> <th>Aantal punten</th><th>Toelichting:</th></tr> <tr> <td>0</td><td>Het antwoord op de wens voldoet niet aan de verwachtingen.</td></tr> <tr> <td>15</td><td>Het antwoord op de wens voldoet niet volledig aan de verwachtingen.</td></tr> <tr> <td>36</td><td>Het antwoord op de wens voldoet aan de verwachtingen.</td></tr> <tr> <td>60</td><td>Het antwoord op de wens overstijgt de verwachtingen van de Aanbestedende dienst doordat het Technisch Ontwerp (bovenop de omschreven verwachtingen) aanvullende, vernieuwende, originele of slimme voorstellen bevat, waar de beoordelaars positief door worden verrast.</td></tr> </table> Voorschriften uitwerking Wij vragen uw uitwerking in maximaal 15 pagina's A4 (lettertype Arial, lettergrootte 10 en regelafstand 1,0) te verwoorden. Extra pagina's en/of hyperlinks worden niet in de beoordeling meegenomen.	Aantal punten	Toelichting:	0	Het antwoord op de wens voldoet niet aan de verwachtingen.	15	Het antwoord op de wens voldoet niet volledig aan de verwachtingen.	36	Het antwoord op de wens voldoet aan de verwachtingen.	60	Het antwoord op de wens overstijgt de verwachtingen van de Aanbestedende dienst doordat het Technisch Ontwerp (bovenop de omschreven verwachtingen) aanvullende, vernieuwende, originele of slimme voorstellen bevat, waar de beoordelaars positief door worden verrast.
Aantal punten	Toelichting:										
0	Het antwoord op de wens voldoet niet aan de verwachtingen.										
15	Het antwoord op de wens voldoet niet volledig aan de verwachtingen.										
36	Het antwoord op de wens voldoet aan de verwachtingen.										
60	Het antwoord op de wens overstijgt de verwachtingen van de Aanbestedende dienst doordat het Technisch Ontwerp (bovenop de omschreven verwachtingen) aanvullende, vernieuwende, originele of slimme voorstellen bevat, waar de beoordelaars positief door worden verrast.										

Backup & Restore

Het moet mogelijk zijn om het Operating Systeem te herstellen van alle Hosts die verloren zijn gegaan. Omdat databases zoveel als mogelijk zullen worden gecombineerd op de HANA Systemen, dient de B&R van de Oplossing daarnaast ook HANA Tenant aware te zijn, zodat back-up van databases onafhankelijk van elkaar kunnen worden gemaakt en gerestored.

Tevens moeten er backups kunnen worden gemaakt van MAXDB databases (voor SAP Content Server) en Sybase ASE databases (voor SAP IDM), het Kubernetes platform, de software plus traces/logs en overige non-database files van HANA en S/4 producten en overige App. Stacks.

GUE 16.	De backup – en restore snelheid is minimaal 8 TB binnen 6 uur. De sizing van de B&R faciliteit wordt uitgevoerd door de Inschrijver, met inachtneming van de aangegeven backup-cyclus van 28 dagen. Er dient 10% extra ruimte te worden gereserveerd voor incidentele backups. De bewaartermijn van een backup dient op aanvraag van Opdrachtgever incidenteel te kunnen worden verlengd, opdat deze niet na 28 dagen wordt geruimd.
GUE 17.	De B&R Oplossing voorziet in opslag van de back-up in één Datacenter locatie van de Opdrachtgever, waarbij een Incident op de ene locatie niet kan leiden tot een verstoring op de andere. Het veiligstellen van de back-up op deze locatie dient binnen 12 (Klok)uren voltooid te zijn.
GUE 18.	De Beschikbaarheid en de bruikbaarheid van de B&R Oplossing dient op beide locaties van het Twin Datacenter identiek te zijn, onafhankelijk van de SOTA/PB inrichting.

GUE 19.	De B&R Oplossing dient te voldoen aan het Domain Fault principe: fouten in de gebruikte technologie in de primaire opslag mogen niet leiden tot onbeschikbaarheid van de B&R van de Oplossing en de Beschikbaarheid en integriteit van de Gegevens. Het gaat hierbij specifiek om fouten in de software van het opslag systeem.
GUE 20.	De Oplossing dient aangeboden te worden inclusief back-up voorzieningen op de beide fysieke locaties.
GUE 21.	Inschrijver is in staat om het Operating System te herstellen (o.a. in elk opzicht identiek draaiend OS, virtuele hostnaam, netwerk- en firewall instellingen) van alle Hosts die verloren zijn gegaan.
GUE 22.	De Oplossing voorziet in functionaliteit om backups te maken van HANA DB, Sybase ASE, SAPDB en verder alle non-database SAP-directories zoals bijvoorbeeld software, logs, traces, profiles.
GUE 23.	De Oplossing voorziet in functionaliteit om backups te maken van meerdere databases op één HANA Systeem, onafhankelijk van elkaar (Tenant aware).
GUE 24.	De B&R van de Oplossing heeft een retentie cyclus van 28 dagen.
GUE 25.	De Oplossing dient de mogelijkheid te bieden om database back-ups te maken naar disk, te weten back-up storage. Deze storage wordt aangeboden door de Opdrachtgever, welke middels nfs4.1 of hoger dient te kunnen worden gemount. De database back-ups zijn afkomstig van SAP HANA, Sybase en SAP MaxDB.
GUE 26.	De Oplossing is voorzien van monitoring van datagebruik en toegang. Daarbij dient de monitoring abnormal behavior gedrag monitoren, rapporteren (alerten) en het data gebruik te auditen. (Anomaly detection).
GUE 27.	Back-ups moeten immutable weg geschreven kunnen worden.
GUE 28.	Indien immutability aangepast kan worden en/of opgeheven kan worden dient dit minimaal op basis van vier ogen principe en twee Active Directory (AD) accounts inclusief Multi-Factorauthenticatie (MFA) uitgevoerd te kunnen worden (Lokale accounts worden uitgesloten van aanpassing).
GUE 29.	Voor immutability dient er gebruik gemaakt te worden van de Network Time Protocol (NTP) servers van de Opdrachtgever of een interne NTP server binnen de Oplossing. Bij aanpassingen aan de NTP configuratie of pogingen om de systeemtijd te verzetten dienen alerts afgegeven te worden.

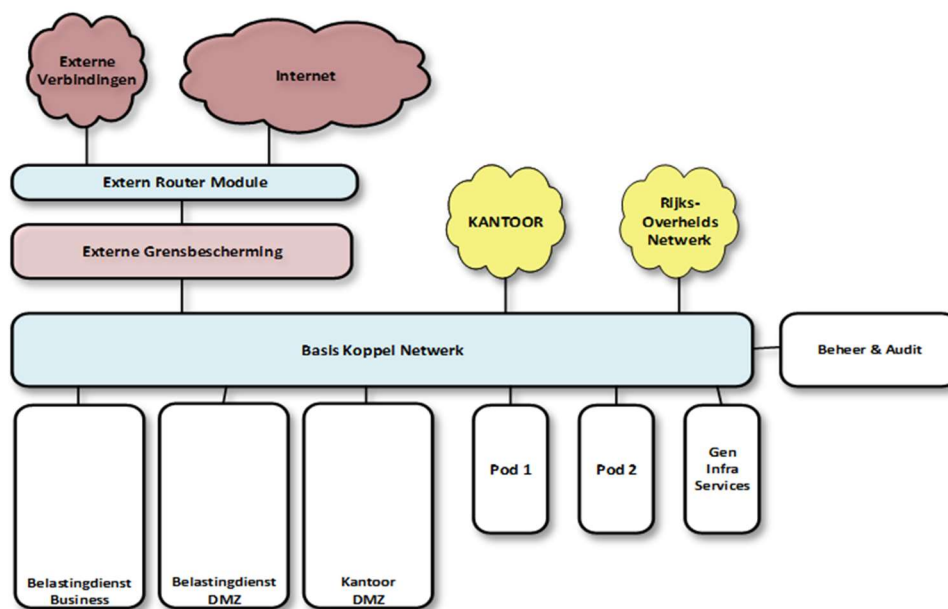
Aansluitvoorwaarden

De Infrastructuur wordt geplaatst in het Twin Datacenter van de Opdrachtgever en moet voldoen aan de daarvoor geldende voorwaarden.

GUE 30.	Het plaatsen, inrichten en operationeel maken van de benodigde Infrastructuur dient te voldoen aan de aansluitvoorwaarden van het Twin Datacenter van de Opdrachtgever. Deze aansluitvoorwaarden zijn opgenomen in Bijlage 7 -Technische Aansluitvoorwaarden Housing ODC Belastingdienst
---------	--

De Oplossing zal binnen het Twin Datacenter van de Opdrachtgever worden opgenomen in een zogenaamde PoD.

GUE 31. De Inschrijver levert de netwerkvoorzieningen binnen de SAP PoD, richt deze in en voert het beheer hierop uit.



Afbeelding 1: PoD

PoD's (zie afbeelding 1) worden op het Basis Koppel Netwerk (BKN) aangesloten. Dit is een gestandaardiseerd koppelvlak waar de verantwoordelijkheid van de PoD-eigenaar eindigt. Via het BKN kan een PoD met andere PoD's en netwerken communiceren.

GUE 32. De Oplossing dient te voldoen aan de Aansluitvoorwaarden Netwerk Aansluitdiensten Datacenter Basiskoppelnets conform Bijlage 8 - Aansluitvoorwaarden Netwerkaansluitdiensten Datacenter Basiskoppelnets.

De eigenaar van de diensten die geleverd worden vanuit een PoD is verantwoordelijk voor zijn eigen Beveiliging. Eén van de aspecten hiervan is de toegang tot een PoD vanuit een ander(e) PoD/netwerk. De PoD die wordt benaderd zal ervoor moeten zorgen dat alleen die services benaderbaar zijn die benaderbaar mogen zijn. Dat wordt gerealiseerd door het netwerkverkeer tussen het BKN en een service (applicatie) binnen de PoD te filteren/blokkeren.

GUE 33. De Inschrijver levert de hierboven omschreven filtering functie tussen het BKN en de services binnen de SAP PoD in de vorm van een firewall. Deze dient compliant te zijn aan actuele marktstandaarden en tenminste 5 Gbps doorvoersnelheid aan te kunnen. Op beide locaties van het Twin Datacenter dient in deze filtering functie te worden voorzien. Hierbij doet de Inschrijver het Technisch beheer van deze functie terwijl de Opdrachtgever de functioneel eigenaar is en bepaalt welke stromen open gezet mogen worden.

De Inschrijver krijgt van de Opdrachtgever een IP-reeks waaruit de IP-adressen van de verschillende Host in de SAP PoD moeten worden toegewezen. Omdat de firewalls, die door de Opdrachtgever worden beheerd in dit concept op basis van IP-adressen filteren zullen de Hosts in de PoD dezelfde IP-adressen moeten behouden

- | | |
|---------|--|
| GUE 34. | De IP adressen binnen de SAP PoD komen uit de Opdrachtgever IP reeksen die door de Opdrachtgever wordt beheerd en uitgedeeld. Dit zijn statische IP adressen, welke door de Inschrijver gebruikt te dienen worden. |
|---------|--|

Binnen de PoD moet er een Domein Name Server (DNS) worden geplaatst waardoor systemen binnen de PoD op basis van DNS namen met elkaar kunnen communiceren. Ook zal een forwarder moeten worden opgenomen naar de nameserver van de Opdrachtgever waardoor communicatie met andere PoD's op basis van DNS mogelijk is.

De Inschrijver zal in haar DNS een forwarder opnemen naar de nameserver in de SAP PoD. Hiermee kunnen systemen buiten de SAP PoD IP-adressen van Hosts in de SAP-PoD resoven.

- | | |
|---------|--|
| GUE 35. | De Inschrijver biedt een authoritative nameserver binnen de PoD waarmee Hosts in de PoD IP-adressen van andere Hosts in deze of andere PoD's kunnen resoven. Als een Dynamic Host Configuration Protocol (DHCP) server benodigd is voor het uitdelen van ip-adressen binnen de SAP PoD, dan dient deze door de Inschrijver te worden geleverd en onderhouden en bij de Prijs inbegrepen te zijn. |
|---------|--|

- | | |
|---------|--|
| GUE 36. | De Inschrijver stelt NTP op basis van stratum twee beschikbaar aan een NTP-server binnen de SAP PoD. NTP-clients binnen de SAP PoD halen hun tijd bij deze server. De Inschrijver biedt een NTP-server binnen de PoD waarmee NTP-clients in de PoD hun tijd synchroniseren |
|---------|--|

- | | |
|---------|---|
| GUE 37. | De Dark Fiber tussen beide Datacenters moet gebruikt worden voor replicatie van storage, backup en HANA replicatie. De datastroom tussen beide Datacenters moet encrypted zijn. |
|---------|---|

- | | |
|---------|---|
| GUE 38. | Versleuteling van de Gegevens geschiedt met een door NIST of NCSC aanbevolen encryptie algoritmes van minimaal 128 bits.
(http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#Approved Algorithms) |
|---------|---|

- | | |
|------|--|
| UE.3 | De Opdrachtnemer zorgt ervoor dat de versleuteling ook in de toekomst aangesloten blijft bij marktconforme encryptie-algoritmes. |
|------|--|

Scheiding van omgevingen

- | | |
|---------|---|
| GUE 39. | De Oplossing moet een netwerktopologie ondersteunen waarbij er een netwerkscheiding wordt gemaakt tussen de verschillende domeinen (zie Bijlage V – SAP Landschap). Eventueel verkeer tussen deze segmenten zal moeten worden gefilterd. Deze zonering wordt door de firewall afgedwongen. De inrichting van deze firewall ligt bij de Inschrijver. |
|---------|---|

- | | |
|---------|--|
| GUE 40. | Communicatie met het Internet vindt plaats via de demilitarized zone (DMZ) binnen het netwerk van de Opdrachtgever |
|---------|--|

- | | |
|---------|--|
| GUE 41. | Alle technische koppelingen (waaronder interfaces, Gegevensuitwisselingen en API's) tussen de Oplossing en systemen die niet tot de Oplossing behoren, zijn gedocumenteerd. Deze Documentatie is actueel, correct en wordt permanent ter beschikbaar gesteld aan de opdrachtgever. |
|---------|--|

Beheerderstoegang

- | | |
|---------|--|
| GUE 42. | Inschrijver is verantwoordelijk voor de inrichting van authenticatie en autorisatie op de geleverde Oplossing middels een Identity Management systeem. |
|---------|--|

GUE 43.	De Oplossing dient te voorzien in de autorisatie en authenticatie van de beheerders van de Opdrachtgever die uit hoofde van hun verantwoordelijkheid voor het uitvoeren van SAP gerelateerde werkzaamheden toegang dienen te hebben tot de Infrastructuur.
GUE 44.	Alle aanpassingen die door medewerkers van de Inschrijver en/of Opdrachtgever op de Infrastructuur worden uitgevoerd, worden gelogd.
GUE 45.	De Inschrijver voorkomt ongeautoriseerd gebruik van Root-access.
GUE 46.	Indien medewerkers van de Opdrachtgever Root-access moeten gebruiken, dienen alle handelingen van de betreffende medewerker herleidbaar te zijn.
GUE 47.	Bij gebruik van root-access, moet gebruik gemaakt worden van het Sudo (superuser do) mechanisme.

Hoofdstuk 3. IV kaders

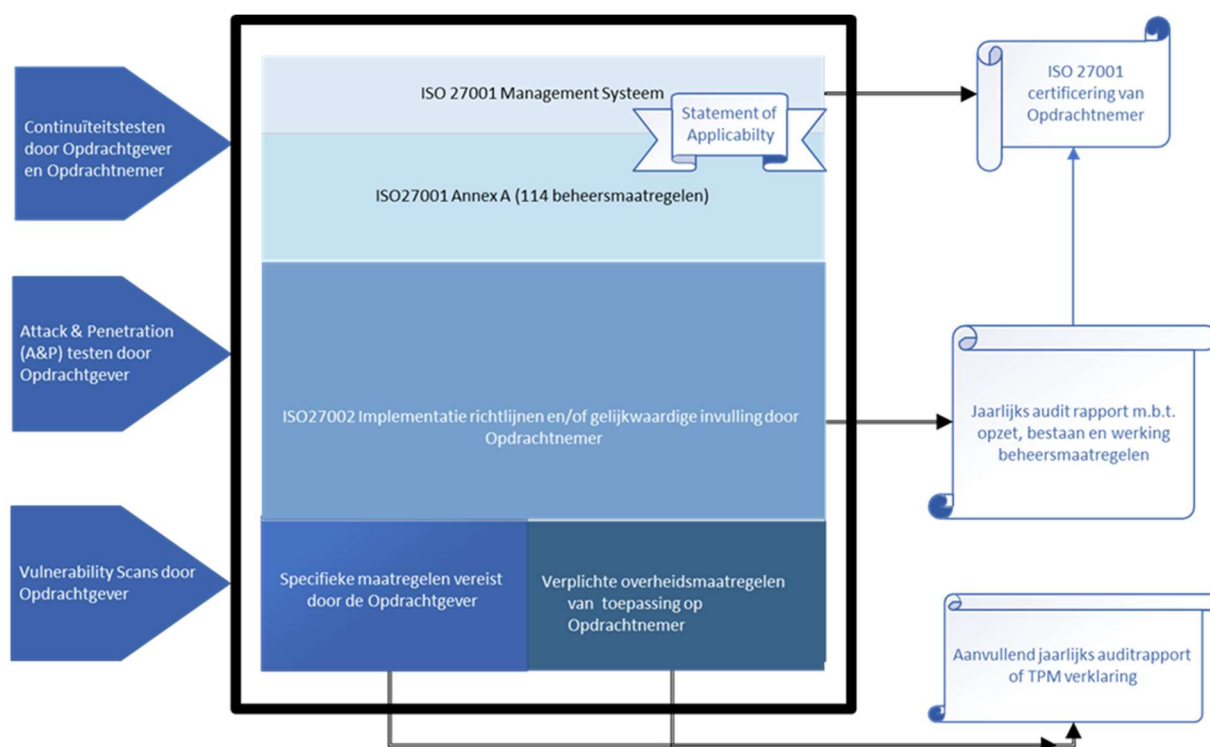
3.1

Beveiligingseisen

De Opdrachtgever verwerkt fiscale en financiële Gegevens van particulieren en ondernemingen. De omgang met deze Gegevens vraagt van de Opdrachtgever een werkwijze die de vertrouwelijkheid en integriteit van deze Gegevens waarborgt. Bij het betrekken van producten en diensten uit de markt dient een deel van de verantwoordelijkheden ingevuld te worden door de Inschrijver. De Inschrijver moet dus minimaal hetzelfde beveiligingsniveau leveren als de Opdrachtgever.

De Opdrachtgever is gehouden aan de Baseline Informatiebeveiliging Overheid (BIO). Deze regelgeving is gebaseerd op de ISO27001 en de ISO27002, en bevat daarnaast aanvullende beveiligingseisen, de zogenoemde overheidsmaatregelen. Vanwege de eigen technische inrichting, stelt de Opdrachtgever zelf ook specifieke beveiligingseisen.

In onderstaande figuur is de samenhang weergegeven tussen beveiligingsmaatregelen, de kaders ISO27001/2 en de BIO, certificering, Audit, en test.



In deze paragraaf stelt de Opdrachtgever eisen die specifiek zijn voor de Opdrachtgever. Hier zijn ook eisen opgenomen om te borgen dat de Opdrachtgever aan het overheidsinformatiebeveiligingsbeleid (Baseline Informatiebeveiliging Overheid, hierna BIO¹) kan voldoen (zie ook Bijlage XIII – BIO). De hier opgenomen eisen zijn dus aanvullend op wat reeds via certificering en de auditcyclus wordt uitgevraagd. Het legt dus aan de ene kant accenten op onderdelen die reeds onderdeel uitmaken van een op 27001/2-gebaseerd Informatiebeveiligingsbeleid, aangevuld met overheids- en Opdrachtgever specifieke zaken.

3.1.1 Forum Standardisatie

De Opdrachtgever is als overheidspartij gehouden aan de standaarden, zoals vastgesteld door het Forum Standardisatie. De verplichte standaarden worden toegepast conform het Pas-toe-of-leg-uit-principe (Comply-or-Explain). Van een aantal standaarden heeft de Opdrachtgever overigens vastgesteld dat Inschrijver deze standaarden moet toepassen (dus zonder Leg-uit-mogelijkheid).

¹ https://www.bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf

Dit is ook van toepassing gedurende de Looptijd van de Overeenkomst. Als deze lijst met standaarden of de standaarden zelf inhoudelijk wijzigen zullen tussentijds afspraken gemaakt worden ter implementatie.

UE.4	Inschrijver committeert zich aan het gebruik van de Verplichte standaarden van het Forum Standaardisatie in relatie tot de Oplossing. Het betreft de volgende standaarden: Opdrachtnemer is in staat voor alle webverbindingen van de Oplossing HTTPS en HSTS toe te passen conform de richtlijnen van het NCSC. Er wordt alleen gebruik gemaakt van standaarden en instellingen die door het NCSC als 'Goed' zijn gekwalificeerd ("ICT-beveiligingsrichtlijnen voor Transport Layer Security"). Met de 'Qualys SSL Labs SSL Server Test' (https://www.ssllabs.com/ssltest/) wordt minimaal een A- behaald. Alleen met nadrukkelijke toestemming van de Opdrachtgever kan hier van worden afgeweken. Inschrijver gaat akkoord met het toepassen van wijzigingen op basis van wijzigingen bij het Forum van Standaardisatie.
------	---

3.2.2 Richtlijnen rond Beveiligingsincidenten

Beveiligingsincidenten zijn incidenten die een vermoedelijke of mogelijk opzettelijke inbreuk veroorzaken op de beschikbaarheid, vertrouwelijkheid of integriteit van de Gegevens in informatie verwerkende systemen of inbreuk maken op deze systemen zelf. Indien er aanleiding toe is dan kan de Opdrachtnemer besluiten zelf een Audit (al dan niet op alle onderdelen) uit te laten voeren op de Oplossing.

GUE 48.	Inschrijver beschikt over een meldloket waar beveiligingsincidenten en (potentiële) Datalekken per direct het hele jaar door 24/7 gemeld kunnen worden. Opdrachtnemer zal de omvang van het incident aangeven, de verwachte consequenties voor de Belastingdienst alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken.
---------	--

UE.5	De Opdrachtgever heeft het recht om zelf (een deel van) de Oplossing aan een Audit te onderwerpen. De basis van de Audit is deze Bijlage A Specificatie van de Opdracht.
------	---

UE.6	Opdrachtnemer heeft van zijn Personeel met toegang tot de Oplossing en haar Gegevens de achtergrond geverifieerd conform relevante wet- en regelgeving. Voor Nederlandse ingezetenen wordt gebruik gemaakt van de VOG. Voor niet-ingezetenen kan een gelijkwaardige verklaring worden overlegd.
------	---

GUE 49.	Gegevens mogen het Datacenter van de Opdrachtgever op geen enkele manier verlaten, ook niet via een scherm, een backup, een afdruk of een dataverbinding. Met uitzondering van remote uitwisselingsmechanisme.
---------	---

GUE 50.	Back-ups van data- en logbestanden dienen versleuteld te worden.
---------	---

GUE 51.	Back-ups mogen het Datacenter van de Opdrachtgever niet verlaten.
---------	--

GUE 52.	Alle onderdelen van de Oplossing die Gegevensdragers bevatten behoren voorafgaand aan verwijdering te worden geverifieerd om te waarborgen dat gevoelige Gegevens en in licentie gegeven software zijn verwijderd of betrouwbaar veilig zijn overschreven (gewist) met een door de overheid gecertificeerd product, zie: https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten
---------	--

Beveiligingstesten (A&P-test, Vulnerability scan) worden regelmatig uitgevoerd op de Oplossing. Normaal gesproken gebeurt dit door de Opdrachtnemer, maar de Opdrachtgever behoudt zich het recht voor ook beveiligingstesten uit te (laten) voeren als hij dit noodzakelijk wordt geacht. In het geval van A&P-testen maakt de Opdrachtgever gebruik van onafhankelijke A&P-testbedrijven. Er is dan een 'Vrijwaringsverklaring Pentesten' nodig. Als er ook Broncodeonderzoek uitgevoerd moet worden dan kan Opdrachtnemer een (aanvullende) 'Non-disclosure agreement Broncodeonderzoek' afsluiten met de A&P-testpartij.

UE.7	Opdrachtnemer en de Opdrachtgever besluiten gezamenlijk de scope van de A&P test. Mochten Partijen er niet gezamenlijk uit komen, dan neemt de Opdrachtgever de uiteindelijke beslissing hierover. De resultaten van de testen worden gedeeld met de Opdrachtnemer. De resultaten worden middels het Common Vulnerability Scoring System (CVSS 4.0) gekwalificeerd door het bureau dat de A&P-test uitvoert in overleg met de Opdrachtgever. Bij het bespreken van de Bevindingen worden afspraken gemaakt met Opdrachtnemer over de Oplostijden en de aansluitende hertest
UE.8	Mochten er na een hertest nog onopgeloste Bevindingen met de classificatie Medium of hoger open staan, dan worden er nieuwe afspraken gemaakt over de Oplostijden voor de nog onopgeloste Bevindingen.
UE.9	A&P tests vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer
UE.10	De Opdrachtgever heeft het recht om Vulnerability scans op de Oplossing uit te laten voeren door het Security Operation Center (SOC) van de Opdrachtgever
UE.11	De Bevindingen worden indien nodig gedeeld en besproken met de Chief Security Officer (CSO) van de Opdrachtnemer. Gevonden kwetsbaarheden worden kosteloos opgelost door Opdrachtnemer
UE.12	De Opdrachtgever voert periodiek –bij voorkeur maandelijks- maandelijks een Vulnerability scan uit op de Oplossing conform haar richtlijnen. Eventuele Kwetsbaarheden die binnen de scope van de Opdrachtnemer vallen, worden conform de richtlijnen van de Opdrachtgever opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.
UE.13	Opdrachtnemer werkt mee aan de Vulnerability scans die door de Opdrachtgever worden uitgevoerd.
UE.14	Opdrachtnemer zorgt ervoor dat het SOC de benodigde toegang heeft om deze scan uit te voeren.
UE.15	Vulnerability scans vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer.

De Opdrachtgever wenst inzage in het beveiligingstestbeleid van Inschrijver. Het betreft opzet, bestaan en zo mogelijk werking van de A&P-testen en Vulnerability scans. Hiertoe worden documenten aangeleverd waarin het beveiligingstestbeleid wordt beschreven en hoe eventuele tekortkomingen worden afgehandeld. Ook moet blijken onder welke omstandigheden dergelijke beveiligingstesten worden uitgevoerd en dat deze worden uitgevoerd

UE.16	Opdrachtnemer informeert de Opdrachtgever onmiddellijk wanneer er een kwetsbaarheid wordt geconstateerd of verwacht, betreffende de Gegevens en/of de Oplossing waar de Opdrachtgever gebruik van maakt die ook in gebruik zijn bij andere klanten van Opdrachtnemer. Opdrachtnemer zal in dat geval tevens de omvang van de kwetsbaarheid aangeven, de verwachte consequenties voor de Opdrachtgever alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken. Dit proces zal beschreven worden in de nog overeen te komen DAP.
-------	---

Voor Beveiligingsincidenten geldt dat bij ontdekking/melding zowel de Impact als Urgentie als Hoog worden gekwalificeerd wat resulteert in een prioriteit 1 Incident. Een Beveiligingsincident wordt altijd per direct opgevolgd met een actie van de Opdrachtnemer.

Na een eerste evaluatie kan onderbouwd besloten worden de prioriteit te verlagen. De Opdrachtgever heeft hierbij het laatste woord.

Er worden vier typen Beveiligingsincident onderkend:

1. (Cyber)hack, of een poging daartoe. Dit is inclusief malware.
2. Coordinated Vulnerability Disclosure (CVD, voorheen: Responsible disclosure).
3. Kwetsbaarheid via CVE-database of Security Note van leverancier van ICT-component of beveiligingsberichten van CERT's (NCSC, Digital Trust Center, bedrijfstak- of sectorgerichte CERT).
4. Kwetsbaarheid vanuit beveiligingstest (A&P-test of Vulnerability scan)

Als waarderingsmethodiek voor kwetsbaarheden wordt gebruik gemaakt van de meest recente versie van marktstandaard Common Vulnerability Score System (CVSS, momenteel versie 4.x). Oplostermijnen die hier aan gekoppeld zijn, zijn:

- Kritisch risico (Critical risk, score 9.0 – 10.0): per direct (voor in productie gaan van een nieuwe Oplossing is dit belemmerend). Voor de Opdrachtgever is dit een incident.
- Hoog risico (High risk, score 7.0 – 8.9): per direct, na afstemming maximaal 1 maand (voor in productie gaan van een nieuwe Oplossing is dit belemmerend). Voor de Opdrachtgever is dit een incident.
- Gemiddeld risico (Medium risk, score 4.0 – 6.9): 3 maanden. Voor de Opdrachtgever is dit een probleem.
- Laag risico (Low risk, 0.1 – 3.9): 6 maanden. Voor de Opdrachtgever is dit een probleem.

Voordat de Oplossing in productie kan gaan is de beveiliging van de Oplossing getest ter acceptatie. Daarna gebeurt dat periodiek (minimaal jaarlijks).

De Belastingdienst heeft geen Oplossingen in productie staan waarin zich Kwetsbaarheden bevinden die als Kritisch of Hoog risico zijn gekwalificeerd. Bij Kritische- en Hoge risico's kan een Leg-uit alleen gebruikt worden om de oplostermijn (beperkt) op te rekken. Dit kan alleen met nadrukkelijke instemming van de Belastingdienst. Het Stekkermanaat wordt uitgevoerd als de Oplossing reeds in productie staat. Staat de Oplossing nog niet in productie dan zal dat ook niet mogen totdat de Kritische- en Hoge risicobevindingen zijn weggenomen. Bekende kwetsbaarheden worden onverwijld gemeld.

Gemiddeld- en Laagrisico bevindingen worden afgehandeld conform het Pas-toe-of-Leg-uitprincipe. Dit laatste, een Leg uit (Explain), betekent dat er besloten is dat de kwetsbaarheid niet weggenomen wordt of dat adresseren ervan meer tijd gaat kosten dan de standaard Oplostermijn. Opdrachtnemer onderbouwt zijn besluit (bijvoorbeeld: er zijn afdoende mitigerende maatregelen getroffen waardoor de kwetsbaarheid niet uitgevoerd hoeft te worden of dat de impact nihil is). Het is aan de Belastingdienst om akkoord te gaan met een Leg-uit.

UE.17	Inschrijver conformeert zich aan de door de Opdrachtgever gebruikte methode (CVSS4.0) om beveiligingsincidenten te kwalificeren en heeft zijn organisatie zodanig ingericht dat de door de Opdrachtgever onderkende typen beveiligingsincidenten voor (onderdelen) van de Oplossing binnen gestelde termijnen opgepakt en opgelost (patchmanagement) worden: • Kritisch risico (Critical risk): per direct (belemmerend voor in productie gaan). • Hoog risico (High risk): 1 maand (belemmerend voor in productie gaan). • Gemiddeld risico (Medium risk): 3 maanden • Laag risico (Low risk): 6 maanden • Een aanpassing van de CVSS Oplostijden kan alleen in overleg met Opdrachtgever. • Security Incidenten worden standaard geclassificeerd als Prio 1 totdat er volgens de CVSS 4.0 bepaald kan worden in welke categorie het Incident thuis hoort. • Opdrachtnemer dient bij het constateren van een kwetsbaarheid met niveau Kritisch (Critical) of Hoog (High Risk) direct (binnen het uur) Opdrachtgever hierover te informeren. • De procedure voor het melden wordt opgenomen in de SLA en/of DAP.
-------	---

3.2.2 Autorisatie en Authenticatie

Toegang tot Oplossing en Gegevens van de Opdrachtgever gebeurt op basis van need-to-know en least privilege. Anders gezegd: gebruikers van zowel Opdrachtgever als Opdrachtnemer krijgen alleen die rechten die nodig zijn voor het uitoefenen van hun vastgestelde taken voor wat betreft Gegevens en functionaliteit van de Oplossing. Dit is overigens ook van toepassing op raakvlaksystemen (koppelende applicaties). De Oplossing is zodanig ingericht dat deze principes zijn toe te passen.

UE.18	Toegang tot de Oplossing (inclusief raakvlaksystemen en tooling) en de Gegevens van de Opdrachtgever gebeurt op basis van de principes need-to-know en least privilege. De Oplossing heeft de (technische) mogelijkheden om invulling te geven aan deze principes.
-------	--

Oplossing en bijbehorende functies en Gegevens mogen alleen gebruikt worden door bevoegde personen. Dit gebeurt door middel van identificatie, authenticatie en autorisatie. Aanvullend kan gekozen worden voor een vorm van multi-factor authentication

Bij authenticatie kan het nodig zijn aanvullend bewijs te leveren. Dit kan door een aanvullende verificatiecode te vragen. Dit gebeurt middels two-factor authentication (MFA).

Een gebruikersaccount is altijd te herleiden naar een Natuurlijk Persoon. Uitzondering zijn gedocumenteerde en geregistreerde systeemaccounts (bijvoorbeeld voor koppelingen).

UE.19	Een gebruikersidentificatie (gebruikersaccount) is altijd één op één herleidbaar naar een Natuurlijk Persoon of een gedocumenteerd en geregistreerd systeem account.
-------	--

De Opdrachtgever stelt de volgende algemene eisen aan authenticatie. Zo is het gebruik van intern gebruikte userIDs niet toegestaan (mailadres van werk mag wel).

UE.20	Wachtwoorden voldoen minimaal aan de onderstaande eisen Algemeen (technisch afdwingen) - Gebruik van wachtwoorden wordt geautomatiseerd afgedwongen - Initiële wachtwoorden (inclusief die gereset zijn) zijn een werkdag geldig en worden bij eerste gebruik gewijzigd. - Eisen aan wachtwoorden worden geautomatiseerd afgedwongen. Indien geen MFA: - Minimaal 12 posities, complex (nummers, klein, groot) - Aantal foutieve inlogpogingen: 10. In dat geval: blokkering account - Minimaal jaarlijks vernieuwen
-------	---

UE.21	Voor authenticatie sluit de Oplossing aan op het aangegeven authenticatiemechanisme van de Opdrachtgever met inachtneming van de daarvoor van toepassing zijnde beveiligingseisen.
-------	--

Gebruikers van Opdrachtnemer en Opdrachtgever met speciale (beheer)rechten binnen de Oplossing of met uitgebreide toegang en mogelijkheden tot de Gegevens, maken gebruik van multi-factor authentication (MFA). Voor andere gebruikers bestaat de mogelijkheid dit aan te zetten.

UE.22	De Oplossing heeft een multi-factor authentication mechanisme. Voor alle Gebruikers met verhoogde rechten (bijvoorbeeld: beheerrechten) is het gebruik verplicht.
-------	---

De Opdrachtgever maakt gebruik van door de Opdrachtgever geaccepteerde methoden en technieken om koppelingen tussen zijn ICT-systemen onderling en zijn ICT-systemen en Oplossingen van Opdrachtnemers aan elkaar te koppelen. Ook stelt de Opdrachtgever eisen aan koppelingen van de Oplossing met andere niet-Opdrachtgerpartijen. Denk aan verplichte API's, versleutelingseigenschappen, en dergelijke.

UE.23	Bij koppeling van de Oplossing aan een systeem van de Opdrachtgever wordt voldaan aan de Aansluitvoorwaarden (Bijlage 7) van de Opdrachtgever.
-------	--

Hoofdstuk 4. Integriteit

4.1. Business Etiquette

Opdrachtgever maakt graag gebruik van de kennis en innovatieve kracht uit de markt. Daarvoor werkt de Opdrachtgever samen met opdrachtnemers. In deze samenwerking speelt u dus een essentiële rol. Opdrachtgever vindt onpartijdigheid en transparantie belangrijk. Daarom maken we afspraken hierover: onze Business Etiquette.

UE.24	Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage 4 - Business etiquette van het Beschrijvend Document.
-------	---

Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI)

Het Inkoopuitvoeringscentrum (IUC) van de Opdrachtgever heeft ambitie op het gebied van duurzaamheid. Zij wil klanten, behoeftebestellers en leveranciers begeleiden in het vormgeven van de duurzaamheidsaspecten in producten en diensten op het vlak van bedrijfsvoering, bij aanbestedingen en gedurende de looptijd van de contracten (maatschappelijk verantwoord inkopen).

Maatschappelijk Verantwoord Inkopen (MVI) binnen de overheid is een uitvloeisel van een politiek besluit. Sinds 2010 is de rijksoverheid verplicht 100% duurzaam in te kopen. Door gelijktijdig milieu-, sociale- en economische afwegingen in alle aankopen mee te nemen leidt dit tot winst voor de belastingbetaler, de overheidsorganisatie en de samenleving. Het nieuwe regeerakkoord stelt dat de overheid zijn inkoopkracht beter gaat benutten voor het versnellen van duurzame transities, inschakelen van kwetsbare groepen en om innovatief in te kopen.

Hoe de Opdrachtgever MVI wil toepassen op deze opdracht vindt u in de volgende paragrafen. Hierin zijn de toepasselijke MVI thema's beschreven.

5.1. Algemeen

UE.25	Opdrachtnemer voldoet gedurende de gehele looptijd van de Overeenkomst aantoonbaar aan alle vigerende milieu en Arbo wet- en regelgeving.
-------	---

5.2. Milieu

Dit thema gaat over voorkomen van een negatieve impact op milieu of over het leveren van een positieve bijdrage. Aspecten van dit thema zijn:

- Lucht, water en bodem;
- Natuur en biodiversiteit;
- Ruimtegebruik, watergebruik en inzet van landbouwgrond.

5.3. Klimaat

Het gaat binnen dit thema om het voorkomen of minimaliseren van de uitstoot van CO₂ en andere broeikasgassen. Aspecten van dit thema zijn:

- Uitstoot van CO₂, methaan, lachgas en waterdamp;
- Energieverbruik en de transitie naar duurzame energiebronnen.

Mogelijke prestatie-indicatoren zijn de CO₂-voetafdruk of de hoeveelheid duurzaam opgewekte energie (percentage of kWh).

5.4. Circulariteit (inclusief Biobased)

In een circulaire economie worden producten en materialen eendeloos hergebruikt, zodat afval niet meer bestaat. Hierdoor behouden producten en materialen hun waarde en wordt verspilling van grondstoffen voorkomen. Om inzet van fossiele, schaarse en niet duurzaam gewonnen grondstoffen te minimaliseren zijn biograndstoffen in een circulaire economie essentieel. Zo kunnen bijvoorbeeld bladeren van landbouwgewassen worden gebruikt om gevelplaten te maken.

Het gaat binnen dit thema om:

- Materialen en grondstoffen;
- Levensduurverlenging;
- Hoogwaardig hergebruik;
- Biobased materiaalgebruik.

Mogelijke prestatie-indicatoren zijn materiaalbesparing in m³ of kg, het percentage hergebruikt materiaal, de impact bepaald door een levenscyclusanalyse (LCA) of de mate waarin levensduurverlenging mogelijk is.

5.5. Ketenvaantwoordelijkheid (ISV)

De internationale sociale voorwaarden (ISV) richten zich op het voorkomen en aanpakken van misstanden op het gebied van arbeidsomstandigheden, mensenrechten en milieu in de toeleveringsketen. Deze voorwaarden vereisen dat leveranciers actie ondernemen om risico's hierop in de keten te verkleinen. Aspecten van dit thema zijn:

- Geen dwangarbeid en kinderarbeid;
- Goede werkomstandigheden;
- Leefbaar loon en leefbaar inkomen;
- Geen discriminatie.

Mogelijke stappen zijn een risicoanalyse en Plan van aanpak om risico's in de keten te prioriteren en mitigeren.

5.5.1. Internationale Sociale Voorwaarden

De Internationale Sociale Voorwaarden (ISV) dragen bij aan het uitbannen van sociale misstanden in de inkoopketen, zoals kinderarbeid, hongerlonen en onmenselijke werkomstandigheden. Via een proces van due diligence richten de ISV zich op het bevorderen van het naleven van de internationale arbeidsnormen en mensenrechten in de productieketens van Rijksleveranciers.

Voor nadere informatie zie Bijlage 3 – 'Handreiking Due Diligence'. Door middel van het inschrijven op onderhavige aanbesteding committeert Inschrijver zich aan het naleven van de ISV. Dit is aldus een uitvoeringsvoorwaarde.

UE.26	Opdrachtnemer committeert zich aan bovenstaande zoals beschreven in dit hoofdstuk.
UE.27	Opdrachtnemer committeert zich aan bovenstaande zoals beschreven in paragraaf 5.5 en 5.5.1 en verplicht zich om de gestelde normen te implementeren, voor zover uit die normen een verantwoordelijkheid voor Opdrachtnemer voortvloeit, door in het kader van de uitvoering van de Overeenkomst de navolgende werkzaamheden te verrichten. • De fundamentele arbeidsnormen, zoals vastgelegd in de conventies van de International Labour Organisation (ILO), inzake afschaffing van dwangarbeid en slavernij (29, 105), afschaffing van kinderarbeid (138, 182), vrijwaring van discriminatie op het werk en in beroep (100, 111), de vrijheid van vakvereniging en recht op collectief onderhandelen (87, 98). • De mensenrechten uit de Universele Verklaring van de Rechten van de Mens (UVRM) en uitwerkingen daarvan in bindende verdragen, die arbeids- en bedrijfsrelevant zijn.
UE.28	Uiterlijk 3 maanden na startdatum Operationele fase levert de Opdrachtnemer aan Opdrachtgever een risicoanalyse aan van de risico's op schending van arbeids- en mensenrechten van de gehele keten.
UE.29	<i>Plan van aanpak mitigeren risico's:</i> Indien van toepassing levert Opdrachtnemer uiterlijk 6 maanden na de definitieve gunning van de opdracht een Plan van aanpak op om de risico's die in de risicoanalyse zijn vermeld te mitigeren. In het Plan van aanpak zijn opgenomen: • een overzicht en beschrijving van de inspanningen die de Opdrachtnemer zal leveren om de risico's te mitigeren (SMART); • een planning ten aanzien van de inspanningen die de Opdrachtnemer zal leveren; • (optioneel) een toelichting op het tot stand komen van het Plan van aanpak, bijvoorbeeld informatie over de betrokkenheid van stakeholders. Het plan van aanpak moet inzichtelijk maken hoe de inspanningen volgens de Opdrachtnemer leiden tot een concrete aanpak van de risico's die op basis van de risicoanalyse (UE.28) geprioriteerd zijn. Als het niet mogelijk is om alle risico's aan te pakken, moet worden begonnen met de meest ernstige risico's. Opdrachtnemer maakt in dat geval inzichtelijk voor Opdrachtgever waarom niet alle risico's aangepakt konden worden.

UE.30	<i>Monitor de praktische toepassingen en resultaten</i> Gedurende de contractperiode rapporteert de Opdrachtnemer jaarlijks ten opzichte van de ingangsdatum van de Overeenkomst over zijn inzet ten aanzien van het naleven van de ISV. Hieruit moet blijken dat de Opdrachtnemer een ‘redelijke inspanning’ heeft geleverd om de ISV na te leven. De rapportage moet tevens gelijktijdig openbaar worden gemaakt, al dan niet als onderdeel van een rapportage die een breder deel van de activiteiten van de Opdrachtnemer betreft, zoals een (duurzaamheids)jaarverslag. Openbaarmaking kan worden bereikt door plaatsing op de website van de Opdrachtnemer. De rapportage aan de opdrachtgever bevat in ieder geval: • een geüpdatete risicoanalyse • een beschrijving van de maatregelen die (in het jaar waarover gerapporteerd wordt) zijn genomen om risico’s te verminderen en eventuele misstanden op het gebied van mensenrechten en milieu in de waardeketen te verhelpen (zoals beschreven onder stap 3); • een beschrijving van de resultaten van de genomen maatregelen. • informatie over hoe eventueel ontvangen signalen (intern en extern) over schending van de ISV afgehandeld zijn. De rapportage is vormvrij. • De rapportage is weliswaar vormvrij, maar moet voor de bruikbaarheid ervan in het Nederlands- of Engels opgesteld zijn.
UE.31	Opdrachtnemer dient rekening te houden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2 Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: • Opdrachtgever, www.Opdrachtgever.nl; • het Ministerie van Infrastructuur en Waterstaat, https://www.rijksoverheid.nl/ministeries/ministerie-van-infrastructuur-en-waterstaat; • het Ministerie van Sociale Zaken en Werkgelegenheid, www.rijksoverheid.nl/ministeries/szw.

5.6. Social return

Als onderdeel van het maatschappelijk verantwoord ondernemen heeft de Rijksoverheid beleidsdoelstellingen geformuleerd ten aanzien van social return. De Rijksoverheid kiest voor maatregelen die eraan bijdragen dat iedereen zoveel mogelijk participeert in de samenleving en om mensen perspectief te bieden op werk en inkomen. Voor wie dit niet op eigen kracht kan, heeft de overheid de taak ondersteuning te geven om tot de arbeidsmarkt toe te treden. Het toepassen van social return past hierin. Met de toepassing van social return zorgt de Rijksoverheid ervoor dat elke investering die binnen het Rijk wordt gedaan, naast het ‘gewone’ rendement, een concrete, sociale winst oplevert.

Social return heeft tot doel het creëren van extra (leer)werkplekken, bovenop de bestaande formatie. Het gehanteerde percentage is daarmee geen quotum, zodat mensen met een beperking die reeds werkzaam zijn bij de Inschrijver niet meetellen.

De gehele overheid (Rijk, provincies, waterschappen en gemeenten) doet de laatste jaren steeds meer ervaring op met het leveren van een bijdrage aan deze doelstelling. Door social return op te nemen in aanbestedingen binnen de

categorie ‘werken’ en ‘diensten’ met een loonsom hoger dan € 250.000,00 exclusief BTW, wil de Rijksoverheid een extra impuls geven aan social return.

Opdrachtnemer dient bij de uitvoering van de opdracht aan social return bij te dragen door het creëren van extra werk(ervarings)plaatsen voor mensen met een grote(re) afstand tot de arbeidsmarkt. Voor deze aanbesteding wordt uitgegaan dat minimaal 5% van het totale aantal in te zetten uren van de Overeenkomst wordt ingezet voor de doelgroep. De werkzaamheden dienen gerelateerd te zijn aan de opdracht.

Voorafgaand aan het sluiten van de Overeenkomst wordt afgestemd op welke wijze Opdrachtnemer invulling geeft aan social return en hoe de invulling geverifieerd kan worden door de Opdrachtgever.

UE.32	Na het tekenen van de Overeenkomst stemmen Partijen met elkaar af over de wijze waarop invulling wordt gegeven aan social return.
-------	---

5.7. Diversiteit en inclusie

Diversiteit gaat over de verscheidenheid aan mensen in een organisatie. Inclusie gaat over hoe diverse mensen tot hun recht komen en gewaardeerd worden. Samen zorgen zij voor een maatschappij met eerlijke kansen voor iedereen, het tegengaan van discriminatie en een representatieve overheid. Aspecten van dit thema zijn:

- Divers personeelsbestand in de (eigen) organisatie;
- Faciliteren van diverse werknemers;
- Representatieve beeldvorming;
- Sociale veiligheid;
- Toegankelijkheid.

Mogelijke prestatie-indicatoren zijn maatregelen die werknemerstevredenheid, de samenstelling of doorstroom van personeel bevorderen.

5.8. Duurzaamheidsbijdrage Inschrijver

W 2	Duurzaamheidsbijdrage Inschrijver wordt gevraagd zijn onderscheidend vermogen te laten zien in een verifieerbare uiteenzetting van zijn bijdrage aan de duurzaamheidsdoelstellingen van de Rijksoverheid bij de uitvoering van de Overeenkomst. Inschrijver dient in zijn uiteenzetting inzichtelijk te maken hoe hij aan de hand van gerealiseerde of binnenkort te realiseren acties rondom de bovengenoemde 6 thema's Opdrachtgever helpt in het bereiken van de gestelde doelen. Uitdrukkelijk wordt er op gewezen dat uw antwoord concreet toegespitst dient te zijn op deze Opdracht. Een algemeen antwoord dat Opdrachtgever zelf ook uit allerlei gepubliceerde informatie van Inschrijver kan samenstellen is niet afdoende. 1) Inschrijver dient uitgebreid in te gaan op het thema ISV gericht op de gehele keten die bij de Oplossing is betrokken, Van belang is met name de genoemde risicoanalyse van de risico's op schending van arbeids- en mensenrechten van de gehele keten.. Opdrachtgever wenst een uiteenzetting te ontvangen over de wijze waarop en mate waarin deze risicoanalyse invloed heeft gehad op uw keuze voor de Oplossing, welke mogelijke risico's u te dienaangaande voorziet en welke maatregelen u overweegt om deze te mitigeren Van de overige thema's per thema aan te geven: • In hoeverre het thema relevant is, op basis waarvan dat wordt geconcludeerd en de mate waarin het thema relevanter is ten opzichte van de overige thema's (uitgedrukt in een relatieve score qua relevantie/rangorde); • Welke concrete acties reeds zijn gerealiseerd; • Welke acties in gang zijn gezet en binnen 6 maanden zullen zijn gerealiseerd alsmede hoe hierop wordt gestuurd;
------------	--

- Welke overige acties worden voorgenomen en welke afhankelijkheden er zijn om deze te kunnen realiseren;
- Welke aantoonbare toegevoegde waarde op gebied van duurzaamheid de acties opleveren voor Opdrachtgever;
- In welke mate de acties (kunnen) resulteren in een hoger tarief voor Opdrachtgever.

Opdrachtgever laat zich graag positief verrassen door extra (niet genoemde) doelstellingen en thema's op het gebied van duurzaamheid die voor Opdrachtgever van toegevoegde waarde zijn.

Inschrijver wordt geadviseerd om bij de beantwoording gebruik te maken van de ambitieweb tool en -handleiding van PIANOo (<https://www.pianoo.nl/nl/handreiking-aan-de-slag-met-het-ambitieweb>)

2) Op welke wijze Opdrachtgever, zowel voor de gunning als bij de uitvoering van de overeenkomst, in staat is en wordt gesteld om de duurzaamheidsbijdrage van Inschrijver te verifiëren.

3) welke algemene (niet op deze Opdracht of op een bepaald thema betrekking hebbende) duurzaamheidsresultaten of -prestaties u kunt noemen die ter zake van toegevoegde waarde zijn. Denk bijvoorbeeld aan

- een milieumanagement tool dat Inschrijver in gebruik heeft zoals ISO 14001, EMAS of vergelijkbaar,
- doorgevoerde duurzaamheid in de eigen bedrijfsvoering bijvoorbeeld aan de hand van beoordelingsaspecten als:
 - Wat het huidige niveau is van de prestaties van de eigen bedrijfsvoering (waar mogelijk kwantitatief gemaakt a.d.h.v. CO₂-emissies)
 - De reeds behaalde resultaten in de afgelopen drie jaar t.a.v. het verbeteren van prestaties ondersteund met verifieerbare prestatie informatie;
 - De doelstellingen die de organisatie heeft m.b.t. de verduurzaming van de eigen bedrijfsvoering; Een Plan van aanpak waarin de doelstellingen worden onderbouwd, al dan niet met beleidsdocumenten.

Beoordeling

Zie in de beantwoording toe op volledigheid, onderbouwing (concreetheid), realiseerbaarheid en toegevoegde waarde. Deze wens wordt beoordeeld op basis van de mate waarin het antwoord toeziet op deze aspecten.

Aantal punten	Toelichting:
0	Het antwoord op de Wens ziet hier niet op toe
5	Het antwoord op de Wens ziet hier niet volledig op toe.
12	Het antwoord op de Wens ziet hier voldoende op toe.
20	Het antwoord op de Wens ziet hier volledig op toe en overstijgt ook de verwachtingen van de Aanbestedende dienst doordat er aanvullende, vernieuwende, originele of slimme voorstellen bevat, waar de beoordelaars positief door worden verrast.

De beantwoording is maximaal 6 A4 enkelzijdig, inclusief bijlagen en afbeeldingen.

Voor deze Wens kunt u maximaal **20 punten** verdienen.

Hoofdstuk 6. Juridische kaders

De in Bijlage 2 van het Beschrijvend Document opgenomen concept Overeenkomst kan - alvorens deze door Inschrijver(s) wordt ondertekend - door de Aanbestedende dienst worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de door de Inschrijver gedane opmerkingen en tekstsuggesties als bedoeld in paragraaf 3.2.1 (nadere inlichtingen of vragen over de aanbestedingsstukken). De wijzigingen en/of de aangepaste overeenkomst zullen/zal de Inschrijvers per nota van inlichtingen kenbaar worden gemaakt.

GUE 53.

Inschrijver gaat akkoord met de concept Overeenkomst (Bijlage 2) met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen zoals genoemd in deze paragraaf.

Hoofdstuk 7. Prijsstelling

7.1. Algemene eisen ten aanzien van Prijzen

In de in Bijlage VIII “Prijzenformulier” geoffreerde Prijzen dienen alle kosten voor de Oplossing verdisconteerd te zijn. Deze kosten kunnen door Opdrachtnemer niet verbijzonderd worden verrekend aan Opdrachtgever. Hierbij kan (en niet limitatief) worden gedacht aan:

- periodieke rapportages,
- periodiek overleg,
- inspecties,
- evaluaties,
- toekomstverkenningen,
- deelname aan begeleidings- en stuurgroepen,
- reis- en verblijfkosten voor externe bijeenkomsten,
- het verstrekken van de benodigde toegangscode voor gebruik van de Oplossing,
- Materialen en Documentatie vereist voor het gebruik van de Oplossing..
- (periodieke) kosten met betrekking tot security gerelateerde zaken

UE.33	Kosten die niet in de Inschrijving genoemd worden en niet verdisconteerd zijn in de Prijzen, maar toch noodzakelijk blijken te zijn voor een optimaal functioneren van de Prestatie conform de in de Aanbestedingsstukken gestelde eisen en de in de Inschrijving opgenomen beantwoording van de wensen, kan Opdrachtnemer niet in rekening brengen bij Opdrachtgever.
GUE 54.	Eventuele valutarisico's zijn volledig voor rekening van Inschrijver en worden geacht in de geoffreerde Prijzen te zijn verwerkt.
UE.34	Voor zover Opdrachtnemer gehouden is omzetbelasting in rekening te brengen, zullen de in het Prijzenformulier vermelde bedragen worden verhoogd met het geldende percentage omzetbelasting.

7.2. Toelichting Prijscomponenten in Bijlage VIII “Prijzenformulier”

De Aanbestedende dienst wenst een Inschrijver te contracteren die marktconforme Prijzen offreert ten aanzien van de Oplossing, Diensten en Additionele dienstverlening ten behoeve van de Aanbestedende dienst. In Bijlage VIII ‘Prijzenformulier’ is een aantal tabbladen opgenomen die door Inschrijver dienen te worden ingevuld.

Tabblad ‘Samenvatting’

Het betreft hier een samenvatting van de hieronder genoemde tabbladen. De Vergelijkingswaarde (deze is gebaseerd op netto contante waarde, NCW, en een contractduur van 10 jaar) betreft het totaal van de geoffreerde Prijzen. De Vergelijkingswaarde wordt gebruikt om de Inschrijvingen met elkaar te vergelijken en de ‘Economisch Meest Voordelige Inschrijving’ te bepalen. In dit tabblad dient Inschrijver enkel de naam van de Inschrijver in te vullen (cel D9).

Tabblad ‘o. Dimensionering’

Dit tabblad geeft een overzicht van de te verwachte dimensionering. Hierin hoeft de Inschrijver niets in te vullen. Deze dimensionering is een indicatie en hier kunnen geen rechten aan ontleend worden.

Tabblad ‘1. Migratie VM’s’

Dit tabblad geeft een overzicht van de migratie van het aantal VM's (zie hiervoor ook Bijlage VI - Migratie). In dit tabblad vult inschrijver in de gele cel zijn eenmalige kosten (all-in prijs) op voor de Migratie van de VM's.

Tabblad '2. Managed Service'

In dit tabblad wordt de Vergoeding voor de Managed Service geoffreerd, hierin vult de Inschrijver de geel gearceerde velden in. De Vergoeding voor de Managed Service bestaat uit een Vaste Vergoeding per jaar voor de ICT Infrastructuur en een flexibele Vergoeding per jaar voor de VM's.

Vaste Vergoeding

De Vaste Vergoeding per jaar omvat kosten voor de ICT-infrastructuur ten minste bestaande uit Apparatuur en Programmatuur en alle noodzakelijke activiteiten voor het implementeren, inrichten en het Beheren en Onderhouden van de ICT-infrastructuur.

De Apparatuur binnen de ICT-infrastructuur heeft een minimale levensduur van 5 jaar conform UE 1 en zal derhalve in het 5e contractjaar door Opdrachtnemer worden vervangen door Fabrieksnieuwe Apparatuur. De kosten hiervoor worden over de jaren 6 tot en met 10 verrekend als onderdeel van de jaarlijkse Vaste Vergoeding. Deze kosten worden bepaald op basis van de op dat moment geldende Listprijs, verminderd met hetzelfde kortingspercentage als toegepast op de aanschaf van Apparatuur (cel H61).

Voor Beheer en Onderhoud wordt dezelfde procentuele opslag (cel K61) gehanteerd. De Vaste Vergoeding voor de jaren 6 tot en met 10 wordt als volgt berekend: Vaste Vergoeding jaar 5 (cel H5 plus eventuele indexering conform UE 40) minus $1/5 \times$ Aanschaf Apparatuur (cel I87), minus Beheer en Onderhoud Apparatuur (cel L87) plus $1/5$ deel van de Aanschaf van de vervangende Apparatuur (o.b.v. de dan geldende Listprijzen minus de korting (cel H61), plus Beheer en Onderhoud (o.b.v. procentuele opslag op Apparatuur (cel K61). Voor de jaren 11 tot en met 15 geldt hetzelfde uitgangspunt. Inschrijver dient de in dit tabblad opgenomen Kit-list van de Apparatuur volledig in te vullen.

Flexibele Vergoeding

De flexibele Vergoeding per jaar omvat de kosten voor alle activiteiten nodig voor het implementeren en het Beheren en Onderhouden van de VM's en is gebaseerd op het aantal VM's. Hiervoor dient Inschrijver een staffel in te vullen in de geel gearceerde velden. In kolom E kunt u steeds de drempelwaarde van een staffel opnemen, met in kolom H de bijbehorende korting op de Vergoeding per VM (cel D35). Biedt u geen korting dan kunt u in de eerste staffelregel het ">"-teken invullen. De hoogste staffeltrede staat steeds automatisch ingevuld, behalve de bijbehorende korting.

In het tabblad dient Inschrijver alleen de geel gearceerde velden in te vullen.

Tabblad '3. Additionele diensten'

Hier dient Inschrijver de Prijs voor de Additionele diensten, te weten Consultancy, te offrenen, bestaande uit: algemene ondersteuning, bijdrage aan disaster recovery test, deployment SAP, optimalisatie gebruik Infrastructuur, ontwikkelen nieuwe koppelingen, opleidingen, on site support.

De te verwachte uren zullen gedurende de 10 jaar 1.500 uur bedragen. Deze uren zullen gedurende de contractjaren minder worden, waarin het eerste jaar de meeste uren gebruikt zullen worden.

GUE 55.	Inschrijver gaat akkoord met het gestelde in paragraaf 7.2 met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen.
---------	--

7.3. Specifieke eisen ten aanzien van Prijzen

UE.35	De door Inschrijver geoffreerde (minimale) Kortingspercentages zijn op basis van de Listprijs en blijven gedurende de Overeenkomst van kracht.
UE.36	De Vergoeding voor Beheer en Onderhoud biedt het recht om altijd gebruik te maken van de nieuwste versies van de geleverde Programmatuur zonder dat sprake is van een additionele licentievergoeding.
UE.37	Consultancy die op verzoek van Opdrachtgever wordt geleverd gedurende de Operationele fase van de Overeenkomst wordt verrekend op basis van nacalculatie conform de Prijzen ‘Consultancy’, tabblad ‘3. Additionele diensten’ Bijlage VIII ‘Prijzenformulier’.
UE.38	De aangeboden Prijzen (uurtarieven) voor Consultancy zijn inclusief reis- en verblijfskosten.
UE.39	De kosten voor de Oplossing, zijn pas verschuldigd na Acceptatie van de afgesproken mijlpalenplanning (zie afbeelding 2 mijlpalenplanning) en facturatiemomenten.

7.4. Indexering Prijs

De door Inschrijver geoffreerde Prijzen : de Managed Service en Additionele dienstverlening, zoals opgegeven in Bijlage VIII “Prijzenformulier” mogen vanaf 2027 jaarlijks en steeds per 1 januari worden geïndexeerd op basis van de CBS-tabel ‘Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2021 = 100’, (CPA2008, kwartaalindex) conform de volgende webpagina:

<https://opendata.cbs.nl/#/CBS/nl/dataset/85817NED/table?dl=AE1CF>

Prijsaanpassingen dienen uiterlijk voor 1 november van enig jaar aan de contractmanager ter goedkeuring te worden aangeboden, waarbij het op dat moment – door het CBS – meest recent beschikbare en gepresenteerde indexcijfer, Jaarmutatie per kwartaal, gehanteerd wordt. Het percentage voor de tariefstijging wordt afgerond op één decimaal achter de komma. Inhaalslagen op niet doorgevoerde indexeringen worden niet geaccepteerd.

Voorbeeld: als de overeenkomst op 1 januari 2024 geïndexeerd had mogen worden, was de prijsindexatie 4,5% geweest (jaarmutatie DPI 3e kwartaal 2023, meest recent beschikbare indexcijfer).

UE.40	De door de Opdrachtnemer geoffreerde Prijzen met betrekking tot de Managed Service en Additionele dienstverlening mogen jaarlijks per 1 januari geïndexeerd worden conform paragraaf 7.4. De eerste indexering vindt plaats niet eerder dan vanaf 1 januari 2027 jaarlijks
-------	--

UE.41	Opdrachtnemer dient voor 1 november, voorafgaande aan de genoemde momenten van indexering, een schriftelijk verzoek in met bijbehorende onderbouwing om voor de indexering in aanmerking te komen.
-------	--

Afrekenmomenten

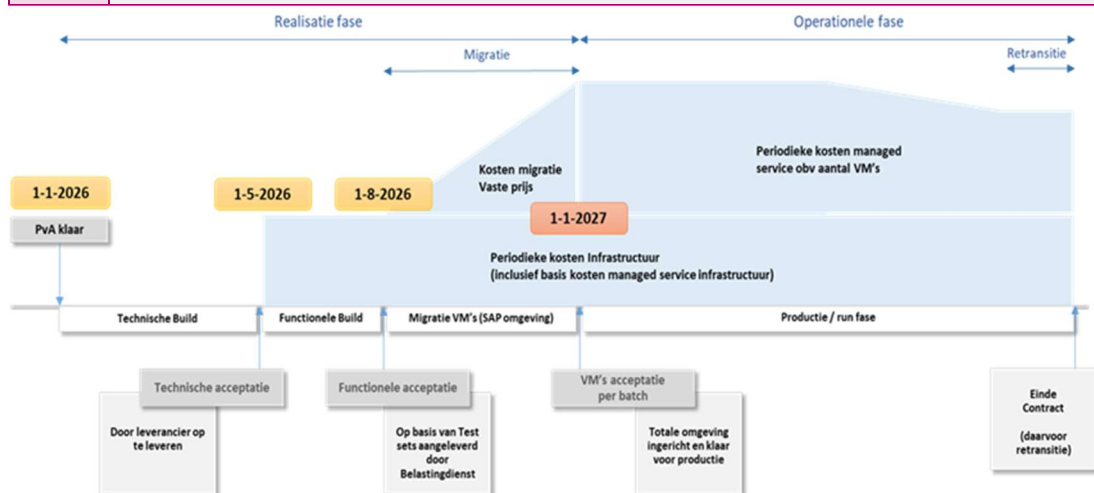
Er zijn 2 afrekenmomenten die zich samenvoegen in de Operationele fase en leiden tot een totaal maandelijks facturatie van de Managed Service.

De start van het eerste afrekenmoment is na technische Acceptatie van de technische build. De maandelijks (ook wel periodieke) kosten van de volledige Infrastructuur kunnen dan in rekeneing gebracht worden (zie ook paragraaf 10.1).

De start van het tweede afrekenmoment is na Acceptatie van de Migratie. Nu kunnen ook de maandelijks (periodeke) kosten van de VM's in rekening gebracht worden.

Na acceptatie gaat de Realisatie fase over naar de Operationele fase en is daarmee de Oplossing operationeel en conform SLA (zie Hoofdstuk 10 Operationele fase).

UE.42	De Opdrachtnemer heeft een resultaatverplichting voor het Productiewaardig opleveren van de Oplossing conform de mijlpalenplanning vanuit het gezamenlijk afgestemde Plan van Aanpak. Het in Gebruik nemen van de Oplossing vindt plaats na Acceptatie van de Oplossing door de Opdrachtgever (zie afbeelding 2: mijlpalenplanning).
-------	--



Afbeelding 2: Mijlpalenplanning

Hoofdstuk 8. Documentatie

8.1. Documentatie

UE.43	Opdrachtnemer zal Opdrachtgever tijdig voorzien van actuele en volledige Documentatie in elektronische vorm, ten behoeve van de Realisatie van de Oplossing en het gebruik van de Oplossing in de Operationele fase. Hierbij is de Documentatie over de eigenschappen en gebruiksmogelijkheden van de Oplossing in de Nederlandse en/of Engelse taal.
UE.44	De Documentatie dient zodanig te zijn dat zij een juiste, volledige en gedetailleerde beschrijving geeft van de door Opdrachtnemer te leveren Oplossing en de functies daarvan, zodat Functionele Beheerders op eenvoudige wijze van alle mogelijkheden van de Oplossing gebruik kunnen maken.
UE.45	De Documentatie dient in een bewerkbaar format aangeleverd te worden, zodat Opdrachtgever deze zelf kan aanpassen wanneer Opdrachtgever in de toekomst zaken wijzigt in de configuratie van de Oplossing.
UE.46	Opdrachtgever mag de Documentatie voor gebruik binnen de eigen organisatie reproduceren en wijzigen.
UE.47	Opdrachtnemer zal de door hem geleverde Documentatie zo spoedig mogelijk vervangen, wijzigen of aanpassen indien op enig tijdstip tijdens het gebruik door Opdrachtgever van de Prestatie, blijkt dat de Documentatie onjuiste informatie bevat of anderszins onvolledig, onvoldoende, onduidelijk en/of verouderd is.
UE.48	Opdrachtnemer is verantwoordelijk dat Documentatie na een nieuwe Release actueel blijft. Na oplevering van een nieuwe Release wordt de geactualiseerde Documentatie digitaal beschikbaar gesteld.
UE.49	Opdrachtnemer geeft in de Documentatie de in de Release opgenomen aanpassingen duidelijk weer.

Hoofdstuk 9. Voorbereiding- en Realisatiefase

9.1. Voorbereiding

Er zijn 2 hoofdfasen: Realisatie fase en Operationele fase. Tijdens de Realisatie fase wordt de infrastructuur (die ten grondslag ligt aan de Managed Service) en Managed Service opgebouwd en ingericht. Laatste deel van de Realisatie fase is de Migratie waarin de bestaande omgeving wordt overgezet naar de nieuwe Oplossing. De richtlijnen voor de migratie zoals de Opdrachtgever dit ziet is beschreven in Bijlage VI- Migratie. Tijdens de Realisatie fase zijn een aantal acceptatie momenten, deze zijn opgenomen in Bijlage XVII - Acceptatie.

De Opdrachtnemer dient de leiding te nemen bij de Realisatie van de Oplossing. Opdrachtnemer is verantwoordelijk voor de Realisatie fase voor wat betreft de technische build en de migratie (zie hiervoor afbeelding 2 mijlpalenplanning). Om inzicht te krijgen op welke wijze de Opdrachtnemer de Realisatie uit gaat voeren, dient de Opdrachtnemer een Plan van Aanpak van de Oplossing aan te leveren (zie Wens 3) die op 1-1-2026 definitief wordt opgeleverd.

De afbeelding (afbeelding 2) met betrekking tot mijlpalenplanning geeft aan in hoeverre de in Bijlage XVII - Acceptatie uitgewerkte Realisatie fase en Operationele fase in mijlpalen, planning, en acceptatiecriteria in de tijd worden weggezet.

Technische Build

Bovenstaande afbeelding met betrekking tot mijlpalenplanning geeft ook een aantal tussen fase weer te weten de technische build en de functionele build. Tijdens de technische build wordt de volledige Infrastructuur door Opdrachtnemer opgebouwd. Daar zal door de Opdrachtnemer een technische Acceptatie op plaatsvinden conform een door de Opdrachtnemer opgezette Acceptatie. In het Plan van Aanpak verwacht Opdrachtgever een beschrijving van de technische build en de technische Acceptatie. De opzet en het resultaat van de technische Acceptatie wordt door Opdrachtgever beoordeeld. Na de technische Acceptatie kan Opdrachtnemer de maandelijkse kosten van de Managed Service infrastructuur factureren.

Functionele Build

Na de technische build zal een functionele build plaatsvinden waarin een deel van de nieuwe SAP-omgeving tijdelijk wordt opgebouwd en getest. Deze fase wordt afgesloten met een functionele Acceptatie op basis van test sets aangeleverd door de Opdrachtgever. De functionele Acceptatie wordt door Opdrachtgever uitgevoerd met ondersteuning van Opdrachtnemer (bijvoorbeeld testen van de backups). Het resultaat moet zijn dat de totale Infrastructuur klaar is voor de Migratie van de gehele SAP-omgeving.

Migratie

Na de functionele build volgt een migratie van alle VM's naar de nieuwe omgeving. Opdrachtnemer is verantwoordelijk voor het uitvoeren van de Migratie. Opdrachtnemer zet de VM's over en gaat het beheer uitvoeren op de overgezette VM's. Een beschrijving van de Migratie is opgenomen in Bijlage VI- Migratie. VM's worden per domein in batches gemigreerd en geaccepteerd. Opdrachtgever zal de gemigreerde batches testen en accepteren (Opdrachtgever maakt hiervoor het acceptatie plan dat minimaal gebaseerd is op Bijlage VI- Migratie en Bijlage XVII - Acceptatie), zie hiervoor ook Wens 3.

9.1.1. Plan van Aanpak Oplossing

GUE 56.	Inschrijver levert bij Inschrijving een (concept) Plan van aanpak op, uitgaande van gebruiksklare oplevering van Oplossing, per datum 1-1-2027. In het concept Plan van aanpak komen tenminste de volgende onderwerpen aan bod: • Beschrijving aanpak; • Projectmanagement methodiek; • Governance; • Planning; • Mijlpalen (Fatale termijnen) / Go or no Go momenten (mijlpalenplanning); • Documentatie; • Test plan.
---------	---

GUE 57. Inschrijver levert bij Inschrijving een Plan van Aanpak voor de Technische build en de Migratie.

W 3	Plan van Aanpak Middels deze Wens wil de Opdrachtgever inzicht krijgen het Plan van Aanpak van Inschrijver welke, indien u de opdracht gegund krijgt, de basis zal vormen voor de realisatie fase van de Oplossing. Opdrachtnemer is verantwoordelijk voor de realisatie fase voor wat betreft de technische build en de migratie. Vraag: Beschrijf uw Plan van Aanpak voor de technische build en de migratie van de Oplossing. Gebruik daarbij het overzicht en de planning van het figuur paragraaf 10.1 afbeelding 2 mijlpalenplanning. De datum voor het in gebruik nemen van de Oplossing is 1-1-2027. Beschrijf in uw Plan van Aanpak het volgende: • Projectmanagementmethode, projectaanpak en projectplanning. • Projectorganisatie en governance inclusief escalatieprocedure en interactie met Opdrachtgever (welke verantwoordelijken worden wanneer betrokken en geïnformeerd). • Beschrijving van de beheersmaatregelen van risico's om de start van de Operationele fase te borgen. • De randvoorwaarden waar de Opdrachtgever aan moet voldoen om de start van de Operationele fase te borgen. • De aanpak voor het instrueren, begeleiden en ondersteunen van de verschillende Gebruikers. • Beschrijving van de technische build. • Acceptatie aanpak; ○ Opdrachtnemer maakt de aanpak voor de technische acceptatie. Na goedkeuring door Opdrachtgever wordt deze uitgevoerd. Uitgangspunt is dat de complete infrastructuur is ingericht. • De migratie is (op hoofdlijnen en naar inzichten van de Opdrachtgever) beschreven in Bijlage VI- Migratie Beschrijf de in het Plan van Aanpak de detail migratiestappen en bij wie de verantwoordelijkheid en uitvoering ligt van de onderdelen (Opdrachtnemer, oude leverancier of Opdrachtgever). Verwachting De Opdrachtgever verwacht van het antwoord van de Inschrijver dat: • De beantwoording volledig is en ingaat op alle hierboven genoemde aspecten. • De verantwoordelijkheden van Partijen op heldere wijze terugkomen in het Plan van Aanpak • Het beschreven Plan van Aanpak biedt zekerheid dat de operationele fase voor de Oplossing kan worden gestart en aan alle Specificaties wordt voldaan. • Wordt beschreven op welke wijze Opdrachtgever door Opdrachtnemer ontzorgt wordt. • Het antwoord inhoudelijk overtuigend, relevant, samenhangend en logisch van opbouw is. Beoordeling: Deze wens wordt beoordeeld op basis van de mate waarin het antwoord voldoet aan de verwachtingen van de Aanbestedende dienst. Het maximale aantal punten dat behaald kan worden voor deze wens is 80 punten. <table border="1"> <tr> <th>Aantal punten</th><th>Toelichting:</th></tr> <tr> <td>0</td><td>Het antwoord op de wens voldoet niet aan de verwachtingen.</td></tr> </table>	Aantal punten	Toelichting:	0	Het antwoord op de wens voldoet niet aan de verwachtingen.
Aantal punten	Toelichting:				
0	Het antwoord op de wens voldoet niet aan de verwachtingen.				

	20	Het antwoord op de wens voldoet niet volledig aan de verwachtingen.
	48	Het antwoord op de wens voldoet aan de verwachtingen.
	80	Het antwoord op de wens overstijgt de verwachtingen van de Aanbestedende dienst doordat het Plan van Aanpak (bovenop de omschreven verwachtingen) aanvullende, vernieuwende, originele of slimme voorstellen bevat, waar de beoordelaars positief door worden verrast.
Voorschriften uitwerking Wij vragen uw uitwerking in maximaal 10 pagina's A4 (lettertype Arial, lettergrootte 10 en regelafstand 1,0) te verwoorden. Extra pagina's en/of hyperlinks worden niet in de beoordeling meegenomen.		

GUE 58.	Inschrijver conformeert zich aan de data in afbeelding 2 mijlpalenplanning.
GUE 59.	Het door Inschrijver in te dienen Plan van Aanpak, vormt de basis voor de uitvoering van de Realisatie fase en de wijze waarop de Oplossing wordt gerealiseerd. Het Plan van Aanpak zal binnen 6 weken na het tekenen van de Overeenkomst tussen Inschrijver en de Opdrachtgever worden besproken en door Partijen gezamenlijk worden vastgesteld. Pas nadat er akkoord is tussen Partijen over het Plan van Aanpak zal worden gestart met het uitvoeren van de Realisatie fase.
UE.50	Opdrachtnemer Migreert in samenwerking met de huidige opdrachtnemer en de Opdrachtgever de door de Opdrachtgever aangegeven VM's naar de nieuwe Oplossing zoals beschreven Bijlage VI - Migratie . De VM's worden per domein (zie Bijlage V – SAP Landschap) gemigreerd. Dit komt overeen met alle VM's van een domein. Aangezien e.e.a. met downtime voor de SAP applicaties gepaard gaat dient dit in overleg plaats te vinden.
UE.51	Na ondertekening van de Overeenkomst zal Opdrachtnemer in goed overleg daartoe binnen 30 Werkdagen een planning opstellen en na afstemming met Opdrachtgever uiterlijk op 1-1-2026 een definitief Plan van aanpak opleveren. De vervolgbepalingen in de Overeenkomst gelden hierbij onverkort.
UE.52	Het door Opdrachtnemer definitief opgeleverde Plan van aanpak dient eerst door Opdrachtgever zoals omschreven in de Overeenkomst te zijn goedgekeurd. Pas na schriftelijke goedkeuring kan worden aangevangen met de Realisatie van de Oplossing.

9.2. Implementatie

UE.53	De Oplossing dient uiterlijk op 1-3-2027 gebruiksklaar en geaccepteerd te zijn door Opdrachtgever.
UE.54	Opdrachtnemer is gedurende de Realisatiefase bereid tot overleg en samenwerking met andere partijen van overige systemen.

9.3. Documentatie

UE.55	Opdrachtnemer levert gedurende de voorbereidings- en Realisatiefase van de Overeenkomst Documentatie conform de eisen zoals neergelegd in Hoofdstuk 8 'Documentatie.
-------	--

Hoofdstuk 10. Operationele fase

Na acceptatie van de Migratie fase gaat de Realisatie fase over naar de Operationele fase en is daarmee de Oplossing operationeel en conform SLA. Dit alles is gepland op uiterlijk 1 januari 2027.

Aan het eind van de Operationele fase kan een Retransitie (paragraaf 10.4) plaatsvinden waarbij de Oplossing moet worden overgezet naar een nieuwe oplossing.

Tijdens de Operationele fase is er na de initiële contractduur van 5 jaar, 2 keer de mogelijkheid om de overeenkomst met 5 jaar te verlengen. Bij een verlenging zal de economische levensduur van de hardware zijn bereikt en wordt alle hardware vervangen door fabrieksnieuwe exemplaren. Partijen zullen bij verlenging, in overleg treden om te bepalen welke nieuwe sizing, onderdelen en inzichten worden gebruikt.

UE.56	De communicatie gedurende de contractperiode dient volledig in de Nederlandse taal te geschieden.
-------	---

10.1. Onderhoud en Support

De Managed Service is inclusief het leveren van Onderhoud en Support ten behoeve van Oplossing. Dit betekent onder andere dat Opdrachtnemer zowel tweede als derde lijns Onderhoud en Support levert bij Incidenten. Hier wordt een Dossier Afspraken en Procedures (DAP) en Service Level Agreement (SLA) voor afgesloten.

Binnen de DAP worden afspraken gemaakt hoe de Opdrachtnemer en de Opdrachtgever samenwerken. Binnen de SLA worden afspraken gemaakt aangaande het te leveren Onderhoud en Support. Ook bevat de SLA een beschrijving van de vastgestelde normen in de vorm van Service Levels.

Op basis van de SLA wordt maandelijks gerapporteerd door Opdrachtnemer. Dit gebeurt via een Service Niveau Rapportage (SNR).

Activiteiten die om redenen niet binnen de termijn kunnen worden opgelost worden opgenomen in een Verbeterplan.

UE.57	Opdrachtnemer levert een SLA aan welke binnen 8 weken na het tekenen van de Overeenkomst tussen Opdrachtnemer en Opdrachtgever zal worden besproken en vastgesteld. De SLA dient gebaseerd te zijn op de uitgangspunten zoals genoemd in dit document. Opdrachtgever heeft het recht om de vastgestelde SLA vast te leggen met een door Opdrachtgever bepaald template (zie voorbeeld Bijlage XVIII). Na vaststelling van de versie 1.0 zal deze periodiek worden onderhouden als er wijzigingen in de SLA optreden. De versienummering geeft aan welke SLA de laatste versie is. De SLA zal na ondertekening door Partijen als bijlage A aan de Overeenkomst worden toegevoegd
-------	--

UE.58	Naast de SLA is de Opdrachtgever voornemens een Dossier Afspraken en Procedures (DAP) op te stellen samen met Opdrachtnemer. Op verzoek van Opdrachtgever zal Opdrachtnemer meewerken aan het opstellen van de DAP. Opdrachtgever heeft het recht om de vastgestelde DAP vast te leggen met een door Opdrachtgever bepaald template (zie voorbeeld Bijlage XIV). Na vaststelling van de versie 1.0 zal deze periodiek door de Opdrachtgever worden onderhouden. De versienummering geeft aan welke DAP de laatste versie is. De SLA zal na ondertekening door Partijen als bijlage B aan de Overeenkomst worden toegevoegd
-------	--

UE.59	Opdrachtnemer rapporteert in de maandelijkse SNR het volgende: • KPI opgeloste beveiligingsincidenten/-problems. • Status, voortgang en afhandeling van openstaande en opgeloste vragen, beveiligingsincidenten, -problems en -verbetervoorstellen. Hierbij wordt aangegeven: datum ontvangst, datum in behandeling, verwachte opleverdatum en datum afgevoerd. • Cumulatieve rapportage (minimaal 14 maanden) over bovenstaande voor trend-analyse. Er wordt tenminste jaarlijks, of voor zover van toepassing, inzage gegeven in de datum en het resultaat van: • Wijziging van de Statement of Applicability en/of ISO27001-certificering (of gelijkwaardig).
-------	--

UE.60	Opdrachtnemer verplicht zich om ten minste Onderhoud te verlenen op de voorlaatste (verse n-1) en nieuwste versie (versie n) van de Oplossing
-------	---

In de Operationele fase worden onderstaande standaard activiteiten (Zie tabel: Standaard activiteiten) uitgevoerd binnen het Beheer en Onderhoud en binnen de gestelde normen zoals opgenomen in onderstaande tabel.

Activiteit	Responsetijd	Realisatietijd	Indicatie Aantal / jaar	Benodigde inspanning Opdrachtgever
Aanmaken nieuwe Host volgens specificaties.	1 Werkdag	1 Werkdag	20	Geen
Afvoeren Host	1 Werkdag	1 Werkdag	20	Geen
Aanpassen resources van een bestaande Host.	1 Werkdag	1 Werkdag	20	Geen
Restoren OS van een SAP Host	1 Werkdag	1 Werkdag	4	Afstemming/uitvoering met Opdrachtnemer
Configuratie van verkeersstromen	1 Werkdag	3 Werkdagen	10	Afstemming/uitvoering met Opdrachtnemer
Op-/afvoeren beheerders	1 Werkdag	2 Werkdagen	10	Geen
Ondersteuning performance onderzoeken	1 Werkdag	In overleg	12	Afstemming/uitvoering met Opdrachtnemer
Ondersteuning bij incident analyse	1 Werkdag	In overleg	25	Afstemming/uitvoering met Opdrachtnemer

Tabel: Standaard activiteiten

UE.61	Ten aanzien van de standaard activiteiten die minimaal in de vaste Prijs voor Onderhoud en Beheer zijn inbegrepen wordt ten minste voldaan aan de minimale Service Levels zoals opgenomen in de tabel Standaard Activiteiten
-------	--

10.1.1. Service Levels

10.1.1.1. Kwetsbaarheden

Kwetsbaarheden kunnen onder andere ontdekt worden naar aanleiding van cyberhack, responsible disclosure, beveiligingstesten, berichten in de media, meldingen van leveranciers en op basis van informatie uit de CVE database.

UE.62	Bij het constateren van Kwetsbaarheden met een niveau van kritisch (critical) of hoog (high), conform CVSS 4.0, wordt de Opdrachtgever daarover binnen één (1) uur door Opdrachtnemer geïnformeerd.
-------	---

UE.63	Kwetsbaarheden die leiden tot een Incident worden gekwalificeerd door middel van CVSS 4.0. Op basis van de CVSS 4.1 kwalificaties gelden de volgende Oplostijden voor Opdrachtnemer: • Kritisch (critical): per direct (binnen vier (4) uren) op te lossen. • Hoog (high): binnen één (1) maand. • Gemiddeld (medium): binnen drie (3) maanden. • Laag (low): binnen zes (6) maanden.
-------	---

10.1.1.2. Beschikbaarheid

De Beschikbaarheid is volledig wanneer er geen degradatie van het gebruik bestaat voor de Opdrachtgever. De Oplossing heeft dan de 'Productie status'.

Voorbeelden:

- Een kortstondige onderbreking van de Monitoring functie van de Opdrachtnemer hoeft niet te leiden tot verminderde Beschikbaarheid.
- Een Incident (betreft prio 1 en prio 2) is opgelost als de Productie status weer is bereikt.

PI	Service Level
Beschikbaarheid 7x24x365	99,9%

UE.64	De Oplossing voldoet minimaal aan een Beschikbaarheid van 99,9% per maand tijdens openstelling. Geplande, in overleg besloten, downtime in verband met Onderhoud en Support wordt niet meegeteld bij het vaststellen van de Beschikbaarheid. Geplande downtime in verband met Onderhoud en Support mag enkel plaatsvinden in weekenden en met goedkeuring van de Opdrachtgever (dit geldt alleen voor de productie- en beheersystemen van de opdrachtgever). De tijdsduur per geplande downtime is maximaal 3 uur aaneengesloten. Indien meer dan 3 uur nodig is dan mag dat na overleg en na akkoord van Opdrachtgever. Een Calamiteit telt niet mee in de vaststelling van de Beschikbaarheid.
-------	---

UE.65	Het maximum aantal Prio 1 Incidenten (met uitzondering van security Incidenten) is 3 per jaar. Indien dit getal per jaar hoger is dan 3, start een verbeterd traject. Dat wordt vastgelegd in het Verbeterplan.
-------	---

10.1.1.3. Helpdesk en Incidentmanagement

Incidenten kunnen met drie verschillende prioriteiten aangemeld worden. Aan elk Incident, ongeacht de vermoedelijke oorzaak van een Incident, wordt een prioriteit toegekend op basis van Impact en Urgentie inclusief Afhandelingstijd. Naast de door de Opdrachtgever gemelde Incidenten aan de Helpdesk van de Opdrachtnemer worden tevens de meldingen die middels het automatisch uitbellen/signaleren van de Oplossing bij de Opdrachtnemer beschouwd als daadwerkelijke Incidenten.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor • één of meer bedrijfsprocessen die de burger en/of het bedrijf direct raken, en/of • één of meer fabriekstaken voor (massale) Gegevensverwerking en/of

	- de Informatiebeveiliging en/of - het imago van de Opdrachtgever en/of - onacceptabele hoge kosten.
Laag	Overige situaties
Urgentie	
Hoog	Een Incident - beïnvloedt kwaliteit van functies/Beschikbaarheid/beveiliging en/of - brengt integriteit van de Gegevens in het geding en/of - treedt op tijdens piektijd/-periode van het bedrijfsproces en/of - brengt uiterste verzenddatum van klantbescheiden in gevaar en/of - verstoot de communicatie met de klanten van de Opdrachtgever en/of - er geen Workaround mogelijk is en/of - de verwerking kan niet worden uitgesteld en/of - de schade is al een feit of zal dat zijn binnen 24 uur.
Laag	Overige situaties
Prioriteit	- Impact Hoog / Urgentie Hoog geeft Prio 1 - Impact Hoog / Urgentie Laag geeft Prio 2 - Impact Laag / Urgentie Hoog geeft Prio 2 - Impact Laag / Urgentie Laag geeft Prio 3

Tabel Impact, Urgentie en Prioriteit

PI	Prioriteit	Service Level	Norm
Openstelling Helpdesk	Stand-by Openingstijd service desk voor melden Prio 1 Incidenten	7 x 24 uur	100%
	Reguliere Openingstijd service desk	Werkdagen van 08:00 – 18:00 uur	100%
Service Window	Stand-by service uren waarin voor Prio 1 verstoringen ondersteuning wordt geleverd	7x24 uur	100%
	Reguliere service uren waarin ondersteuning wordt geleverd	Op Werkdagen: 8:00 – 18:00 Nederlandse tijd	100%
Stand-by	Extra (stand-by) openstelling service desk en/of ondersteuning t.b.v. speciale situaties (b.v. Realisaties).	Wordt aangevraagd uiterlijk 5 Werkdagen voor aanvang. (Optionele offerte).	
Openstelling	Tijdvak waarbinnen de Oplossing beschikbaar is voor gebruik	7x24 uur 365 dagen per jaar	99,9%
Monitoring en alerting	Opdrachtnemer heeft een Monitoring en alerting proces ingericht om direct (binnen 2 Klokuren, conform Reactietijd Prio1) te kunnen handelen in geval van Incidenten en (dreigende) verstoring van de Beschikbaarheid van de Oplossing	7x24 uur 365 dagen per jaar	100%
REACTIETIJD			
Reactietijd	Prio 1*	15 minuten	90%
Reactietijd	Prio 2	1 uur (werkuur)	90%

Reactietijd	Prio 3	2 uur (werkuur)	90%
Reactietijd	Service request	1 Werkdag	90%
*Bij Prio 1 Incidenten heeft Opdrachtnemer een tussentijdse informatieverplichting. De aanmelder van het Incident dient elke uur geïnformeerd te worden over de status van het Incident en de voortgang van het oplossen.			
OPLOSTIJD			
Oplostijd	Prio 1	4 klokuur	95%
Oplostijd	Prio 2	1 Werkdag 24 klokuren	95%
Oplostijd	Prio 3	3 Werkdagen 72 klokuren	85%
Hierbij geldt in alle gevallen een RPO van ~o (Klok)uren			
HERSTELTIJD			
Hersteltijd	Prio 1	2 Werkdagen	98%
Hersteltijd	Prio 2	5 Werkdagen	95%
Hersteltijd	Prio 3	10 werkdagen	90%

Tabel Service Levels Helpdesks en Incidentmanagement

UE.66	Ten aanzien van de Openstelling van de Helpdesk wordt ten minste voldaan aan de Service Levels zoals onder andere opgenomen in de tabel Service Levels Helpdesk en Incidentmanagement.
UE.67	Ten aanzien van de afhandeling van Incidenten en Service requests wordt ten minste voldaan aan de Service Levels zoals onder andere opgenomen in de tabel Service Levels Helpdesk en Incidentmanagement.
UE.68	Bij Prio 1 Incidenten heeft Opdrachtnemer een tussentijdse informatieverplichting. De aanmelder van het Incident dient elke 60 minuten (op Werkdagen binnen Kantoortijden) geïnformeerd te worden over de status van het Incident en de voortgang van het oplossen.
UE.69	Indien een Incident niet binnen de Oplostijd wordt opgeslost, wordt het Incident geëscaleerd naar de bovenliggende Prioriteit (Prio 3 wordt Prio 2 en Prio 2 wordt Prio 1).
UE.70	Opdrachtnemer zorgt er voor dat de Opdrachtgever op elk willekeurig moment (buiten het tijdstip dat de Oplossing in gepland Onderhoud is) online een actueel overzicht van de incidentadministratie kan raadplegen. In de incidentadministratie wordt minimaal aangegeven: • Datum Ontvangst • Datum in behandeling • Verwachte opleverdatum • Datum afgevoerd

In samenwerking met de Opdrachtnemer zal, nadat de Oplossing in Productie is, gedurende een representatieve situatie, de baseline worden vastgesteld op basis van metingen van in samenspraak afgestemde grootheden (bijvoorbeeld CPU Utilization of Memory Utilization). Deze baseline geldt als de referentie en wordt opgenomen in de SLA. Naast de vaststelling van de grootheden en de baseline worden in samenspraak normen vastgesteld per grootheid (de 'thresholds') die bij overschrijding leiden tot actie.

UE.71	Van de Opdrachtnemer wordt geëist: • Dat hij meewerkt aan het gezamenlijk vaststellen van een baseline; • Een set van representatieve grootheden te geven voor capacity management. • Dat de grootheden continu worden gemonitord. • Dat bij de Monitoring van de uitnutting van de capaciteit pro-actief wordt geacteerd bij het overschrijden van de vastgestelde thresholds.
-------	--

De Opdrachtgever gebruikt voor de ondersteuning van haar eigen service management processen een service management applicatie; op dit moment Service Now. Ten behoeve van de routing van Incidenten en problems dient deze applicatie gekoppeld te kunnen worden aan de service management applicatie van de Opdrachtnemer.

GUE 60.	Ten behoeve van security Monitoring door de Opdrachtgever en ten behoeve van Audit Logging moet de aangeboden Oplossing via open standaarden, op niet compromiteerbare wijze, Gegevens kunnen aanleveren aan de Splunk realisatie bij de Opdrachtgever conform Bijlage 6 – Splunk.
---------	--

De Opdrachtgever heeft zicht in afwijkende/verdachte activiteiten binnen de Oplossing om herstelacties te kunnen formuleren en zo mogelijk in de toekomst te voorkomen. Denk aan (ongeautoriseerde) toegang tot de Oplossing, maar ook inzage, wijziging of verwijdering van Gegevens. Speciale aandacht voor gevoelige Gegevens, zoals PersoonsGegevens. Ook, bijvoorbeeld, financiële Gegevens kunnen extra aandacht nodig hebben. Acties van gebruikers met veelomvattende rechten/privileges zijn ook inzichtelijk.

De Oplossing (inclusief raakvlaksystemen en tooling) wordt volcontinu gemonitored op beveiligingsinbreuken zodat er direct adequaat gereageerd kan worden op (beveiligings)incidenten. Er is een alertingproces ingericht om direct (prio 1) te kunnen handelen in geval van Incidenten en (dreigende) verstoringen en als de drempelwaarden voor de RTO (dreigen te) worden overschreden.

Excepties worden gelogd. Beveiligingsincidenten worden daarnaast gelogd voor forensisch onderzoek.

Inbreuken worden vastgelegd en acties worden genomen de ontstane risico's te mitigeren

Voor het toepassen van ketenmonitoring maakt de Opdrachtgever gebruik van een Centrale Event Manager (CEM). De CEM is de "spin in het web" van de Monitoring. De DCS Infrastructuur kent verschillende domeinen die beheerd worden met diverse Domein Event Managers. Bijvoorbeeld SCOM voor Windows of NNMI voor Netwerken. Alle events uit de verschillende domeinen komen in de CEM terecht. Hiervoor worden de producten Netcool/Operations Insight en Netcool/Omnibus van IBM gebruikt. Voor de aansluiting op de CEM bestaan 2 mogelijkheden: de Tivoli EIF probe of middels SNMP.

UE.72	Ten behoeve van Ketenmonitoring dient de Oplossing gekoppeld te worden aan het generieke beheerplatform van de Opdrachtgever.
-------	---

UE.73	Alle berichten ten behoeve van remote Monitoring in de vorm van logmeldingen, alerts, events en SNMP traps dienen ontdaan te zijn van metadata en moeten via de XML gateway van de Opdrachtgever (IBM Datapower) te worden verstuurd.
-------	---

10.1.1.4. Business Continuity Management (BCM)

De Opdrachtgever maakt in het kader van BCM een onderscheid binnen het twin Datacenter tussen:

- Operationele continuïteit
één Datacenter met productie/beheer servers is volledig weggefallen, het 2e Datacenter is nog volledig intact.
- Calamiteiten
Op beide locaties dient een gehele recovery plaats te vinden, doordat één Datacenter is weggefallen, en de storage voorziening van beide Datacenters niet meer intact is.

In beide gevallen mag de OTA en Lab omgeving in overleg worden opgeofferd ten behoeve van het vrijmaken van resources voor de Productieomgeving.

Operationele continuïteit

UE.74	De Oplossing voldoet aan onderstaande eisen betreffende de operationele continuïteit: • RTO: <= 1 (Klok)uur. • RPO: ~0 (Klok)uren. • Gedegradeerde capaciteit is toegestaan. • Minimaal gegarandeerde Beschikbaarheid conform SLA. • De OTA en Sandbox omgeving mogen in overleg worden gestopt en de daarvoor in gebruik zijnde Infrastructuur mag worden ingezet voor de Productie- en Beheer omgeving. Herstelduur oorspronkelijke situatie na aanvang Incident: 2 Kalenderdagen
-------	--

UE.75	Per Datacenter locatie bevindt zich een gehele hard - en software stack van een SAP Systeem. Dit geldt ook voor de B&R Apparatuur en Programmatuur.
-------	---

Replicatie tussen de twee Datacenters

Om de operationele continuïteit waar te maken zijn replicatie technieken niet te vermijden. Te denken valt bijvoorbeeld aan een combinatie van HANA replicatie door middel van logreplay, welke invloed heeft op de sizing van de servers naar het tweede Datacenter, in combinatie met het opbrengen van de virtuele Hosts voor de SAP Netweaver WAS met stretched cluster technieken

GUE 61.	De standaard transport layer die gebruikt moet worden voor datareplicatie is Dark Fiber.
---------	--

UE.76	De Opdrachtnemer voorziet de Oplossing van Apparatuur en/of Programmatuur om de Gegevens over Dark Fiber te kunnen zenden en ontvangen. Hierbij mag uitgegaan worden van de situatie in Groningen waarbij de afstand tussen beide Datacenter locaties 20 km bedraagt (afstand in Apeldoorn bedraagt 5 km).
-------	--

Er zijn drie verschillende vormen van replicatie tussen de 2 Datacenters:

1. **Primaire storage replicatie**
De primaire storage dient (near-)real-time te worden gerepliceerd. Dit geldt alleen voor productie- en beheersystemen (met uitzondering van de HANA Systemen). De verantwoordelijkheid hiervoor ligt geheel bij de Opdrachtnemer.
2. **Backup replicatie**
Voor alle systemen, dus van Datacenter locatie A naar Datacenter locatie B en omgekeerd. De verantwoordelijkheid hiervoor ligt geheel bij de Opdrachtnemer, waarbij de backups binnen 12 uur naar het andere Datacenter moeten zijn gerepliceerd.
3. **HANA replicatie**
Dit geldt alleen voor productie- en beheersystemen, van Datacenter locatie A naar Datacenter locatie B. De verantwoordelijkheid hiervoor ligt bij de Opdrachtgever voor wat betreft de uitvoering.

GUE 62.	De Oplossing moet waarborgen dat de Gegevens die moeten worden gerepliceerd, conform punt 1, 2 en 3 hierboven, ook daadwerkelijk gerepliceerd worden.
---------	---

Calamiteiten (Disaster recovery)

UE.77	De Opdrachtnemer dient voorbereid te zijn op de situatie dat de Oplossing dusdanig beschadigd raakt dat voor herstel de backup van de Gegevens nodig zijn.
-------	--

UE.78	Opdrachtnemer werkt op verzoek mee aan een jaarlijkse Disaster recovery test. Hieraan zijn voor de Opdrachtgever geen kosten verbonden.
-------	---

W 4	Disaster recovery De Opdrachtgever wenst een beeld te krijgen welke maatregelen Inschrijver neemt om in geval van een Calamiteit en na vrijgave van de Manged Service door de Opdrachtgever de Oplossing te herstellen. Uitgangspunten hierbij zijn: • RTO: best effort, max. 24 uur. • RPO: best effort, max. 12 uur. • Gedegradeerde capaciteit is toegestaan • De OTA en Sandbox omgeving mag worden gestopt en de daarvoor in gebruik zijnde Infrastructuur mag worden ingezet voor Productie en Beheer.
------------	--

In uw beschrijving dienst u in ieder geval de volgende aspecten uit te werken:

- Aanpak en snelheid van herstel
- Technische maatregelen
- Organisatorische maatregelen

Verwachting:

De Opdrachtgever verwacht van het antwoord van de Inschrijver dat:

- De beantwoording volledig is conform de hierboven genoemde uitgangspunten en aspecten.
- Het antwoord overtuigend, samenhangend en logisch is.

Beoordeling:

Deze wens wordt beoordeeld op basis van de mate waarin het antwoord voldoet aan de verwachtingen van de Aanbestedende dienst. Het maximale aantal punten dat behaald kan worden voor deze wens is **60 punten**.

Aantal punten	Toelichting:
0	Het antwoord op de wens voldoet niet aan de verwachtingen.
15	Het antwoord op de wens voldoet niet volledig aan de verwachtingen.
35	Het antwoord op de wens voldoet aan de verwachtingen.
60	Het antwoord op de wens overstijgt de verwachtingen van de Aanbestedende dienst doordat het Plan van Aanpak (bovenop de omschreven verwachtingen) aanvullende, vernieuwende, originele of slimme voorstellen bevat, waar de beoordelaars positief door worden verrast.

Voorschriften uitwerking

Wij vragen uw uitwerking in maximaal **10 pagina's A4** (lettertype Arial, lettergrootte 10 en regelafstand 1,0) te verwoorden. Extra pagina's en/of hyperlinks worden niet in de beoordeling meegenomen.

10.1.1.5. Release – en Patch management

UE.79	Opdrachtnemer informeert Opdrachtgever tijdig (binnen 3 maanden) over nieuwe Releases en Patches ten behoeve van het optimaal gebruik van de Oplossing en de daarbij verwachte Impact voor Opdrachtgever. Waar mogelijk wordt een jaarplan opgesteld voor Releases / Patches.
UE.80	Het doorvoeren van Releases en Patches ten behoeve van het optimaal gebruik van de Oplossing wordt in overleg met Opdrachtgever ingepland.
UE.81	Releases / Patches mogen de Beschikbaarheid van de Oplossing niet negatief beïnvloeden (tenzij er de Release / Patches een calamiteit oplost). Releases / Patches worden altijd gefaseerd (per locatie of indien mogelijk per domein geïmplementeerd.
UE.82	Opdrachtnemer stelt Releases middels een download beschikbaar.

UE.83	Gedurende de Overeenkomst is er voor Opdrachtgever een actuele Release kalender van de Oplossing beschikbaar.
-------	---

W 5	Minimalisatie geplande downtime Geef aan op welke manier er Onderhoud aan de Oplossing kan plaatsvinden zonder geplande downtime van de HANA-database en S/4HANA, alsmede ook andere SAP en niet SAP producten, zoals SAP NetWeaver, MaxDB database en SAP Sybase . Beoordeling: Al het Onderhoud (m.u.v. Onderhoud aan het operating system) kan plaatsvinden zonder geplande downtime van de SAP applicaties en databases voor de gebruikers = 180 punten Een deel van het onderhoud (m.u.v. Onderhoud aan het OS) kan plaatsvinden zonder geplande downtime van de SAP applicaties en databases voor de gebruikers = 90 punten Onderhoud kan niet plaatsvinden zonder geplande downtime van de SAP applicaties en databases voor de gebruikers = 0 punten Het maximale aantal punten dat behaald kan worden voor deze wens is 180 punten. Voorschriften uitwerking Wij vragen uw uitwerking in maximaal 1 pagina's A4 (lettertype Arial, lettergrootte 10 en regelafstand 1,0) te verwoorden. Extra pagina's en/of hyperlinks worden niet in de beoordeling meegenomen.
------------	---

10.1.1.6. Verbeterplan

UE.84	Indien de Oplossing voor een periode van drie (3) maanden niet voldoet aan één of meerdere Service Levels levert Opdrachtnemer hiervoor een Verbeterplan (ook wel herstelplan genoemd), inclusief een bijbehorend realisatievoorstel, aan bij de Opdrachtgever. Het Verbeterplan moet leiden tot een situatie waarbij de Service Levels wel worden gerealiseerd. Het Verbeterplan wordt binnen tien (10) Werkdagen na verzoek van de Opdrachtgever opgeleverd. Toepassing van het Verbeterplan laat de overige rechten van Opdrachtgever onverlet, waaronder die op schadevergoeding en bevat minimaal de volgende elementen: • Naam van Verbeterpunt. • Startdatum. • Geplande einddatum. • Beoogde aanpak (kort). • Status. • Lessons learned. • De Security roadmap
-------	--

10.1.2. Remote support

Voor remote toegang tot de SAP PoD (zie afbeelding 1: PoD) biedt de Opdrachtgever de Privileged Remote Access (PRA) dienst wat een onderdeel is van de Privileged Access Management (PAM) dienstverlening. Deze dienst vervangt de huidige Secure Access dienst. Op dit moment zijn er nog geen dienstbeschrijving of aansluitvoorwaarden beschikbaar.

GUE 63.	De Inschrijver maakt voor remote toegang uitsluitend gebruik van de Privileged Remote Access dienst van de Opdrachtgever.
---------	---

Opdrachtnemers die gebruik willen maken van de Remote support functionaliteit, gaan vooraf akkoord met de

huisregels in relatie tot het gebruik van Remote support. Door gebruik te maken van Remote support gaat u akkoord met onderstaande voorwaarden:

1. Door het gebruik van de aan u verstrekte URL krijgt u toegang tot vertrouwelijke Gegevens van de Opdrachtgever. U mag hiervan uitsluitend zelf gebruik maken en alleen voor het doel waarvoor u uitgenodigd bent door de gastheer van de Opdrachtgever.
2. U mag verkregen informatie op geen enkele wijze overdragen, verveelvoudigen, bewerken of verspreiden dan uitsluitend voor de uitvoering van de overeengekomen werkzaamheden.
3. U bent verplicht om aanwijzingen van de Opdrachtgever omtrent het gebruik van de informatie en/of Remote support op te volgen.
4. Bij het inloggen dient u zich met uw volledige naam, voorletters en bedrijfsnaam bekend te maken.
5. De Opdrachtgever kan een lijst opleveren van ondersteunde besturingssystemen en browsers.
6. De Opdrachtgever is niet verantwoordelijk of aansprakelijk voor eventuele schade ten gevolge van het gebruiken van Remote support.
7. Ziet u iets afwijkends bij het gebruik van Remote support? Neem dan direct contact op met de gastheer van uw Remote support sessie.
8. Misbruik wordt bestraft.
9. Op het gebruik van Remote support is Nederlands recht van toepassing.

GUE 64.	Inschrijver die gebruik wil maken van de Remote support functionaliteit, gaan vooraf akkoord met de bovenstaande huisregels van Opdrachtgever in relatie tot het gebruik van Remote support.
---------	--

Het up- en downloaden van bestanden ten behoeve van Beheer- en Onderhoudswerkzaamheden kan niet door gebruik te maken van de Privileged Remote Access dienst. Dit dient op een andere, veilige wijze plaats te vinden via een datasluis.

GUE 65.	De Inschrijver dient binnen de SAP PoD een voorziening te realiseren die fungeert als datasluis. Deze voorziening mag alleen bestanden ontvangen en accepteren die zijn voorzien van een digitale handtekening (code signing). In deze datasluis moet functionaliteit aanwezig zijn waarmee bestanden kunnen worden geschoond van kwaadaardige software zoals virussen, malware etc. De datasluis dient gemonitord te kunnen worden door het Security Operations Center van de Opdrachtgever. Het up- en downloaden van bestanden ten behoeve van Beheer- en Onderhoudswerkzaamheden kan niet door gebruik te maken van de Privileged Remote Access dienst. Dit dient op een andere, veilige wijze plaats te vinden via een datasluis.
---------	--

GUE 66.	Het up- en downloaden van bestanden ten behoeve van Beheer- en Onderhoudswerkzaamheden kan niet door gebruik te maken van de Privileged Remote Access dienst. Dit dient op een andere, veilige wijze plaats te vinden via een datasluis.
---------	--

10.1.3. Rapportage

UE.85	Opdrachtnemer zorgt ervoor dat Opdrachtgever inzicht heeft in de geleverde Prestaties ten opzichte van de overeengekomen Prestaties in dit document. Dit inzicht dient minimaal maandelijks actueel te zijn. Met name wil Opdrachtgever inzicht in: • KPI opgeloste Incidenten binnen en buiten Service Levels; • KPI Beschikbaarheid. • KPI Service desk • KPI Service Window • KPI Standaard service activiteiten; • Status, voortgang en afhandeling van openstaande en opgeloste vragen, (Security) Incidenten, Problems en verbetervoorstellen. Hierbij wordt aangegeven: datum ontvangst, datum in behandeling, verwachte opleverdatum en datum afgevoerd; • Een cumulatieve Rapportage over alle vragen, Incidenten en Problems. De gecumuleerde Rapportage laat de historie over een periode van minimaal 14 maanden zien, zodat trends kunnen worden geanalyseerd;
-------	--

	• Datum laatste en volgende A&P testen; • Vervaldata certificaten zoals ISO27001-certificering (of gelijkwaardig), TLS-certificaat. Tevens worden volgende onderdelen verwacht indien deze van toepassing zijn: • Status Additionele dienstverlening (opdrachten en/of strippenkaart). Hierbij wordt minimaal aangegeven: datum opdrachtverstrekking, startdatum, (verwachte) Opleverdatum, (verwachte) Acceptatiedatum, uitnutting budget; • Licentie gebruik (t.o.v. aantal gekochte licenties). In overleg kunnen onderwerpen worden toegevoegd of verwijderd. Het gevraagde inzicht kan bijvoorbeeld middels een maandelijkse SRN toegestuurd worden vóór de 10e van elke maand, tevens is een aanvullend dashboard met actuele informatie is ook mogelijk. Het is Opdrachtnemer vrij hier een keuze in te maken, zolang het inzicht maar gegeven wordt.
--	---

10.2. Documentatie

UE.86	Opdrachtnemer levert gedurende de operationele fase van de Overeenkomst Documentatie, conform de eisen zoals neergelegd in Hoofdstuk 8 'Documentatie'.
-------	--

10.3. Factureren en bestellen

Als leverancier bent u verplicht elektronisch te factureren

Wij zijn als overheid vanaf november 2018 verplicht om e-factureren te implementeren. Dit is vastgelegd in de EU-Richtlijn Elektronische facturering bij overheidsopdrachten (2014/55/EU). De Rijksoverheid werkt sinds 1 januari 2017 bij nieuwe overeenkomsten met e-facturering.

Manieren van e-factureren

Ondernemers die goederen of diensten aan de Rijksoverheid leveren en een e-factuur willen sturen, kunnen dat op verschillende manieren doen,

- via een DigiPoort aansluiting
- via het netwerk Peppol
- via het leveranciersportaal.

Bekijk de video op de website: [Home | Helpdesk e-factureren \(helpdesk-efactureren.nl\)](#).

DigiPoort

De DigiPoort is een technische voorziening die beheerd wordt door Logius en die het mogelijk maakt om diverse elektronische berichten (waaronder facturen) met de Rijksoverheid uit te wisselen. Meer informatie over berichtenuitwisseling via de DigiPoort vindt u op [Handleiding Aansluiten op Digipoort voor Bedrijven | Logius](#)

Peppol

Peppol is een digitale infrastructuur gebaseerd op open standaarden voor het eenvoudig en veilig uitwisselen van e-facturen en andere elektronische berichten. Met Peppol kunt u e-facturen rechtstreeks versturen vanuit uw boekhoudsysteem of e-facturen versturen via een (commercieel)Peppol-portaal. Peppol is de nieuwe EU standaard voor elektronisch berichtenverkeer met de overheid. Meer informatie over Peppol vindt u op www.peppolautoriteit.nl/

Leveranciersportaal

U kunt ook gebruik maken van het e-factuurportaal van de Rijksoverheid, het leveranciersportaal. Op dit portaal kunt u e-facturen versturen en inkooporders of tijdkaarten ontvangen indien het departement dit ondersteunt. Het Rijk bevindt zich in een transitiefase wat betreft het leveranciersportaal. Het huidige leveranciersportaal van DigiInkoop wordt vervangen. U wordt tijdig geïnformeerd over de overgang naar het nieuwe leveranciersportaal.

UE.87	De Opdrachtnemer voldoet aan de vereisten van e-facturatie via het leveranciersportaal of een geautomatiseerde koppeling met de DigiPoort (toekomstig E-procurementpoort) of het Peppol netwerk met daarin de referentie naar de inkooporder en de inkooporderregel.
UE.88	Kosten die voortkomen uit het realiseren van de koppeling voor elektronische berichten uitwisseling met de Rijksoverheid worden gedragen door de Opdrachtnemer.
UE.89	Opdrachtnemer vermeldt het inkoopordernummer als referentie op elke pakbon en factuur aan Opdrachtgever. Zonder dit Inkoopordernummer kan Opdrachtgever de levering of de factuur weigeren.
UE.90	Opdrachtnemer is verantwoordelijk voor de realisatie aan haar zijde. Op verzoek van Opdrachtgever kunnen wijzigingen in het Plan van aanpak en/of Realisatie worden aangebracht die invloed hebben op het bestelproces. Hieronder valt in ieder geval het inzetten van extra expertise.
UE.91	Opdrachtnemer accepteert dat er gedurende de looptijd van de Overeenkomst nieuwe-/verbeterde versies van de programmatuur van het leveranciersportaal in gebruik genomen kunnen worden.

10.4. Kaders voor (re)transitie

10.4.1. Inleiding

In geval van (tussentijdse) beëindiging of afloop van de Overeenkomst van SAP Manged Platform, dient de Opdrachtnemer ten allen tijde alle medewerking te verlenen aan een gecontroleerde en projectmatige overdracht aan een opvolgende opdrachtnemer of Opdrachtgever en daarmee alle Documentatie, Gegevens en informatie te verstrekken die nodig zijn voor een goede overdracht.

De termijn waarbinnen de Retransitie dient te worden afgerond zal tussen Opdrachtnemer en Opdrachtgever worden overeengekomen.

10.4.2. Documentatie en Gegevens(overdracht)

UE.92	Zodra partijen bekend zijn met het feit dat de Overeenkomst om welke reden dan ook eindigt of wordt beëindigd, waaronder begrepen opzegging en ontbinding, inventariseren Partijen gezamenlijk welke assistentie van Opdrachtnemer, tegen marktconforme tarieven (met een maximum van de consultancy tarieven), noodzakelijk is voor een succesvolle Retransitie waarbij de continuïteit van de Prestatie gewaarborgd blijft. Hierbij wordt, indien noodzakelijk, het Retransitieplan dat is opgesteld in het Plan van Aanpak, door de Partijen herzien, waarvoor de (Uitvoerings)eisen uit de hoofdstuk leidend zijn.
UE.93	Opdrachtnemer verleent volledige medewerking aan de Retransitie en verstrekt daarbij alle relevante Documentatie aan Opdrachtgever c.q. opvolgende opdrachtnemer verstrekken.

10.4.3. (Proces)afspraken Retransitiefase

Om te waarborgen dat de Retransitie op een efficiënte en ongestoorde wijze plaatsvindt, zal de Opdrachtnemer in ieder geval voldoen aan de volgende uitvoeringseisen:

UE.94	Bij overgang naar een nieuwe opdrachtnemer moet de Prestatie voor een periode van 6 maanden tegen gelijkblijvende condities (naar rato), voor Opdrachtgever beschikbaar blijven.
UE.95	Opdrachtnemer stelt gedurende de periode van Retransitie de voor Opdrachtgever ontwikkelde methoden, technieken, Programmatuur en andere technische voorzieningen ter beschikking en laat deze ontwikkelde methoden, technieken, Programmatuur en andere technische voorzieningen gebruiken door Opdrachtgever en opvolgende Opdrachtnemer, met als doel een efficiënte Retransitie te bewerkstelligen. De opvolgende Opdrachtnemer wordt verplicht een geheimhoudingsverklaring te ondertekenen.
UE.96	Opdrachtnemer houdt voldoende gekwalificeerd personeel beschikbaar voor de Retransitie.
UE.97	Opdrachtnemer verleent medewerking aan een Audit betreffende de inhoud en de kwaliteit van de informatie die Opdrachtnemer in het kader van Retransitie beheerd.
UE.98	Opdrachtnemer dient inzage te geven in de gebruikte middelen en processen tijdens de periode van Retransitie.
UE.99	Opdrachtnemer dient onder meer de verbindingen te verbreken, eventueel aan Opdrachtgever ter beschikking gestelde Apparatuur terug te geven en elektronische sleutels aan Opdrachtgever ter beschikking te stellen.