BIJLAGE A SPECIFICATIE VAN DE OPDRACHT

Europese aanbesteding

“Technology Business Management oplossing”

Versie: 1.1
Kenmerk: IUC 25-025
Datum: 28 april 2026

INHOUDSOPGAVE

Hoofdstuk 1. Inleiding

Dit document beschrijft de eisen en wensen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding “Technology Business Management oplossing”, hierna TBM-oplossing, met kenmerk IUC 25-025. Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

Hoofdstuk 2. Functionals

2.1. Algemeen

GUE 1.	De TBM-oplossing ondersteunt versiebeheer van TBM-modellen.

GUE 2.	De TBM-oplossing ondersteunt OTAP-fasering (Ontwikkel, Test, Acceptatie, Productie) waarbij meerdere omgevingen met verschillende versies gelijktijdig (tijdelijk) beschikbaar zijn.

GUE 3.	Binnen de TBM-oplossing zijn meerdere en verschillende testomgevingen (OTA) beschikbaar.

GUE 4.	De TBM-oplossing beschikt over ingebouwde mogelijkheden voor benchmarking die de Opdrachtgever in staat stellen te benchmarken tegen diverse peer groups. De TBM-oplossing beschikt minimaal over de volgende ingebouwde benchmarkmogelijkheden: - Met peer groepen van organisaties; - Op IT-Tower niveau ten opzichte van andere organisaties.

GUE 5.	De TBM-oplossing ondersteunt IT-kostentransparantie en showback/chargeback.

GUE 6.	De TBM-oplossing ondersteunt meerdere allocatiemethoden zoals directe allocatie en activity-based costing.

GUE 7.	De TBM-oplossing ondersteunt het separaat inzichtelijk maken van uitgaven, kosten, investeringen en budgetten voor run (-the-business) en change (-the-business).

GUE 8.	De TBM-oplossing ondersteunt het inladen en inzichtelijk maken van data tot op het laagste granulariteitsniveau via doorklikfunctionaliteit.

GUE 9.	De TBM-oplossing ondersteunt geautomatiseerde als ook handmatige gegevensinvoer via ten minste: - File formaten: JSON, CSV en custom defined; - Bronnen: File, FTP, SFTP en Windows share; - API's, SOAP of REST, JDBC of ODBC; - Directe aanpassingen in regels in de TBM-oplossing zelf.

GUE 10.	De TBM-oplossing biedt de mogelijkheid Total Cost of Ownership te volgen voor Technology Solutions met meerdere componenten, leveranciers en interne middelen voor de gehele levenscyclus.

GUE 11.	De TBM-oplossing ondersteunt configuratie en aanpassing van het TBM-model aan maatwerkprocessen en allocaties door Gebruikers. Bijvoorbeeld door het toevoegen van Opdrachtgever-specifieke IT-towers en costpools. Dit wordt incidenteel toegepast.
GUE 12.	De TBM-oplossing ondersteunt het meerlaags modelleren van Technology Solutions.
GUE 13.	De TBM-oplossing biedt versiebeheer van Gegevens en auditing van dataveranderingen over tijd aan.
GUE 14.	De TBM-oplossing volgt en beheert IT-uitgaven op ten minste maand- en kwartaal- en jaarbasis, inclusief ondersteuning voor het vastleggen van zowel CapEx als OpEx.
GUE 15.	De TBM-oplossing ondersteunt financiële tijdsbewustheid (bijvoorbeeld kalenderjaar, gebroken boekjaar, maandelijkse trends, en afsluitcycli) als standaarddimensie in databeheer en rapportages.
GUE 16.	In één (1) TBM-model in de TBM-oplossing worden de financiële stelsels 'baten-lasten' en 'kas verplichtingen' ondersteunt.
GUE 17.	De TBM-oplossing biedt functionaliteit voor toerekening van niet-financiële waarden waaronder CO2 en energieconsumptie in Kwh in dezelfde structuur als kosten, voor alle componenten van de TBM Taxonomie, met gedeelde en/ of alternatieve allocatiemethoden.
GUE 18.	De TBM-oplossing faciliteert besluitvorming op basis van duurzaamheidsaspecten door scenario-analyse uit te kunnen voeren met Kosten, en CO2 en/of KWh: bv. wat is het effect op kosten en CO_2 als workload verplaatst wordt, of als apparatuur langer in gebruik wordt genomen.
GUE 19.	De TBM-oplossing biedt mogelijkheden tot toekennen van het kenmerk vast of variabel aan kosten en maakt het mogelijk het onderscheid maken tussen vaste en variabele kosten.
GUE 20.	De TBM-oplossing biedt mogelijkheden tot het toekennen van attributen (ook wel labels of tags genoemd) aan Technology Solutions in de TBM-oplossing om deze door te kunnen vertalen naar andere kostprijsmodellen zoals IT-kosten per wet of per proces.
GUE 21.	Versiewijzigingen in de TBM-taxonomie zijn uiterlijk binnen 12 maanden na publicatie door de TBM Council beschikbaar in de TBM-oplossing.
GUE 22.	Bij versiewijzigingen van de TBM-taxonomie blijven oudere versies van de TBM-taxonomie minimaal gedurende 12 maanden beschikbaar in de TBM-oplossing.

W 1	Beschrijf op welke wijze de TBM-oplossing meerdere (IT) organisaties (enterprises) met eigen grootboek, eigen en/of gedeelde IT-infrastructuur eigen producten en dienststructuur en onderlinge kostprijsverrekening ondersteunt. **Optie 1** Meerdere IT organisaties kunnen separaat gebruik maken van de TBM-oplossing. De IT-organisaties hebben allemaal een eigen afgebakende omgeving en de credentials voor toegang zijn per IT-organisatie verschillend. **Optie 2** Meerdere IT organisaties kunnen separaat gebruik maken van de TBM-oplossing en kunnen via dezelfde user-credentials verschillende toegangsniveau krijgen voor de diverse organisaties **Optie 3** Meerdere IT organisaties kunnen separaat gebruik maken van de TBM-oplossing en kunnen via dezelfde user-credentials verschillende toegangsniveau krijgen voor de diverse organisaties. Deze IT organisaties hangen samen onder eenzelfde overkoepelend organisatiecluster. De verschillende IT organisaties kunnen binnen de grenzen van de TBM-oplossing data met elkaar delen en gebruik maken van gedeelde datasets. De beoordeling voor deze Wens is als volgt: De TBM-oplossing geen van de genoemde opties1 0 punten; De TBM-oplossing ondersteunt optie 1 20 punten; De TBM-oplossing ondersteunt optie 1 en optie 2 65 punten; De TBM-oplossing ondersteunt optie 1, optie 2 en optie 3 80 punten. Op deze Wens kunnen maximaal 80 punten worden behaald. Voor de beantwoording van deze Wens moet Inschrijver de Bijlage IX Beantwoording Overige wensen.odt gebruiken.

W 2	Opdrachtgever vindt het belangrijk hoe de TBM-oplossing concrete sturing door middel van duurzaamheidsaspecten faciliteert door transparant inzicht te creëren in diverse duurzaamheidsmetrieken. Geef voor onderstaande punten aan of de TBM-oplossing hier invulling aan geeft: 1. De TBM-oplossing biedt het inzicht in emissie-metrieken met betrekking tot e-waste; 2. De TBM-oplossing biedt het inzicht in emissie-metrieken met betrekking tot watergebruik; 3. De TBM-oplossing biedt de mogelijkheid om emissie-metrieken (waaronder minimaal KWh en CO2) van de top 3 Hyperscalers (Zie ook: https://datacentremagazine.com/articles/top-10-hyperscalers.)in de TBM-oplossing te volgen om besluitvorming tussen on-premise hosting en public cloud hosting omwille van duurzaamheid te faciliteren; 4. De TBM-oplossing biedt ingebouwde analytics die automatisch patronen herkennen en middels signalering suggesties doen voor energiebesparing of CO_2-reductie; 5. De TBM-oplossing heeft benchmarking-mogelijkheden hebben met peers of industriewaarden op duurzaamheid KPI's (vergelijkbaar met cost benchmarking); 6. De TBM-oplossing voorziet in gebruikersrollen en Governance die duurzaamheid versus kostenbesparing als aparte dimensie behandelen (dus ownership van "sustainability value driver");

	7. De TBM-oplossing ondersteunt ESG extensies; 8. Voor de allocatie van duurzaamheidsmetrieken is het startpunt de modellering van de allocatie van kosten om zo met minimale aanpassing inzicht in duurzaamheidsaspecten te creëren. De beoordeling voor deze Wens is als volgt: De TBM-oplossing ondersteunt optie 1 6 punten; De TBM-oplossing ondersteunt optie 2 6 punten; De TBM-oplossing ondersteunt optie 3 6 punten; De TBM-oplossing ondersteunt optie 4 6 punten; De TBM-oplossing ondersteunt optie 5 8 punten; De TBM-oplossing ondersteunt optie 6 6 punten; De TBM-oplossing ondersteunt optie 7 6 punten; De TBM-oplossing ondersteunt optie 8 6 punten. Op deze Wens kunnen maximaal 50 punten worden behaald. Voor de beantwoording van deze Wens moet Inschrijver de Bijlage IX Beantwoording Overige wensen.odt gebruiken.

GUE 23.	De TBM-oplossing faciliteert signalering van diverse scenario's waaronder minimaal: - Consolidatiekansen bij leveranciers; - Rationalisatie-initiatieven van applicaties; - Outliers in kosten; - Kansen voor capaciteitsmanagement.

GUE 24.	De TBM-oplossing identificeert nog niet toegewezen kosten in de TBM-taxonomie en faciliteert de reducering hiervan.

GUE 25.	De TBM-oplossing biedt mogelijkheden voor auditing en tracking van gebruikersactiviteit en dataveranderingen, inclusief versiebeheer en gelijktijdig gebruik zonder dataverlies.

GUE 26.	De TBM-taxonomie is standaard in de TBM-oplossing opgenomen zodat er geen aanpassingen aan de TBM-oplossing nodig is en deze direct toepasbaar is.

W 3	Beschrijf in maximaal één (1) A4 welke mogelijkheden de TBM-oplossing biedt om de data in de TBM-oplossing te verbeteren. De beoordelingscriteria voor deze Wens zijn: - Op welke wijze verbeteracties van datakwaliteit worden geïdentificeerd en gestimuleerd; - Of signaalfuncties ten behoeve van fouten in dataloads worden geboden; - Of signaalfuncties behoeve van verbeteracties van datakwaliteit worden geboden; - Of signaalfuncties ten behoeve van verbetermogelijkheden in integratieprocessen worden geboden; - Of prioritering op datakwaliteitsissues wordt gefaciliteerd. Voor deze Wens geldt de volgende waardering: 0 Zeer slecht; 15 Slecht; 50 Matig;

	120 Voldoende; 160 Goed; 210 Uitstekend Zie tabel 3 Beoordeling Wensen uit het Beschrijvend document voor een uitleg bij de beoordeling. Voor de beantwoording van deze Wens moet Inschrijver de Bijlage IX Beantwoording Wens 3 Verbetering data.odt gebruiken.

GUE 27.	De TBM-oplossing is gebaseerd op TBM Taxonomy, version 4.3 of hoger.

GUE 28.	De TBM-oplossing biedt de mogelijkheid om Gegevens vanuit de cost-pools voor de actuals en de budgetten onafhankelijk van elkaar op te kunnen werken vanuit verschillende bronnen.

GUE 29.	De TBM-oplossing faciliteert het mappen van Gegevens vanuit de bron op het datamodel in de TBM-oplossing middels templates voor allocaties en/ of geautomatiseerde allocaties.

W 4	**FinOps** Voor deze Wens geldt dat deze als een Herzieningsclausule is gedefinieerd en het op moment van deze aanbesteding niet duidelijk is of en wanneer deze Herzieningsclausule eventueel wordt gelicht. Geef aan of de TBM-oplossing ook de mogelijkheid biedt gebruik te maken van functionaliteiten voor FinOps die door de FinOps Foundation erkende zijn als FinOps tool. Geef aan hoe deze functionaliteiten gebruikt kunnen worden binnen de TBM-oplossing eventueel als aanvullende module of uitgebreide licentie. Voor deze Wens geldt de volgende waardering: 0 punten De TBM-oplossing biedt geen mogelijkheid gebruik te maken van een door de FinOps Foundation erkende FinOps tool; 35 punten De TBM-oplossing biedt wel de mogelijkheid vanuit de TBM-oplossing gebruik te maken van een geïntegreerde door de FinOps Foundation erkende FinOps tool. Voor de beantwoording van deze Wens moet Inschrijver de Bijlage IX Beantwoording Overige wensen.odt gebruiken.

2.2. Rapportage

GUE 30.	De TBM-oplossing beschikt over de functionaliteit voor het creëren en delen van rapportages door gebruikers en administrators zonder programmeercodering; die alleen voor geselecteerde gebruikers inzichtelijk zijn.

GUE 31.	De TBM-oplossing biedt configureerbare standaard rapportages voor IT-kostenanalyses, inclusief trendanalyses, prognoses en variantieanalyses.

GUE 32.	De TBM-oplossing biedt configureerbare standaard rapportages die door de gebruikers aan specifieke behoeften aangepast kunnen worden.

GUE 33.	De TBM-oplossing beschikt over standaardrapportages op alle lagen van de TBM-taxonomie.

GUE 34.	De TBM-oplossing biedt mogelijkheden tot het configureren van bestaande, en creëren van nieuwe, rapportages binnen de TBM-oplossing.

GUE 35.	De TBM-oplossing ondersteunt integratie en beheer van financiële en niet-financiële aspecten, zoals personeelsaantallen, benuttingsgraden, servicevolumes en projectmijlpalen.

Het is voor de Opdrachtgever belangrijk om de dwarsdoorsnedes m.b.t.:

- Interne arbeidskosten binnen IT-functies en projecten te volgen en beheren, inclusief tijdregistratie, loontarieven en allocatiemethoden;
- Onderscheid te maken tussen geactiveerde en operationele arbeidskosten binnen de TBM-oplossing;
- Het volgen en categoriseren van IT-spend en uitgaven over Abonnementen, overeenkomsten, en eenmalige aankopen en
- Arbeidskostenanalyses, inclusief uitsplitsingen per organisatieonderdeel dienst en project;
- Werkelijke versus geplande kosten.

GUE 36.	De TBM-oplossing ondersteunt de mogelijkheden zoals hierboven beschreven.

GUE 37.	De TBM-oplossing koppelt budgetten per Costpool aan werkelijke uitgaven voor nauwkeurige financiële planning en beschikt over een geïntegreerde forecast op basis van realisaties en resterend budget.

GUE 38.	De TBM-oplossing ondersteunt het berekenen van kosten per eenheid door koppeling van infrastructuurdata aan consumptiemetrics, zoals bijvoorbeeld CPU seconden of Terabyte opslag.

GUE 39.	De TBM-oplossing ondersteunt het aggregeren van alle directe en indirecte kosten over de levenscyclus van een product of dienst.

GUE 40.	De TBM-oplossing biedt de mogelijkheid kostendrijvers voor een TCO-object met gedetailleerde weergaven te visualiseren.

GUE 41.	De TBM-oplossing ondersteunt scenario-analyse en simulatiefunctionaliteit binnen het TBM-model ten behoeve van forecasting.

GUE 42.	De TBM-oplossing is in staat zijn de Gegevens geautomatiseerd te ontsluiten naar .csv of .xlsx of rechtstreeks naar Selfservice BI tools waaronder minimaal PowerBI voor analyse in combinatie met andere KPI's.

GUE 43.	De TBM-oplossing biedt mogelijkheden om seizoen fluctuaties vast te leggen.

GUE 44.	De TBM-oplossing faciliteert het definiëren van meerjarige technologie-budgetten.

GUE 45.	De TBM-oplossing maakt het mogelijk om annotaties en verklaringen van budgetafwijkingen door budgeteigenaren vast te leggen in de TBM-oplossing

GUE 46.	De TBM-oplossing biedt standaardrapportages en dashboards met specifieke weergaven voor verschillende belanghebbenden waaronder ten minste IT, financiën en business leaders.

GUE 47.	De TBM-oplossing genereert uitgebreide rapportages en analyses voor diverse belanghebbenden, met inzichten in IT-prestaties, kosten en waarde, inclusief standaard en aanpasbare rapporten.

GUE 48.	De TBM-oplossing biedt functionaliteit voor het analyseren van trends en afwijkingen in arbeidskosten.

GUE 49.	De TBM-oplossing beschikt over standaardrapportages die KPI's ondersteunen die specifiek sustainability meten, waaronder: - CO2 per gebruiker, en per IT-dienst of applicatie; - Energieverbruik (kWh) per gebruiker, en per IT-dienst of applicatie; - Emissies toebedeeld aan business units/consumers.

W 5	Beschrijf in maximaal 2 pagina's welke mogelijkheden de TBM-oplossing biedt voor rapportages en Self-service BI. Beschrijf hoe deze mogelijkheden zich vertalen naar mogelijke handelingen voor diverse stakeholders. Maak hierbij een overzicht verschillende belanghebbenden vanuit de Finance, IT en business view en de mogelijkheden die ze hebben. De beoordelingscriteria voor deze Wens zijn: 1. Het antwoord beschrijft rapportagemogelijkheden en vertaalt deze naar concrete handelingen; 2. Het antwoord beschrijft diverse relevante stakeholders vanuit de drie verschillende views; 3. Het antwoord beschrijft welke inzichten de rapportages deze stakeholders verschaffen en hoe ze dit inzicht kunnen gebruiken om tot handelingen te komen; 4. Het antwoord beschrijft duidelijk mogelijkheden voor BI selfservice en de benodigde vaardigheden om hiermee te kunnen werken; 5. Het antwoord omschrijft hoe de TBM-oplossing de communicatie tussen de stakeholders vanuit de verschillende views faciliteert en bevordert; 6. Het antwoord laat zien hoe diverse stakeholders na de implementatie van de TBM-oplossing de TBM-oplossing kunnen gebruiken om waarde toe te voegen aan de processen van de IV-organisatie en haar klanten; 7. Het antwoord biedt nieuwe concrete inzichten in de toegevoegde waarde van de rapportages uit de TBM-oplossing en beschrijft in voor IV herkenbare situaties hoe deze in praktijk worden gebracht; 8. Het antwoord beschrijft in welke mate de TBM-oplossing (standaard)rapportages en SSBI faciliteert op, door de Opdrachtgever de gedefinieerde attributen/labels/tags die zijn toegekend aan solutions, om deze te kunnen vertalen naar andere kostprijsmodellen zoals IT-kosten per wet. Voor deze Wens geldt de volgende waardering:

	0 Zeer slecht; 20 Slecht; 60 Matig; 130 Voldoende; 200 Goed; 260 Uitstekend. Zie tabel 3 Beoordeling Wensen uit het Beschrijvend document voor een uitleg bij de beoordeling. Voor de beantwoording van deze Wens moet Inschrijver de Bijlage IX Beantwoording Wens 4 Rapportages en Self-service BI.odt gebruiken.

2.3. Technische interface integratie

GUE 50.	De TBM-oplossing ondersteunt voor alle componenten van de TBM-oplossing een functionele ontsluiting via een REST-API.

GUE 51.	Inschrijver heeft een beschrijving van de REST-API interface beschikbaar.

GUE 52.	De TBM-oplossing ondersteunt een interface die in staat is minimaal 500.000 records per uur te importeren en/of updaten met ondersteuning voor parallelle verwerking.

GUE 53.	De TBM-oplossing ondersteunt de laatste twee (2) versies van de ondersteunde webbrowsers, zonder gebruik te maken van aanvullende Programmatuur. Zie voor meer informatie: https://www.communicatierijk.nl/vakkennis/rijkswebsites/aanbevolen-richtlijnen/browsersupport .

Hoofdstuk 3. IV kaders

3.1. Non-functionals

GUE 53.	De user interface van de TBM-oplossing is minimaal beschikbaar in de Engelse taal.

Inzicht in gebruik

GUE 54.	De TBM-oplossing geeft inzicht in het gebruik van de TBM-oplossing in: - Hoeveel unieke Gebruikers gebruik maken van de TBM-oplossing; - Welke Gebruikers gebruik maken van de TBM-oplossing; - Hoe vaak per maand de Gebruikers inloggen.

GUE 55.	De TBM-oplossing informeert Opdrachtgever wanneer het Licentiegebruik overschreden wordt. Dit kan bijvoorbeeld door een (automatisch) alert in de vorm van een e-mail aan een in te stellen contactpersoon.

Webheaders zijn regels die voor een webapplicatie ingesteld kunnen worden richting de web browser. Met de juiste instellingen worden maatregelen geïmplementeerd die een webapplicatie veiliger kunnen maken. Denk hierbij bijvoorbeeld aan X-Frame-Options, X-Consent-Type-Options, Content-Security-Policy en Referred-Policy. Zie voor meer informatie de website van OWASP Foundation.

Om te bepalen of de beveiliging via webheaders afdoende is geborgd, gebruikt de Belastingdienst de dienst ‘Security Headers’ (https://securityheaders.com/).

GUE 56.	Als de TBM-oplossing webheaders toepast, dan voldoet de TBM-oplossing aan bovenstaande alinea.

Bij het ontwerpen en ontwikkelen van oplossingen wordt gewerkt vanuit de principes dat een oplossing voldoet aan informatiebeveiligingsstandaarden, voldoet aan de privacywetgeving en de gedachte dat beschikbaarheid zowel operationeel als bij uitzonderingssituaties geborgd is. Deze principes zijn cyclisch in het ontwerp geborgd, op een correcte manier geïmplementeerd en geëvalueerd.

In de markt wordt dit wel aangeduid met ‘Security by Design’, ‘Privacy by Design ’en ‘Continuity by Design’. Deze principes vallen onder Secure Software Development.

Dit betekent dat altijd de meest recente (veilige) versie vanuit een betrouwbare bron gebruikt wordt. Er mogen geen bekende Kwetsbaarheden in aanwezig zijn. Hiertoe heeft een evaluatie van de broncode plaatsgevonden (onder andere code scanning). Ook na ingebruikname vinden dergelijke evaluaties periodiek plaats.

Een hulpmiddel is een Software Bill of Material (op dit moment is het nodig in ieder geval inzicht te hebben in de gebruikte Programmatuur) waardoor er altijd inzicht is in alle gebruikte Programmatuur.

Mochten Kwetsbaarheden toch bestaan/ontstaan dan worden deze opgelost via de leverancier van de Programmatuur of conform de van toepassing zijnde Open Source-licentie. Niet weg te nemen Kwetsbaarheden worden gemeld als beveiligingsincident.

GUE 57.	De gangbare principes rondom 'Security by Design', 'Privacy By Design' (samen met 'Privacy by Default') en 'Continuity by Design' voor het ontwerp en de ontwikkeling van Programmatuur en systemen worden toegepast. Inschrijver hanteert een Secure Software Development proces (secure software development life-cycle) te waarborgen dat de betreffende Programmatuur veilig is ontwikkeld. De Inschrijver heeft minimaal de volgende maatregelen geborgd: - Secure coding guidelines zijn onderdeel van de ontwikkelrichtlijnen; - Tijdens het ontwikkelproces worden statische en dynamische code analyse uitgevoerd; - Richtlijnen voor wat betreft het wegnemen van Kwetsbaarheden zijn in lijn met die van de Belastingdienst; - Toegang tot de source code is beperkt (need-to-know, least privileged); - Releases: uitgangspunt is hierbij dat oplossingen van de Opdrachtgever geen als Kritisch of Hooggekwalificeerde Kwetsbaarheden mogen bevatten; - Er is een ingerichte procedure voor wijzigingsbeheer (wijzigingsadministratie, risicoafweging van mogelijke gevolgen, goedkeuringsprocedure, communicatie met de Opdrachtgever); - Inzicht in de gebruikte Programmatuur (Software Bill of Material): - Een up-to-date overzicht alle gebruikte/ingezette (open source) Programmatuur is beschikbaar.

Ontwikkel-, test, - acceptatie- en productieomgevingen zijn van elkaar gescheiden (het is toegestaan ontwikkel- en testomgevingen met elkaar te integreren). Programmacode wordt op een gecontroleerde manier tussen de omgevingen getransporteerd. In de productieomgeving worden geen testen uitgevoerd. Acceptatie-en beveiligingstesten worden uitgevoerd in de acceptatie-omgeving.

De acceptatieomgeving dient daartoe, op de gegevens set na, in alle opzichten gelijk te zijn aan de productieomgeving. Productiegegevens worden alleen in de productieomgeving gebruikt.

GUE 58.	Inschrijver maakt gebruik van gescheiden ontwikkel-, test-, acceptatie-en productieomgevingen (OTAP). In de Productieomgeving wordt niet getest. Er wordt niet getest met productiegegevens. Programmacode wordt op een gecontroleerde manier van omgeving tot omgeving getransporteerd. Alleen met expliciete toestemming van de Opdrachtgever (Gegevenseigenaar) kan hiervan worden afgeweken met toepassing van goedgekeurde (aanvullende) waarborgen.

3.2. Algemene eisen vanuit beveiligingsperspectief

De Belastingdienst verwerkt fiscale en financiële gegevens van particulieren en ondernemingen.

UE 1.	Opdrachtnemer deelt en/of gebruikt geen Gegevens voor eigen doeleinden, anders dan strikt noodzakelijk voor de uitvoering van de Overeenkomst én dan alleen ná expliciete toestemming van de Opdrachtgever. Opdrachtnemer zal in een dergelijk geval aangeven welke Gegevens als noodzakelijk worden geacht voor de uitvoering van de Overeenkomst.

UE 2.	Opdrachtnemer conformeert zich aan dat bij testen van de TBM-oplossing geen gebruik wordt gemaakt van Productiegegevens: - Gegevens die te relateren zijn aan de Belastingdienst mogen zonder expliciete toestemming van de Opdrachtgever niet buiten de TBM-oplossing verwerkt worden. Productiegegevens worden alleen in de Productieomgeving verwerkt. - Buiten de Productieomgeving zijn de Gegevens, conform marktstandaarden, bijvoorbeeld die van de NCSC, gepseudonimiseerd of geanonimiseerd. Opdrachtnemer geeft de Opdrachtgever vooraf inzicht in hoe dit plaats vindt. Indien het voor het testen van de TBM-oplossing noodzakelijk is om productiegegevens te gebruiken dan moeten beveiligingsmaatregelen, gelijk aan die van de Productie-omgeving, getroffen worden en moet er een door de Opdrachtgever ondertekende Waiver overlegd worden. Deze Waiverprocedure wordt vastgelegd in een DAP met de Belastingdienst.

GUE 59.	De TBM-oplossing voldoet aan encryptie-algoritmes en sleutelsterkte zoals geadviseerd door het NCSC.

Beschikbaarheid, integriteit en vertrouwelijkheid van Gegevens van de Belastingdienst mogen op geen enkele manier gecompromitteerd raken. Van medewerkers van Opdrachtnemer met toegang tot Gegevens en TBM-oplossing wordt vooraf de achtergrond gecontroleerd. Voor Nederlandse ingezetenen wordt gebruik gemaakt van de VOG (algemeen screeningsprofiel, functie-aspecten: 11, 12, 13 en 41).

Voor niet ingezeten kan een gelijkwaardige verklaring worden overlegd. De Opdrachtgever oordeelt over de bruikbaarheid hiervan.

Niet Nederlandse ingezetenen kunnen voor informatie terecht bij Justis. Zie voor meer informatie: https://www.justis.nl/service-contact/veelgestelde-vragen/vog/hoe-kan-ik-een-vog-aanvragen-als-ik-niet-ben-ingeschreven-in-de-brp#:~:text=Sluiten-,Hoe%20kan%20ik%20een%20VOG%20aanvragen%20als%20ik%20niet%20ben,VOG%20rechtstreeks%20bij%20Justis%20aanvragen

en

https://www.rijksoverheid.nl/wetten-en-regelingen/productbeschrijvingen/aanvragen-verklaring-omtrent-het-gedrag-vog-bij-justis

UE 3.	Opdrachtnemer beschikt voor medewerker(s) die werkzaamheden m.b.t. genoemde Gegevens gaan uitvoeren, over een geldige Verklaring Omtrent Gedrag (hierna VOG.) (Zie voor meer informatie artikel 28.5 van de Overeenkomst.)

3.2.1. Gegevens

Gegevens van de Opdrachtgever worden gescheiden verwerkt (waaronder opgeslagen) van andere klanten van Opdrachtnemer: de Opdrachtgever heeft geen zicht in Gegevens van andere klanten, andere klanten hebben geen zicht in die van de Opdrachtgever.

Medewerkers van Opdrachtnemer hebben alleen toegang tot de Gegevens van de Opdrachtgever voor zover dat noodzakelijk is voor het uitvoeren van de Overeenkomst.

UE 4.	Gegevens van de Opdrachtgever worden logisch gescheiden opgeslagen van de Gegevens van andere klanten van Opdrachtnemer.

	Toegang tot deze Gegevens is beperkt tot de Opdrachtgever en –voor zover noodzakelijk voor het uitvoeren van de Overeenkomst- Opdrachtnemer.

Voor bepaalde testsituaties, bijvoorbeeld het testen van importeeracties voor ingebruikname van de TBM-oplossing, kan een uitzondering gemaakt worden. De Opdrachtgever heeft daar dan expliciet toestemming voor verleend en de desbetreffende omgeving is met hetzelfde niveau beveiligd als de Productieomgeving.

UE 5.	Bij het testen van de TBM-oplossing mag geen gebruik worden gemaakt van Productiegegevens, tenzij anders overeengekomen.

De Opdrachtgever maakt gebruik van versleutelde Gegevens bij opslag (encryption-at-rest). Eén van de voordelen is dat als de Gegevens op ongecontroleerde wijze buiten de TBM-oplossing terecht komen, derden geen gebruik kunnen maken van deze Gegevens.

UE 6.	Bij opslag van Gegevens in de TBM-oplossing wordt encryption-at-rest toegepast.

Als de Opdrachtgever dat nodig acht dan kan de Opdrachtgever Opdrachtnemer verzoeken zijn Gegevens of een deel van zijn Gegevens te verstrekken voor verdere verwerking.

Aanleveren van de Gegevens gebeurt via een beveiligd kanaal van de Opdrachtgever in een door de Opdrachtgever bruikbaar digitaal formaat.

UE 7.	Opdrachtnemer levert op verzoek van Opdrachtgever een voor de Opdrachtgever bruikbare digitale kopie van de meest actuele Gegevens en haar structuur. Vertrouwelijkheid en integriteit van de Gegevens blijven geborgd.

3.3. Specifieke Eisen van de Opdrachtgever vanuit beveiligingsperspectief

In deze paragraaf stelt de Opdrachtgever specifieke Eisen vanuit beveiligingsperspectief. Hier zijn ook eisen opgenomen om te borgen dat de Opdrachtgever aan het overheidsinformatiebeveiligingsbeleid (Baseline Informatiebeveiliging Overheid) kan voldoen. 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.

Versleuteling

De Aanbestedende dienst maakt bij voorkeur gebruik van versleutelde Gegevens bij opslag. Eén van de voordelen is dat als de Gegevens op ongecontroleerde wijze buiten de TBM-oplossing terecht komen, andere partijen geen gebruik kunnen maken van deze Gegevens. Ter voorbereiding op quantum computing volgt Opdrachtgever de adviezen van het NCSC en AIVD.

GUE 60.	De Gegevens in de TBM-oplossing zijn conform marktstandaarden (de richtlijnen van de AIVD en NCSC zijn hierbij leidend) encryption-at-rest en encryption-in-transit versleuteld.

GUE 61.	Data-at-rest is versleuteld in de TBM-oplossing opgeslagen.

GUE 62.	Data-in-transit is altijd versleuteld in de TBM-oplossing; hierbij is minimaal TLS 1.3 het uitgangspunt.

UE 8.	Opdrachtnemer heeft mitigerende maatregelen getroffen voor situaties waar verwerkte Gegevens in verkeerde handen belanden, en daarmee veiligheidsrisico's opleveren.

UE 9.	Opdrachtnemer heeft mitigerende maatregelen waarmee continuïteitrisico's bij het onbeschikbaar zijn van de TBM-oplossing wordt ondervangen.

UE 10.	Opdrachtnemer heeft mitigerende maatregelen waarmee voorkomen wordt dat Personeel van de Opdrachtnemer toegang heeft tot de (de Gegevens in de) TBM-oplossing van Opdrachtgever.

UE 11.	Als Personeel van Opdrachtnemer noodzakelijkerwijs toegang tot de (de Gegevens in de) TBM-oplossing van de Opdrachtgever moet hebben, dan wordt dit alleen toegestaan na uitdrukkelijke toestemming van Opdrachtgever.

3.3.1. Forum Standaardisatie

De Belastingdienst is als overheidspartij gehouden aan de standaarden, zoals vastgesteld door het Forum Standaardisatie. 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).

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 12.	Opdrachtnemer committeert zich aan het gebruik van de streefbeeldafspraken informatieveiligheid van het Forum Standaardisatie (https://www.forumstandaardisatie.nl/onderwerpen/veilig-internet/streefbeeldafspraken) in relatie tot de TBM-oplossing.

UE 13.	Opdrachtnemer committeert zich aan het gebruik van de Verplichte standaarden van het Forum Standaardisatie in relatie tot de TBM-oplossing. Het betreft de volgende standaarden: 1. HTTPS en HSTS; 2. OpenAPI Specification 3.0; 3. TLS 1.3; 4. OpenID, OAuth en SAML (Authenticatie); 5. DNSSEC; 6. IPv4 en IPv6.

UE 14.	Opdrachtnemer is akkoord met het toepassen van wijzigingen op basis van aanpassingen bij het Forum van Standaardisatie.

Het is mogelijk dat tijdens de looptijd van de Overeenkomst er wijzigingen optreden in de lijst met Open Standaarden. In een dergelijk geval treden partijen in overleg wat hiermee te doen.

UE 15.	Opdrachtnemer is akkoord om in overleg te treden als de lijst Open Standaarden wijzigt.

GUE 63.	De TBM-oplossing biedt de mogelijkheid om voor alle webverbindingen van de TBM-oplossing HTTPS en HSTS toe te passen conform de richtlijnen van het NCSC. Hierbij geldt dat alleen gebruik gemaakt wordt van standaarden en instellingen die door het NCSC als 'Goed' zijn gekwalificeerd ("ICT-beveiligingsrichtlijnen voor Transport Layer Security") en moet op de 'Qualys SSL Labs SSL Server Test' minimaal een A- worden behaald. Zie https://www.ssllabs.com/ssltest/index.html.

GUE 64.	De TBM-oplossing is transparant voor zowel IPv4 als IPv6.

GUE 65.	De TBM-oplossing biedt de mogelijkheid om voor elke domeinnaam van de TBM-oplossing, voor communicatie met bedrijven die werkzaamheden voor IV uitvoeren, gebruik te maken van DNSSEC. De domeininformatie, zoals bijbehorende IP-adressen, is met een geldige DNSSEC-handtekening ondertekend.

3.3.2. Richtlijnen rond Beveiligingsincidenten en ontdekken Kwetsbaarheden

3.3.2.1. 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.

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 CERTs (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 4.0). 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 TBM-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 TBM-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 Problem;
- Laag risico (Low risk, 0.1 – 3.9): 6 maanden. Voor de Opdrachtgever is dit een Problem.

De Opdrachtgever 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 Oplostijd (beperkt) op te rekken. Dit kan alleen met nadrukkelijke instemming van de Opdrachtgever.

De Opdrachtgever kan besluiten dat Gegevens onbeschikbaar gemaakt moeten worden en dat de TBM-oplossing geheel dan wel gedeeltelijk onbeschikbaar gemaakt moet worden voor derden. Staat de TBM-oplossing nog niet in productie dan zal in productie name niet mogen totdat de Kritische-en Hoge risicobevindingen zijn weggenomen.
Bekende Kwetsbaarheden worden onverwijld gemeld.

Gemiddeld- en Laag risicobevindingen 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 Oplostijd. 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 Opdrachtgever om akkoord te gaan met een Leg-uit. Indien geen akkoord dan zullen de acties met bijhorende planning opgenomen worden in het Verbeterplan.

UE 16.	Opdrachtnemer conformeert zich aan de door de Opdrachtgever gebruikte methode (CVSS4.0) om Incidenten te kwalificeren en heeft zijn organisatie zodanig ingericht dat de door de Opdrachtgever onderkende typen Beveiligingsincidenten voor (onderdelen) van de TBM-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.

Opdrachtnemer stelt de TBM-oplossing ook aan derden beschikbaar. Indien in dergelijke instances zich inbreuken op beveiliging en/of privacy voordoen, die zich ook kunnen voordoen in de aan de Opdrachtgever geleverde TBM-oplossing, dan wordt de Opdrachtgever daarvan onverwijld van op de hoogte gebracht om zo nodig mitigerende maatregelen te kunnen treffen. Opdrachtgever monitort dit actief.

Het gaat niet alleen om opgetreden (Beveiligings) Incidenten, maar ook om mogelijke toekomstige (Beveiligings)Incidenten waar Opdrachtnemer van kan uitgaan dat deze in de (nabije) toekomst kunnen optreden. Denk aan een zero-day exploit.

Het gaat de Opdrachtgever om het (technisch) inhoudelijke (Beveiligings)Incident om deze te kunnen analyseren en, zo nodig, mitigerende maatregelen te treffen. Er worden nadrukkelijk geen bedrijfsgegevens van getroffen partijen gedeeld.

Opdrachtnemer zal in dat geval tevens de omvang van het (Beveiligings)Incident aangeven, de verwachte consequenties voor de Opdrachtgever, alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken.

UE 17.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. inbreuken op Beveiliging in de TBM-oplossing bij derden. Het proces hiervoor moet worden beschreven in een DAP met de Belastingdienst.

Beveiligingsincidenten moeten direct gemeld kunnen worden bij zowel Opdrachtnemer als de Opdrachtgever. Er is 24/7 een loket waar Beveiligingsincidenten gemeld kunnen worden en van

waaruit actie genomen kan worden om het incident verder af te handelen.
Dit is ook van toepassing op meldingen voor wat betreft inbreuk op persoonsgegevens. Inschrijver heeft hier een proces voor ingericht.

Elk Beveiligingsincident wordt in eerste instantie als prioriteit 1-incident beschouwd. De Opdrachtgever wordt hiervan per direct op de hoogte gesteld.

Zie voor meer informatie Tabel 3 Service Levels Helpdeks en Incidentmanagement in paragraaf 10.3.1.3.

3.3.2.2. Coordinated Vulnerabilty Disclosure

De Opdrachtgever heeft een Coördinated Vulnerabilty Disclosure-procedure (CVD-procedure). Goedwillende beveiligingsonderzoekers kunnen via een vastgesteld proces Kwetsbaarheden, mits er geen wetten worden overtreden, melden. Het CVD-proces is op deze pagina beschreven: https://www.belastingdienst.nl/security#coordinated-vulnerability-disclosure.

Het NCSC heeft hier richtlijnen over gepubliceerd: https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/besturen/cvd-beleid.

UE 18.	Opdrachtnemer handelt via de Opdrachtgever gemelde CVD-meldingen af conform het CVD-proces van de Opdrachtgever. Dit proces zal door Opdrachtnemer beschreven worden in het DAP.

3.3.2.3. Beveiligingstesten

Inleiding

Beveiligingstesten zijn een belangrijk onderdeel in het stelsel van beveiligingseisen-en maatregelen. De Opdrachtgever stelt eisen aan deze beveiligingstesten. Deze eisen betreffen de testmethode, waardering van de bevindingen, de testende partij, de rapportage en de afhandeling van de Kwetsbaarheden (zie ook paragraaf 3.3.2.1 'Beveiligingsincidenten'.
Deze testen worden uitgevoerd door de Opdrachtnemer en/ of toeleverancier(s).

Er worden periodiek of rond een omvangrijke release beveiligingstesten uitgevoerd op een internet-facing ICT-oplossing. Het betreffen zowel Attack & Penetration testen (minimaal 1 x per jaar) als Vulnerabilty scans. De Opdrachtnemer is de eerstverantwoordelijke om deze beveiligingstesten uit te voeren.

Beveiligings- en continuïteitstesten zijn slechts momentopnamen. Herhaling is dus van belang. Net als het hertesten van geadresseerde bevindingen.

De kosten van uitvoering van dergelijke beveiligingstesten worden gedragen door de partij die conform de eisen uit de Functionals security de beveiligingstest behoort uit te voeren. De andere partij werkt op verzoek kosteloos mee aan dergelijke testen. Onder het kosteloos meewerken, valt onder andere:

- Het beantwoorden van vragen in de verschillende fasen van voorbereiding en uitvoering van een beveiligingstest;
- Het oplossen van bevindingen die uit de beveiligingstesten volgen. Dit is inclusief eventueel benodigd overleg hierover.

De partij die de A&P-test laat uitvoeren bepaalt zelf welke partij de A&P-test uitvoert en wat de inhoud van de A&P-test is. De Opdrachtgever stelt wel eisen aan de kwaliteit van zowel de A&P-test, als de rapportage en het oplosproces van de gevonden bevindingen daarover.

Relevante bevindingen (kwalificatie Kritisch en Hoog) volgend uit de beveiligingstesten zullen tussen de Opdrachtgever en Opdrachtnemer worden gedeeld en zo nodig besproken. Hetzelfde geldt voor plannen van aanpak en Verbeterplannen. Om de A&P-test te kunnen beoordelen wordt het volgende tussen de partijen gedeeld:

- De scope van de test (infrastructuur, middleware, tooling en (API-)koppelingen) is beschreven. Het is duidelijk welke delen van de TBM-oplossing binnen en buiten scope zijn geweest. Het is bekend welke beveiligingsmaatregelen (tijdelijk) uitgeschakeld waren;
- Welke testmethodieken (black-, grey- of crystal boxtesting, wel of niet inclusief broncodereview) zijn gebruikt, en welke normenkaders zijn gebruikt (bijvoorbeeld STRIDE, OWASP Top 10, SANS Top 25, OWASP Mobile Top 10, etc.);
- Hoe getest is; geautomatiseerd, handmatig (worden geautomatiseerd gevonden handmatig geverifieerd?) en wordt er ook door pentesters zelf naar (combinaties van) kwetsbaarheden gezocht;
- Managementsamenvatting met een definitie van de opdracht, relevante kenmerken van de A&P-test, een conclusie en aanbevelingen;
- Alle gevonden Kwetsbaarheden zijn opgenomen in de rapportage met CVSS-waardering. Aangegeven welke versie van CVSS (vanaf 4.0) is gebruikt. Bij voorkeur met de statusaanduiding, bijvoorbeeld “In behandeling” (met plandatum) of “Opgelost (en hertest)”;
- Kwetsbaarheden gekwalificeerd als Kritisch of Hoog risico worden terstond gemeld aan de Opdrachtgever en zo mogelijk tijdens de A&P-test opgelost en hertest...

UE 19.	Opdrachtnemer conformeert zich: - Dat er een veilige TBM-oplossing beschikbaar is gesteld en gedurende de looptijd van de Overeenkomt veilig blijft; - Dit wordt aangetoond middels uit te voeren beveiligingstesten voor in gebruik name en periodiek gedurende de levensduur van de TBM-oplossing; - Dat A&P-testen minimaal één (1) keer per jaar of na een significante wijziging van de TBM-oplossing worden uitgevoerd door een onafhankelijke testpartij; - Dat Vulnerability scans minimaal één (1) keer per maand worden uitgevoerd.

In een Verbeterplan wordt het volgende opgenomen:

- Onderwerp/naam van het Verbeterpunt;
- Startdatum;
- Geplande einddatum oplossing;
- Beoogde aanpak (kort);
- Status;
- Lessons learned;
- De Security Roadmap.

Vulnerability scans

Deze zijn bedoeld om geautomatiseerd te scannen op bekende Kwetsbaarheden. Een Vulnerability scan kan dus met een grote regelmaat worden uitgevoerd. De reden is dat aan de ene kant de TBM--oplossing ge-update wordt en aan de andere kant hackers en beveiligingsonderzoekers constant op zoek zijn naar nieuwe Kwetsbaarheden.

Aanvullend kan de TBM-oplossing tijdens het ontwikkelproces on-the-fly worden getest met daarvoor geschikte hulpmiddelen.

UE 20.	Opdrachtnemer voert minimaal maandelijks een Vulnerability scan uit op de TBM-oplossing conform bovenstaande.

	Hierbij geldt dat de gebruikte tooling, waar Opdrachtnemer zelf in dient te voorzien, gebruik maakt van up-to-date kwetsbaarhedendefinitiebestanden. Op verzoek worden testresultaten, zeker als ze gekwalificeerd zijn als Kritisch of Hoog, gedeeld met de Belastingdienst. Eventuele Kwetsbaarheden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.

UE 21.	Opdrachtnemer conformeert zich aan onderstaande. De gebruikte tooling t.b.v. het uitvoeren van een Vulnerability scan, waar Opdrachtnemer zelf in dient te voorzien, maakt gebruik van up-to-date kwetsbaarhedendefinitiebestanden. Op verzoek worden testresultaten, zeker als ze gekwalificeerd zijn als Kritisch of Hoog, gedeeld met de Belastingdienst. Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.

Beveiligingstestbeleid

De Opdrachtgever wenst inzage in het beveiligingstestbeleid van de TBM- oplossing. Het betreft opzet, bestaan en 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. Hier maken ook voorbeelden van een A&P-testrapport en een Vulnerability testrapport deel van uit.

GUE 66.	Inschrijver beschikt over een beveiligingstestbeleid ten aanzien van de TBM-oplossing dat in bovenstaande informatiebehoefte voorziet. Dit beveiligingstestbeleid wordt in de verificatieperiode bij de beste Inschrijver opgevraagd.

3.3.2.4. Continuïteit en continuïteitstesten

Het is voor de Opdrachtgever van belang is om te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én hoe snel de Gegevens beschikbaar zijn dan wel de TBM-oplossing weer volledig operationeel kan zijn, indien de onbeschikbaarheid toch groter mocht zijn dan gepland. Het gaat hierbij dus niet om de operationele beschikbaarheidseisen (waar het vooral draait om wanneer de TBM-oplossing wel of niet te gebruiken is), maar om de excepties als het mis gaat (Calamiteiten en Back-up & Restore.)

Van Opdrachtnemer wordt verwacht dat de TBM-oplossing bij onbeschikbaarheid binnen bepaalde termijnen weer beschikbaar is zonder verlies van integriteit en vertrouwelijkheid.

UE 22.	Opdrachtnemer conformeert zich aan bovenstaande alinea's.

3.3.2.5. Gegevens en processen veiligstellen

In geval dat de Gegevens of Processen van de Opdrachtgever in gevaar komen, bijvoorbeeld door als Hoog of Kritisch gekwalificeerde Kwetsbaarheden, kan de Opdrachtgever besluiten dat de Gegevens van de Opdrachtgever veiliggesteld moeten worden door:

- De Gegevens van de Opdrachtgever voor derden ontoegankelijk te maken en/of
- (Relevante delen van) de TBM-oplossing voor derden onbeschikbaar te maken.

Opdrachtnemer werkt, daar waar relevant, mee bij:

1. Exportacties van Gegevens indien het proces via een andere TBM-oplossing/procedure voortgezet dient te worden bij de Opdrachtgever;
2. Het onbeschikbaar maken van (delen van) de TBM-oplossing of de Gegevens (dit is inclusief andere portalen en koppelingen).

De TBM-oplossing wordt weer in productie (on-line) gebracht na toestemming van de Security Officer van de Opdrachtgever. Gegevens en processen zijn hierbij weer conform afspraken beschikbaar.

UE 23.	Opdrachtnemer conformeert zich aan bovenstaande. Tussen het inroepen van de actie om Gegevens en processen veilig te stellen en het afronden van de uitvoering mag maximaal 4 uur verstrijken. De acties om de Gegevens en processen veilig te stellen worden direct na binnenkomst van het verzoek in gang gezet. Gegevens worden alleen via een beveiligd kanaal uitgewisseld. Zowel integriteit als vertrouwelijkheid zijn geborgd.

Het weer beschikbaar maken van de TBM-oplossing (Reinstate) houdt in dat de TBM-oplossing weer in productie wordt gebracht met gebruikmaking van de meest actuele Gegevens. Dit is inclusief importacties van de Gegevens indien het proces via een andere oplossing/procedure voortgezet is geweest.

Speciale aandacht hierbij voor de situatie dat Gegevens van voor het stopzetten van de TBM-oplossing samengevoegd moeten worden met de Gegevens die in de tussentijd mogelijk elders zijn gegenereerd. Integriteit en vertrouwelijkheid van de Gegevens blijven te allen tijde geborgd.

UE 24.	Op aangeven van een Security Officer van de Opdrachtgever wordt de TBM-oplossing weer ter beschikking gesteld, zodat Gegevens en Processen weer conform afspraken beschikbaar zijn. Opdrachtnemer werkt mee met het opnieuw in gebruik nemen van de TBM-oplossing, waarbij vertrouwelijkheid en integriteit van de Gegevens gewaarborgd is. Ook als er integratie van Gegevens van de TBM-oplossing met Gegevens die tijdens de onbeschikbaarheid zijn gegenereerd, moet plaatsvinden.

De Aanbestedende dienst vindt het van belang dat zijn Gegevens veilig zijn. Gegevens moeten Beschikbaar zijn, maar ook betrouwbaar (niet onbevoegd gewijzigd) en alleen toegankelijk voor de personen die die Gegevens daadwerkelijk nodig hebben.

UE 25.	Opdrachtnemer heeft (technische) maatregelen getroffen om te voorkomen dat Gegevens van de Opdrachtgever geleverd (kunnen) worden aan andere partijen die niet onder Nederlandse en/of Europese wetgeving vallen; Dit betekent dat Gegevens alleen worden verwerkt in lidstaten van de EU of een land met een door de EU goedgekeurd beveiligingsniveau én deze landen niet verlaten.

3.3.3. Monitoring, Alerting en Logging

De Opdrachtgever heeft zicht in afwijkende/verdachte activiteiten binnen de TBM-oplossing om herstelacties te kunnen formuleren en zo mogelijk in de toekomst te voorkomen. Denk aan (ongeautoriseerde) toegang tot de TBM-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 TBM-oplossing (inclusief raakvlaksystemen en tooling) wordt volcontinu gemonitord 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. Beveiligingsinbreuken worden daarnaast gelogd voor forensisch onderzoek.

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

GUE 67.	Logbestanden zijn beveiligd tegen ongeautoriseerde toegang/wijziging en zijn geschikt om forensisch onderzoek te verrichten. Logbestanden in het kader van technische beveiligingslogging worden minimaal 18 maanden bewaard. Logbestanden die onderdeel uitmaken van forensisch onderzoek naar een beveiligingsincident worden bewaard, zolang het onderzoek niet afgesloten is. Logregels bevatten geen informatie waarmee de beveiliging van de TBM-oplossing gecompromitteerd kan worden.

GUE 68.	Via alerting wordt direct adequaat gereageerd op excepties om de situatie te onderzoeken en eventuele risico's te mitigeren. Onder excepties vallen ook incidenten rond ongeautoriseerde toegang en wijziging van logbestanden.

UE 26.	De TBM-oplossing wordt volcontinu gemonitord en excepties worden gelogd: • Datum en tijd; • IP-adres of hostnaam van het device dat de informatie logt; • IP-adres van het remote systeem (indien met een ander systeem wordt gecommuniceerd); • Identificatie van de Gebruiker of het proces; • Beschrijving van de activiteit of gebeurtenis; • Het resultaat van de activiteit of gebeurtenis. Gebeurtenissen die worden gelogd: • Authenticatie/autorisatie pogingen, inloggen en uitloggen; • Acties die betrekking hebben op gebruikersprofielen, bestanden en databases of systeemservices; • Transacties tussen systemen; • Activatie en/of de-activatie van beveiligingsfunctionaliteit; • Niet gespecificeerd gedrag van systemen en Applicaties (uitzonderingen, fouten en storingen); • Beveiligingsincidenten.

UE 27.	Opdrachtnemer levert op verzoek inzicht in de logging.

GUE 69.	De TBM-oplossing ondersteunt het instellen van loglevels en onderscheidt hier minimaal info-, error- en fatal-meldingen in.

GUE 70.	De TBM-oplossing biedt de mogelijkheid om na een foutsituatie Gegevens te herstellen zodat de gebruiker zijn/haar werk kan hervatten.

3.3.4. Autorisatie en Authenticatie

GUE 71.	Voor authenticatie sluit de TBM-oplossing aan op de Belastingdienst Active Directory via een SAMLv2/OpenID Connect aansluiting op de Federated Identity Hub.

GUE 72.	De communicatie over het netwerk van de wachtwoorden van gebruikers in relatie met de TBM-oplossing is versleuteld.

Toegang tot TBM-oplossing en Gegevens van de Aanbestedende dienst vindt plaats 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 TBM-oplossing. Dit is overigens ook van toepassing op raakvlaksystemen (koppelende applicaties).

Een belangrijk aspect hierbij is dat de technische Beheerders geen toegang krijgen tot data in de Productieomgeving.

De TBM-oplossing is technisch zodanig ingericht zodat deze principes zijn voldaan.

GUE 73.	De TBM-oplossing voldoet aan wat in bovenstaande alinea is beschreven.

GUE 74.	De TBM-oplossing bevat maatregelen om ongeautoriseerde toegang tot de TBM-oplossing uit te sluiten.

De TBM-oplossing 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.

Identificatie, autorisatie en authenticatie heeft alleen betrekking op Gebruikers en niet op bezoekers van een publieke website. Bezoekers kunnen zonder identificatie toegang krijgen tot het openbare gedeelte van een oplossing. Een oplossing heeft alleen een openbaar gedeelte als dit nadrukkelijk geëist is door de Opdrachtgever.

UE 28.	Het beheer van toegangsrechten voor de TBM-oplossing, inclusief de bewaking van functiescheiding en het gebruik van groepsrollen, geschiedt vanuit één door de Opdrachtnemer geboden (logisch) Identity Managementsysteem (IMS).

De Opdrachtgever stelt de volgende algemene eisen aan authenticatie. Zo is het gebruik van intern gebruikte userIDs niet toegestaan (mailadres van werk mag wel). Voor de Opdrachtgever zijn ook minimale vereisten voor wachtwoorden van toepassing.

UE 29.	Als identificatie is het gebruik van het user ID van de Opdrachtgever niet toegestaan.

UE 30.	Wachtwoorden voldoen minimaal aan de onderstaande eisen: a. Gebruik van wachtwoorden wordt geautomatiseerd afgedwongen; b. Initiële wachtwoorden (inclusief de gereset zijn) zijn een Werkdag geldig en worden bij eerste gebruik gewijzigd; c. Eisen aan wachtwoorden worden geautomatiseerd afgedwongen.

	Indien het authenticatieproces is gekoppeld aan dat van de Opdrachtgever dan zijn de richtlijnen van de Opdrachtgever leidend.

GUE 75.	De TBM-oplossing ondersteunt Single Sign-On (SSO) met standaarden zoals SAML of OAuth.

GUE 76.	De TBM-oplossing ondersteunt SAML en SSO authenticatie en rechtenbeheer.

GUE 77.	De TBM-oplossing ondersteunt een RBAC model voor zowel data als functionaliteit.

GUE 78.	De TBM-oplossing kent verschillende autorisatieniveaus.

GUE 79.	De TBM-oplossing ondersteunt MultiFactor Authenticatie (hierna MFA); MFA is voor alle Gebruikers verplicht.

GUE 80.	Authenticatie wordt federatief afgehandeld via EntraID (in combinatie met de standaard MFA-dienst (op dit moment SecurID))

Beheer-toegang (Privileged Access) tot de SaaS dienst wordt bij voorkeur beperkt tot toegang vanaf een Belastingdienst-werkplek.

Toegang tot de management console van de SaaS dienst zal gefaciliteerd moeten worden vanuit het Belastingdienst Privileged Access Management systeem. Dit PAM-systeem biedt 2 mogelijkheden voor het geven van toegang tot de management-console:

1. De wachtwoorden van de gebruikers die toegang krijgen tot de management console van de SaaS oplossing, worden opgeslagen in de digitale kluis. De gebruikers krijgen, na gebruik van de Belastingdienst MultiFactor Authenticatie (MFA), op basis van zijn autorisatie(s), de mogelijkheid om het wachtwoord uit de kluis te kopiëren en in te vullen (‘plakken’) in het inlogvenster van de management-console. Het PAM systeem kan bij voorkeur de wachtwoorden in de TBM-oplossing geautomatiseerd aanpassen.
2. De wachtwoorden van de accounts die toegang krijgen tot de management-console van de SaaS oplossing, zijn opgeslagen in de digitale kluis. Een gebruiker krijgt, na gebruik van de Belastingdienst MultiFactor Authenticatie (MFA), op basis van zijn autorisatie(s) de mogelijkheid om vanaf het PAM systeem een sessie op te zetten naar de management-console. Het wachtwoord wordt door het PAM-systeem uit de kluis gehaald en automatisch ingevuld bij het authentiseren van de sessie. Het PAM systeem kan de wachtwoorden in uw oplossing geautomatiseerd aanpassen.

3.3.5. Koppelingen

Een ICT-oplossing staat zelden op zichzelf, ook niet als het off-premise staat. ICT-oplossingen zijn vaak met andere ICT-systemen binnen de Opdrachtgever gekoppeld. Denk ook aan de kantooromgeving van de Opdrachtgever. Of aan Gebruikers van buiten de Opdrachtgever die de Opdrachtgever toegang wil verlenen tot de ICT-oplossingen.

*Dit gebeurt via een Service Niveau Rapportage (SNR).*van toepassing zijn.

De Opdrachtgever stelt een aantal specifieke eisen die er op gericht zijn organisatorisch en technisch aan te sluiten op de ICT-infrastructuur van Opdrachtgever.

De Opdrachtgever werkt met een standaard werkplek. Alleen goedgekeurde Programmatuur kan vanuit een centraal punt geïnstalleerd worden. In de praktijk komt het erop neer dat naast een

(standaard) webbrowser geen gebruik gemaakt kan worden van additionele Programmatuur (zoals browser plug-ins) of additionele Apparatuur (zoals dongles). Dit noemt de Opdrachtgever een zero-footprint client.

In de praktijk betekent dat dat er gebruik wordt gemaakt van een webbrowser als clientprogramma.

GUE 81.	De TBM-oplossing maakt gebruik van een zero-footprint client en maakt gebruik van een standaard webbrowser.

UE 31.	Benaderen van de TBM-oplossing middels webbrowsers dient ondersteund te worden door webbrowsers die nog worden voorzien van beveiligingsupdates van de ontwikkelaar. Webbrowsers zijn voorzien van de meest recente security patches.

Gegevens worden niet alleen binnen de TBM-oplossing verwerkt. Er zal ook sprake zijn van transport van Gegevens van en naar de TBM-oplossing en mogelijk tussen de verschillende onderdelen binnen de TBM-oplossing, of zelfs Derde partijen. Ook als de TBM-oplossing uit meerdere deel TBM-oplossingen bestaat die niet direct met elkaar gekoppeld zijn, maar bijvoorbeeld via het internet, dan is er sprake van transport van Gegevens in transitie.

Gegevens in transitie worden versleuteld. Versleuteling conformeert zich aan de richtlijnen van het NCSC. Op de website van het NCSC is altijd de meest recente richtlijn te vinden.

GUE 82.	Er wordt gebruik gemaakt van organization validated-certificaten. Voor in gebruik name wordt aan de Opdrachtgever voorgelegd of het certificaat-en het certificaat gebruikt mag worden.

De Opdrachtnemer maakt gebruik van door de Opdrachtgever geaccepteerde methoden en technieken om koppelingen tussen zijn ICT-systemen onderling en zijn ICT-systemen en ICT-oplossingen van opdrachtnemers aan elkaar te koppelen. Ook stelt de Opdrachtgever eisen aan koppelingen van de TBM-oplossing met andere niet-Belastingdienstpartijen.

Denk aan verplichte APIs, versleutelingseigenschappen, en dergelijke.

UE 32.	Alle koppelingen van de TBM-oplossing met zowel systemen van de Opdrachtgever als die van derden, zijn beveiligd.

GUE 83.	De TBM-oplossing ondersteunt een federatief koppelvlak op basis van OpenID Connect en/of SAMLv2.

GUE 84.	De TBM-oplossing sluit, in het kader van Security Monitoring, aan op de SIEM van SOC door aanleveren logging via Splunk Gateway in Cloud Fundament, inclusief definitie van monitoring use-cases.

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 leveranciers. In deze samenwerking speelt u dus een essentiële rol. Opdrachtgever vindt onpartijdigheid en transparantie belangrijk. Daarom maken we afspraken hierover: onze Business Etiquette.

UE 33.	Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage 4 van het Beschrijvend Document.

Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI)

De Belastingdienst heeft ambitie op het gebied van duurzaamheid. Zij wil klanten, behoeftestellers 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 Belastingdienst MVI wil toepassen op deze opdracht vindt u in de volgende paragrafen. Hierin zijn de toepasselijke MVI thema's beschreven.

5.1. Klimaat

Onder dit thema vallen onder andere:

- Energiegebruik;
- CO_2 reductie en
- Duurzame energie opwekking

100% CO_2-compensatie dienstreizen

Nederland moet voor 2030 de helft minder CO_2 uitstoten ten opzichte van 1990, en in 2050 95% procent minder. In het klimaatakkoord staan de maatregelen die sectoren de komende 10 jaar nemen om de doelen voor CO_2-reductie te halen.

Het klimaatakkoord is een onderdeel van het Nederlandse klimaatbeleid. Het is een overeenkomst tussen veel organisaties en bedrijven in Nederland om de uitstoot van broeikasgassen tegen te gaan. Daarmee wordt de opwarming van de aarde beperkt.

Bron: https://www.rijksoverheid.nl/onderwerpen/klimaatverandering/klimaatakkoord/wat-is-het-klimaatakkoord

De Inschrijver kan hier aan bijdragen door o.a. door de vrijgekomen CO_2 vanwege dienstreizen van medewerkers van de Inschrijver voor 100% te compenseren.

W 6	Geef aan of alle vrijgekomen CO_2 vanwege dienstreizen van medewerkers van de Inschrijver die voor de Implementatie, Consultancy en Opleidingen worden ingezet 100% gecompenseerd wordt. Alleen CO_2-credits worden geaccepteerd waarvoor de CO_2-reductie is gerealiseerd conform de richtlijnen van de CDM methodologie. Het Clean Development Mechanism (CDM) stelt eisen aan het vastleggen van de uitgangssituatie en aan de monitoring van een CDM mitigatie project met als doel de hoeveelheid Certified Emission Reductions (CER's) veroorzaakt door het project te bepalen. Deze methodologie is ook van toepassing op Verified Emission Reductions (VER's) en Emission Reduction Units (ERU's).

	Onder CO2-compensatie wordt verstaan: het compenseren van vrijgekomen broeikasgassen (vertaald naar CO2-equivalenten) door het vastleggen van CO2 in bomen of het voorkomen van CO2-uitstoot door het investeren in duurzame energie en/of energiebesparing. Voor CO2-emissiefactoren voor buitenlandse dienstreizen gelden de waarden (well-to-wheel) zoals opgenomen op de website CO2emissiefactoren.nl. De berekeningsmethodiek voor de vliegafstand wordt bepaald m.b.v. de IATA-code tabel. De beoordelingscriteria voor deze Wens is: Alle vrijgekomen CO2 vanwege dienstreizen wordt 100% gecompenseerd 2 punten Niet alle vrijgekomen CO2 vanwege dienstreizen wordt 100% gecompenseerd 0 punten De Inschrijver toont met een onderstaande mogelijke bewijsmiddelen aan dat aan het criterium is voldaan: - Een Gold Standard certificaat (Informatie over Gold Standard is verkrijgbaar via goldstandard.org (Engelstalig)); - Een ander gelijkwaardig certificaat; - Een ander gelijkwaardig bewijsmiddel. Als er geen bewijs wordt ingediend, worden er geen punten toegekend. Voor de beantwoording van deze Wens moet Inschrijver de Bijlage IX Beantwoording Overige wensen.odt gebruiken.

Duurzame energieopwekking

Op de website van PIANOO zijn voorbeelden gegeven met betrekking tot het gebruik van energie uit duurzame bronnen: https://www.pianoo.nl/nl/themas/maatschappelijk-verantwoord-inkopen/mvi-criteria/productgroep-energie .

Hieruit is de volgende Wens ontstaan:

W 7	Geef aan in welke mate het datacenter waarin de Cloud variant van de TBM-oplossing gehost wordt CO_2 neutraal is. Het beoordelingscriterium voor deze Wens is: Van 96 % tot en met 100% 5 punten; Van 91 % tot 95% 4 punten; Van 81 % tot 90% 3 punten; Van 71 % tot 80% 2 punten; Van 61 % tot 70% 1 punten; Van 0 % tot 60% 0 punten. De Inschrijver toont dit met een bewijs aan waaruit blijkt dat aan dit criterium is voldaan. Als er geen bewijs wordt ingediend, worden er geen punten toegekend. Voor de beantwoording van deze Wens moet Inschrijver de Bijlage IX Beantwoording Overige wensen.odt gebruiken.

5.2. Welzijn & Gezondheid

De Belastingdienst heeft het welzijn en gezondheid van eigen personeel hoog in het vaandel. Dit wordt dan ook van de Opdrachtnemer en, indien van toepassing, zijn toeleveranciers verwacht. De inschrijver wordt daarom verzocht te omschrijven op welke wijze dit is ingericht

W 8	Beschrijf in maximaal 2 A4 op welke wijze Inschrijver zorg draagt voor de welzijn en gezondheid van zijn werknemers. Het beoordelingscriterium voor deze Wens is: Medezeggenschap van de medewerker is geregeld 2 punten; Er zijn stimulerende maatregelen getroffen die bijdragen aan de gezondheid van de werknemer 3 punten; Geen van bovengenoemde onderdelen 0 punten. Op deze Wens kunnen maximaal 5 punten worden behaald. Voor de beantwoording van deze Wens moet Inschrijver de Bijlage IX Beantwoording Overige wensen.odt gebruiken.

5.3. Ketenverantwoordelijkheid (ISV)

Internationale verdragen bevatten morele normen over mensenrechten, arbeidsomstandigheden en beloningen. Het voldoen aan sociale aspecten van duurzaam inkopen betekent dat leveranciers zich moeten inspannen dat deze normen in de hele keten van het productieproces worden nagestreefd. De systematiek die hiervoor is ontworpen, noemen we 'sociale voorwaarden'. De fundamentele normen in de verdragen van Internationale Arbeidsorganisatie en de normen in de Universele Verklaring van de Rechten van de Mens, noemen we generieke normen. Zij gelden voor de inkoop van alle producten. Voor sommige productgroepen heeft de Rijksoverheid aanvullende normen gesteld. Met aanvullende normen streven we in die producten een nog grotere verbetering na van arbeidsomstandigheden en beloningen.

Op deze opdracht zijn de generieke sociale voorwaarden van toepassing.

De ingevulde en ondertekende bijlage sociale voorwaarden maakt onderdeel uit van de Overeenkomst.

UE 34.	Opdrachtnemer zal een rapportage conform de sociale voorwaarden (Bijlage 3) op eerste verzoek van de Aanbestedende dienst, maar niet eerder dan na het mededelen van de gunningsbeslissing, invullen en ondertekend aanleveren.

UE 35.	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 2Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: • Opdrachtgever, www.belastingdienst.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.

5.4. Social return, versie 2.0

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, boven op 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, de inzet bij de Implementatie, Consultancy en Opleidingen, 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 36.	Na het tekenen van de Overeenkomst stemmen Partijen binnen 3 maanden na contractafsluiting met elkaar af over de wijze waarop invulling wordt gegeven aan social return.

UE 37.	Tijdens de looptijd van de Overeenkomst besteedt de Opdrachtnemer gedurende de looptijd van de Overeenkomst minimaal 5% van het totaal afgenomen Consultancy en Opleidingen ex. BTW per jaar aan extra werk(ervarings)plaatsen voor mensen uit genoemde social return doelgroepen.

UE 38.	Opdrachtnemer stuurt aan de Opdrachtgever elk half jaar, uiterlijk 15 kalenderdagen na ommekomst van deze periode, geheel ingevuld en ondertekend een periodiek verantwoordingsformulier social return toe. Dit periodiek verantwoordingsformulier social return is opgenomen als Bijlage bij de Overeenkomst.

UE 39.	Wanneer op basis van de periodieke verantwoordingsformulieren de Opdrachtgever constateert dat de Opdrachtnemer gedurende de looptijd van de Overeenkomst

	tweemaal achtereen niet aan de verplichting voldoet zoals beschreven in UE 38, dan kan de Opdrachtnemer in overleg kan treden met Opdrachtgever. Op basis van dit overleg: a) Stellen Partijen de oorzaken vast voor het niet behalen van het genoemde percentage door de Opdrachtnemer; b) Stelt Opdrachtgever maatregelen vast voor het verbeterd nakomen van de verplichting tot social return door de Opdrachtnemer.

UE 40.	Bij het niet nakomen van de verplichting genoemd in UE 38 kan de Opdrachtgever naar rato van de bijdrage social return die de Opdrachtnemer moest doen, betalingen inhouden of storneren op de waarde van de Overeenkomst, met uitzondering in die situaties dat het voldoen aan de verplichting genoemd in UE 38 buiten de schuld van de Opdrachtnemer om niet lukt(e). De bewijslast rust te allen tijde bij de Opdrachtnemer.

Hoofdstuk 6. Juridische kaders

6.1. Concept Overeenkomst

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

6.2. Service Level Agreement & Dossier Afspraken en Procedures

Gedurende de looptijd van de Overeenkomst is een Service Level Agreement (SLA) van toepassing waarin afspraken over verantwoordelijkheden, kwaliteit en beschikbaarheid tussen Opdrachtnemer en Opdrachtgever zijn beschreven. Dit gebeurt op basis van (meetbare) prestatie-indicatoren en kwaliteitseisen.

In een Dossier Afspraken en Procedures (DAP) wordt vastgelegd hoe de Opdrachtnemer en de Opdrachtgever samenwerken. 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.

Voor deze aanbesteding is niet gekozen om een template SLA en DAP mee te sturen, maar deze gezamenlijk na ingang van de Overeenkomst definitief te stellen. In paragraaf 10.3 is hier meer informatie over te vinden.

GUE 86.	Inschrijver gaat akkoord met de werkwijze om na gunning een definitieve SLA en DAP inclusief gevraagde procedures op te stellen.

Hoofdstuk 7. Prijsstelling

7.1. Algemene eisen ten aanzien van Prijzen

In de in Bijlage VIII "Prijzenformulier" geoffreerde Prijzen dienen alle kosten voor de TBM-oplossing of Prestatie 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 toegangscodes voor gebruik van de TBM-oplossing;
- Materialen en Documentatie vereist voor het gebruik van de TBM-oplossing;
- Beveiligingstesten zoals beschreven in paragraaf 3.3.2.3.

UE 41.	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 TBM-oplossing of Prestatie conform de in de Aanbestedingsstukken gestelde eisen én de in de Inschrijving opgenomen beantwoording van de Wensen, kan Opdrachtnemer niet in rekening brengen bij Opdrachtgever.

GUE 87.	Eventuele valutarisico's zijn volledig voor rekening van Opdrachtnemer en worden geacht in de geoffreerde Prijzen te zijn verwerkt.

GUE 88.	Alle geoffreerde tarieven met betrekking tot de Additionele diensten (Consultancy en Opleidingen) zijn inclusief reis- en verblijfkosten.

UE 42.	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”

Het Prijzenformulier is uit verschillende tabbladen opgebouwd. Voor alle tabbladen geldt dat de gele invulvelden ingevuld moeten worden. Hieronder volgt per tabblad een uitleg/toelichting.

Voor het bepalen van de Vergelijkingswaarde moet Inschrijver bij het invullen van het Prijzenformulier uitgaan van de huidige Prijzen en/of Tarieven.

Voor de beoordeling van de beste prijs kwaliteit verhouding wordt echter alleen naar het totaal van de eerste 6 jaren (de initiële looptijd van de Overeenkomst) gekeken.

Het Prijzenformulier moet voor de volledige 14 jaar worden ingevuld, zodat de Opdrachtgever een inschatting heeft van de totale cash-out over de maximale looptijd van de Overeenkomst.

Tabblad Samenvatting

In dit tabblad vult de Inschrijver alleen de naam in; alle overige cellen worden automatisch vanuit de verschillende tabbladen ingevuld.

Tabblad Componenten (van de TBM-oplossing)

In dit tabblad vult de Inschrijver in de gele velden in kolom B uit welke componenten de aangeboden TBM-oplossing bestaat.

Tabblad Dimensionering

In dit tabblad zijn geen invulvelden.
Dit tabblad dient als input voor de overige tabbladen.

Met betrekking tot de dimensionering van gebruikers geldt dat de gebruikers in de Ontwikkel-, Test- en Acceptatieomgeving genoemd, dezelfde unieke gebruikers zijn als in de Productieomgeving.

Tabblad 1 Implementatie & uitrol

In dit tabblad vult Inschrijver 1 (één) bedrag (op basis van een vaste prijs) is met betrekking tot de Implementatie van de TBM-oplossing;

In dit tabblad vult Inschrijver 1 (één) bedrag (op basis van een vaste prijs) in voor 1,5 FTE voor 1 jaar met betrekking tot de uitrol en inrichting van de TBM-oplossing.

Zie voor meer informatie paragraaf 9.1.

Tabblad 2 Gebruik

In dit tabblad vult Inschrijver op basis van de dimensionering in dit tabblad én de overige dimensionering van het tabblad Dimensionering per Blok (cel B28, cel B40 en cel B52) in de gele cellen de licentiegrondslag, kosten per jaar en een eventueel kortingspercentage in. Daarnaast is het mogelijk overige kosten op te voeren.
Als een Blok niet van toepassing is, dan kunt u in de betreffende cel (cel B40 en/ of cel B52) de tekst ‘NVT’ zetten.

Let op!

Bij dit tabblad moet Bijlage VIIIb Toelichting Prijzenformulier worden ingediend met daarin een duidelijke toelichting op de ingevulde bedragen. Hierbij geldt dat de Bijlage VIII Prijzenformulier TBM oplossing leidend is.

Tabblad 3 Additionele diensten

Consultancy

Inschrijver vult m.b.t. de Consultancy in cel C17 een dagtarief in.

Het totaal van alle kosten per jaar wordt automatisch opgeteld en in cel C19 weergegeven en naar het tabblad 'Samenvatting' gekopieerd.

Bonus/malus; zie ook Tabblad Factor

Voor de Aanbestedende dienst is een marktconforme prijsstelling belangrijk. Daarom past de Aanbestedende dienst in deze aanbesteding een methode toe waarbij een fictieve bonus/ malus wordt verkregen op basis van geoffreerde uurtarieven. Omdat de berekening van de fictieve bonus/ malus plaatsvindt op basis van een algoritme zijn de dagtarieven zoals ingevuld in de cel C19 omgerekend naar een uurtarief; deze staat in cel F27. De berekening is geheel geautomatiseerd; Inschrijver hoeft hiervoor niets in te vullen.

Bij een geoffreerd tarief lager dan de referentieprijs wordt een fictieve bonus verkregen. Bij een geoffreerd tarief hoger dan de referentieprijs wordt een fictieve malus verkregen. De fictieve bonus/ malus is progressief variabel en is vastgesteld op maximaal 10%. De fictieve bonus/ malus heeft alleen invloed op de Vergelijkingswaarde van Inschrijver. Gedurende de looptijd van de Overeenkomst vindt verrekening plaats op basis van de door Inschrijver geoffreerde tarieven exclusief de bonus/ malus. Het tabblad "Factor" geeft inzicht in de hoogte van de bonus/ malus.

De berekende bonus/ malus wordt in cel C21 getoond en naar het tabblad 'Samenvatting' gekopieerd.

Opleiding

Inschrijver vult m.b.t. de Opleiding op gegevens van een opleiding/training in voor 40 Gebruikers.

Als deze Opleiding/training kosteloos wordt aangeboden, dient Inschrijver de waarde 'o' (nul) bij de prijs in te vullen.

Het totaal van alle kosten per jaar wordt automatisch opgeteld en naar het tabblad 'Samenvatting' gekopieerd.

Tabblad Factor

Het tabblad "Factor" geeft inzicht in de hoogte van de bonus/ malus. Inschrijver hoeft in dit tabblad niets in te vullen

Tabblad BKP-Grafiek

In cel F9 is de Vergelijkingswaarde, het totaal van de cel D28, van het tabblad 'Samenvatting' overgenomen.
Inschrijver kan in cel F12 een eigen inschatting invullen om te zien hoe de aangegeven waarde van de Inschrijving zich verhoudt tot de inschatting van de Aanbestedende dienst.
Let op! De werkelijke score van de kwaliteit wordt bepaald door de Aanbestedende dienst.

7.3. Specifieke eisen ten aanzien van Prijzen

Het Prijzenformulier dient uitsluitend voor vergelijking van de aanbiedingen en werkt met fictieve volumes over veertien gebruiksjaren. Hierdoor biedt het Inschrijver geen ruimte om inzicht te geven in het onderliggende afrekenmodel van de Inschrijver. Om te kunnen voorspellen en verifiëren wat het werkelijke verbruik kost is inzicht nodig in de wijze waarop de prijs per gebruiksjaar tot stand komt. Daarom wordt van de Inschrijver verwacht dat hij in een toelichting bij de Inschrijving het

volledige afrekenmodel uiteenzet.

In de toelichting moeten de navolgende zaken beschreven worden:

- Soorten grondslagen waarop wordt afgerekend;
- Staffels;
- Wel of geen onderscheid in het gebruik van de TBM-oplossing voor productie en/of test omgevingen.

GUE 89.	Inschrijver levert op basis van bovenstaande via als Bijlage VIIIb een toelichting bij het Prijzenformulier (Bijlage VIIIb). Zowel tekstueel als rekenkundig moeten de geoffreerde jaarbedragen volledig transparant herleidbaar te zijn. De jaarbedragen moeten in verhouding staan tot de genoemde dimensionering en de in het tabblad "Dimensionering' gegeven uitgangspunten. Hierbij moet onder andere gedacht worden aan de grondslag(en) van bijvoorbeeld Abonnementen, Gebruiksrechten of andere gronden, de gebruikte staffels met aantallen, prijstellingen per eenheden (staffel) en de benodigde aantallen en hoe deze correleren met de aangeven dimensionering. **Let op!** Voor staffels geldt dat de Prijs van een component in de opvolgende staffel minimaal gelijk of lager moet zijn dan de voorgaande staffel.

GUE 90.	Het is niet toegestaan om negatieve Prijzen die de gehanteerde berekeningen frustreren of die bij voorbaat objectief niet afzonderlijk kunnen worden nagekomen, te offreren.

7.4. Indexering Prijs

Indexering Gebruik

De door Inschrijver geoffreerde Prijzen voor 'Gebruik', zoals opgegeven in het spreadsheet Prijzenformulier, Bijlage VIII, tabblad '2 Gebruik' mogen alleen geïndexeerd worden als er voor het Gebruik op basis van user wordt aangeboden.

In dat geval mag er geïndexeerd worden vanaf 2028 jaarlijks en steeds jaarlijkse verlengdatum geïndexeerd worden op basis van de CBS-tabel Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2021 = 100 (CPA2008, kwartaalindex), of de opvolger van deze index, conform de volgende webpagina:

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

Prijsaanpassingen dienen uiterlijk voor 1 mei 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 oktober 2025 geïndexeerd had mogen worden, was de prijsindexatie 3,5 % geweest (jaarmutatie DPI 1e kwartaal 2025, meest recent beschikbare indexcijfer).

Indexering Consultancy & Opleiding

De door Inschrijver geoffreerde Prijzen voor de Additionele diensten in de vorm van Consultancy en/of Opleidingen, zoals opgegeven in het spreadsheet Prijzenformulier, Bijlage VIII, tabblad 3 Additionele Diensten, mogen vanaf 2028 jaarlijks en steeds per 1 juni geïndexeerd worden op basis van de CBS tabel 'CAO-lonen, contractuele loonkosten en arbeidsduur, indexcijfers (2020 = 100)'; onderwerp: CAO- lonen incl. bijz. beloningen; SBI2008: I Informatie en communicatie, conform de volgende webpagina:

https://opendata.cbs.nl/#/CBS/nl/dataset/85663NED/table?dl=CF10F

Prijsaanpassingen dienen uiterlijk voor 1 mei 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 oktober 2025 geïndexeerd had mogen worden, was de prijsindexatie 6,3% geweest (jaarmutatie DPI 1e kwartaal 2025, meest recent beschikbare indexcijfer).

UE 43.	De door de Opdrachtnemer geoffreerde Prijzen mogen jaarlijks per 1 juni geïndexeerd worden conform paragraaf 7.4. De eerste indexering vindt plaats niet eerder dan 1 juni 2028.

UE 44.	Opdrachtnemer dient voor 1 mei, voorafgaande aan de genoemde momenten van indexering, een schriftelijk verzoek in met bijbehorende onderbouwing om voor de indexering in aanmerking te komen.

7.5. Toelichting m.b.t. de facturatie momenten

Deze paragraaf dienst als een extra toelichting met betrekking tot de facturatie momenten.

Met betrekking tot de Implementatie gelden de volgende facturatiemomenten:

- 25% van de fixed price bij aanvang en
- 75% van de fixed price bij afronding.

Met betrekking tot de Uitrol en inrichting gelden de volgende facturatiemomenten:

- 80% van de fixed price wordt maandelijks achteraf gefactureerd;
- De overige 20% van de fixed price wanneer alle doelen zijn behaald.

Met betrekking tot het Gebruik geldt het volgende:

Indien de grondslag op basis van IT-spend is, dan is de facturatie (maandelijks) achteraf;

In alle andere gevallen mogen deze periodiek (bij voorkeur maandelijks) vooraf worden gefactureerd; hierbij geldt dat er maximaal 1 (een) jaar vooruit mag worden gefactureerd.

UE 45.	Opdrachtnemer conformeert zich aan bovenstaande facturatiemomenten.

Hoofdstuk 8. Documentatie, Opleiding en Consultancy

8.1. Documentatie

UE 46.	Opdrachtnemer zal Opdrachtgever tijdig voorzien van actuele en volledige Documentatie in elektronische vorm, ten behoeve van de Implementatie van de TBM-oplossing en het gebruik van de Prestatie in de Operationele fase. Hierbij is de Documentatie over de eigenschappen en gebruiksmogelijkheden van de TBM-oplossing in de Nederlandse en/of Engelse taal.

UE 47.	De Documentatie dient zodanig te zijn dat zij een juiste, volledige en gedetailleerde beschrijving geeft van de door Opdrachtnemer te leveren TBM-oplossing en de functies daarvan, zodat Gebruikers op eenvoudige wijze van alle mogelijkheden van de TBM-oplossing gebruik kunnen maken.

UE 48.	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 TBM-oplossing.

UE 49.	Opdrachtgever mag de Documentatie voor gebruik binnen de eigen organisatie reproduceren en wijzigen.

UE 50.	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.

8.2. Opleiding

UE 51.	Opdrachtnemer levert relevante Opleidingen, inclusief Documentatie, inzake het gebruik van de TBM-oplossing, alsmede het functioneel, technisch en applicatief beheer van de TBM-oplossing.

UE 52.	Opleidingen vinden plaats op locatie van de Opdrachtgever tenzij nadrukkelijk anders overeengekomen.

UE 53.	De Opleidingen vinden plaats in Nederland in de Nederlandse taal.

UE 54.	Opdrachtnemer stelt voor de eindgebruikers de goedgekeurde gebruikersinstructie online beschikbaar gedurende de looptijd inclusief verlengingsopties van de Overeenkomst en houdt deze actueel.

UE 55.	Opleiding en ondersteuning dient door deskundigen, die daartoe bekwaam en geschikt zijn, te worden gegeven. In voorkomend geval kan Opdrachtgever voorafgaand aan de

	inzet van de betreffende deskundige(n), overlegging van, of inzage in, relevante diploma's en/of certificaten vorderen.

UE 56.	Lesmateriaal voor Gebruikers is in de Nederlandse en/ of Engelse Taal beschikbaar.

8.3. Consultancy

Binnen de context van deze aanbesteding kan er gedurende de looptijd van de Overeenkomst gebruik worden gemaakt van Consultancy als Additionele dienstverlening.

Van de consultant wordt het volgende verwacht:

De TBM consultant treedt op als:

- Inhoudelijke expert op het gebied van de TBM-oplossing en de optimale inrichting hiervan gegeven de wensen de data van de Opdrachtgever. De consultant adviseert de TBM Office over hoe de TBM-oplossing in te richten en help bij het verzamelen van de juiste gegevens en het oplossen van Gegevensvraagstukken, etc.;
- Inhoudelijk expert op het gebied van TBM, de TBM Office en Taxonomie, de ontwikkeling van TBM en van implementaties van TBM. De consultant adviseert de TBM Office met betrekking tot inrichtingskeuzes, de organisatie van de TBM Office, de taken en verantwoordelijkheden van de collega's in de TBM Office, etc.;
- Begeleider/ coach op het gebied van TBM. De consultant is in staat de leden van de TBM Office en andere medewerkers binnen de Belastingdienst de kennis bij te brengen die ze nodig hebben voor het werken met de TBM-oplossing.

Verwachtingen ten aanzien van de consultant:

- Expertise en kennisdeling;
- Beschikt over aantoonbare ervaring met TBM-frameworks, methodieken en tooling;
- Adviseert over inrichting, Governance en processen die aansluiten bij de organisatiecontext;
- Brengt actuele marktkennis en lessons learned in om risico's te beperken en kwaliteit te waarborgen;
- Diepgaande TBM-expertise (taxonomie, allocatiemodellen, metrics).
- Governance & organisatie-inrichting (TBM Office, RACI);
- Gegevens & administraties (datakwaliteit, verbeterplannen);
- Rapportages & dashboards (KPI's, tooling);
- Enablement (kennisoverdracht, training).

Ondersteuning en begeleiding

- Werkt nauw samen met, en maakt onderdeel uit van, het interne projectteam en fungeert als sparringpartner;
- Faciliteert workshops, kennisoverdracht en training om interne competenties op te bouwen;
- Ondersteunt bij het opstellen van deliverables zoals datamodellen, rapportages en dashboards.

Objectieve advisering

- Adviseert onafhankelijk en in het belang van de Opdrachtgever;
- Signaleert knelpunten en doet proactief verbetervoorstellen.

Resultaatgerichtheid:

- Draagt bij aan het behalen van projectdoelstellingen binnen afgesproken tijd en budget;

- Zorgt dat het interne team na afronding van het project zelfstandig TBM kan toepassen en door ontwikkelen.

Overige verwachtingen:

- Communicatief sterk;
- Analytisch & resultaatgericht;
- Verandermanagement;
- Samenwerking & sparring;
- Planmatig & gestructureerd.

UE 57.	Consultants die ingezet worden voor de Implementatie en/of andere werkzaamheden voldoen minimaal aan het profiel zoals hierboven beschreven.

Hoofdstuk 9. Voorbereiding- en Implementatiefase

9.1. Voorbereiding en verwachting Implementatie

De Opdrachtnemer dient de leiding te nemen bij de Implementatie van de TBM-oplossing. Om inzicht te krijgen op welke wijze de Opdrachtnemer de Implementatie uit gaat voeren, dient de Opdrachtnemer een Implementatieplan van de TBM-oplossing te leveren.

Verwachting Implementatie

Met betrekking tot de implementatie van TBM bij de Opdrachtgever, maakt de Opdrachtnemer onderdeel uit van de interne projectgroep voor de verdere Implementatie van TBM en de TBM-oplossing. Hier wordt gewerkt volgens het principe voordoen, meedoen, zelf doen zodat de Opdrachtgever zelf de regie heeft en een grote rol speelt in de Implementatie van de TBM-oplossing en daarmee de benodigde expertise op het gebied van TBM en de TBM-oplossing zelf opbouwt. De Opdrachtnemer zal hier samenwerken met de projectgroep en de TBM Office en heeft een inspanningsverplichting om bij te dragen aan de doelen van de projectgroep.

Enkele van deze doelen zijn:

- Binnen een jaar na de start van de Overeenkomst van de TBM-oplossing, is meer dan 80% van de IT-spend van de Opdrachtgever geautomatiseerd via de TBM-oplossing inzichtelijk tot op het niveau van de Business Solution applicatie;
- De TBM Office is ingericht en operationeel;
- Continue verbetering van de inzichten vanuit TBM vindt plaats vanuit de TBM Office.

De Opdrachtnemer treedt op als inhoudelijk expert en adviseur binnen het interne projectteam. De Opdrachtnemer ondersteunt bij het realiseren van TBM-implementatie en draagt kennis over, zodat het interne team zelfstandig TBM kan toepassen.

Van de Opdrachtnemer wordt verwacht dat hij volgende rollen in het project invult:

- Inhoudelijke expert op het gebied van de TBM-oplossing en de optimale inrichting hiervan gegeven de wensen de Gegevens van de Opdrachtgever. Opdrachtnemer adviseert het projectteam over hoe de TBM-oplossing in te richten en help bij het verzamelen van de juiste Gegevens en het oplossen van data vraagstukken, etc.;
- Inhoudelijk expert op het gebied van TBM, de TBM Office en Taxonomie, de ontwikkeling van TBM en van implementaties van TBM. Opdrachtnemer adviseert het projectteam met betrekking tot inrichtingskeuzes, de organisatie van de TBM Office, de taken en verantwoordelijkheden van de collega's in de TBM Office, etc.;
- Begeleider/ coach op het gebied van TBM. De Opdrachtnemer is in staat de leden van de TBM Office, het projectteam binnen de Belastingdienst en medewerkers binnen de Belastingdienst de kennis bij te brengen die ze nodig hebben voor het werken met TBM.

Verwachtingen ten aanzien van de consultants die voor Implementatiefase worden ingezet:

- Expertise en kennisdeling;
- Beschikt over aantoonbare ervaring met TBM-frameworks, methodieken en tooling;
- Adviseert over inrichting, Governance en processen die aansluiten bij de organisatiecontext;
- Brengt actuele marktkennis en lessons learned in om risico's te beperken en kwaliteit te waarborgen;
- Diepgaande TBM-expertise (taxonomie, allocatiemodellen, metrics).
- Governance & organisatie-inrichting (TBM Office, RACI);
- Gegevens & administraties (datakwaliteit, verbeterplannen);
- Rapportages & dashboards (KPI's, tooling);
- Enablement (kennisoverdracht, training).

Ondersteuning en begeleiding:

- Werkt nauw samen met, en maakt onderdeel uit van, het interne projectteam en fungeert als sparringpartner;
- Faciliteert workshops, kennisoverdracht en training om interne competenties op te bouwen;
- Ondersteunt bij het opstellen van deliverables zoals datamodellen, rapportages en dashboards.

Objectieve advisering:

- Adviseert onafhankelijk en in het belang van de Opdrachtgever;
- Signaleert knelpunten en doet proactief verbetervoorstellen.

Resultaatgerichtheid:

- Draagt bij aan het behalen van projectdoelstellingen binnen afgesproken tijd en budget;
- Zorgt dat het interne team na afronding van het project zelfstandig TBM kan toepassen en door ontwikkelen.

Overige verwachtingen:

- Communicatief sterk;
- Analytisch & resultaatgericht;
- Verandermanagement;
- Samenwerking & sparring;
- Planmatig & gestructureerd.

Minimumeisen:

- Minimaal 3 jaar TBM-ervaring;
- Minimaal 2 relevante referenties;
- Betrokkenheid bij opstellen Implementatieplan vanuit Opdrachtnemer;
- Ervaring met minimaal 1 implementaties van TBM.

UE 58.	Opdrachtnemer conformeert zich aan bovenstaande met betrekking tot de Implementatiefase.

UE 59.	Opdrachtnemer realiseert binnen 2 maanden na een goedgekeurd Implementatieplan de koppelingen tussen de TBM-oplossing en de applicaties SAP, ServiceNow en Flexera (FNMS). Een koppeling is pas geaccepteerd als er aantoonbaar Gegevens vanuit het bronbestand in de TBM-oplossing is opgenomen.

UE 60.	Opdrachtnemer is gedurende de fase van Implementatie bereid tot overleg en samenwerking met andere partijen van overige systemen.

UE 61.	Opdrachtnemer garandeert dat dat tijdens de Implementatie van de TBM-oplossing er voldoende gekwalificeerd Personeel beschikbaar is en blijft.

UE 62.	Personeel van de Opdrachtnemer die aan de Implementatie van de TBM-oplossing werken mogen alleen ná schriftelijke toestemming van Opdrachtgever vervangen worden door ander gekwalificeerd Personeel.

9.1.1. Implementatieplan TBM-oplossing

GUE 91.	Inschrijver levert bij Inschrijving een (concept) Implementatieplan op, uitgaande van de beschikbaarstelling van de TBM-oplossing op de ingangsdatum van de Overeenkomst. Zie Wens 9 voor de invulling van het Implementatieplan.

W 9	Met betrekking tot bovenstaande alinea's vraagt Opdrachtgever een Implementatieplan waarin Inschrijver beschrijft hoe de TBM-oplossing beschikbaar gesteld wordt en de voorwaarden worden ingericht om veilig te kunnen koppelen en de TBM-oplossing het meest effectief kan worden ingericht om de gestelde doelen te kunnen halen. Voor de Opdrachtgever is het belangrijk dat binnen 1 jaar na de start van de Overeenkomst de volgende doelen zijn behaald: - Minimaal 80% van alle kosten zijn geautomatiseerd via de TBM-oplossing inzichtelijk tot op het niveau van de Business Solution applicatie; - De TBM Office is ingericht en operationeel; - Er continue verbeteringen van de inzichten vanuit TBM vanuit de TBM Office plaatsvinden. Het Implementatieplan bevat minimaal antwoord op hoe Inschrijver de Opdrachtgever in staat stelt de bovenstaande doelen te behalen. De beoordelingscriteria voor deze Wens zijn: - Een beschrijving met inhoudelijke aanpak waarin wordt aangetoond om te komen tot een werkende TBM-oplossing gekoppeld aan de infrastructuur van de Belastingdienst; - Een beschrijving hoe Inschrijver van plan is de genoemde rollen in het projectteam op te pakken; - Een beschrijving met duidelijke projectfasering waaruit blijkt dat een beheerste control op de voortgang mogelijk is; - Een duidelijke opzet t.a.v. (project)Governance die aansluit op de geschetste werkwijze; - Een beschrijving van wat van de Opdrachtgever verwacht wordt om veilig systemen vanuit de Belastingdienst te kunnen koppelen aan de TBM-oplossing; - Een inschatting van de benodigde inzet (projectmanagement, architect, BizDevOps engineer) per deliverable/projectonderdeel, waarbij tevens doorlooptijden worden aangegeven (zowel van Inschrijver als Opdrachtgever); - Een beschrijving van een helder acceptatieproces, waarbij Acceptatie altijd door Opdrachtgever gebeurt op basis van positief verlopen Acceptatietesten; - Een beschrijving hoe Inschrijver het projectteam en de TBM Office in staat stelt zich alle aspecten van TBM eigen te maken en zelfstandig TBM vanuit de run te kunnen verbeteren; - Een beschrijving hoe de Inschrijver de Opdrachtgever en de Gebruikers de benodigde kennis m.b.t. TBM en de TBM-oplossing bijbrengt; - Een overzicht met mijlpalen (Fatale termijnen) met Go or no-Go momenten; - Een beschrijving welke Documentatie wordt opgeleverd; - Een beschrijving van welke Opleidingen voor welke medewerkers (zie Dimensionering van Bijlage VIII Prijzenformulier) benodigd zijn; - Een beschrijving van de 5 belangrijkste risico's en de maatregelen die Inschrijver voorstelt om deze risico's te beheersen. Het Implementatieplan is, exclusief voorblad, inhoudsopgave en afbeeldingen, maximaal 8 pagina's. Hyperlinks en/of verwijzingen naar andere documenten en/of websites zijn niet toegestaan. Het ingeleverde Implementatieplan dient als startpunt om, na gunning aan de betreffende Inschrijver, tot een definitief goedgekeurd Implementatieplan te komen. Voor deze Wens geldt de volgende waardering: 0 Zeer slecht; 10 Slecht; 20 Matig; 85 Voldoende;

	125 Goed; 175 Uitstekend. Zie tabel 3 Beoordeling Wensen uit het Beschrijvend document voor een uitleg bij de beoordeling. Voor de beantwoording van deze Wens moet de Inschrijver de Bijlage IX Beantwoording Wens 9 Implementatieplan.odt gebruiken. **LET OP!!!** Op deze Wens moet er minimaal een score 'Voldoende' worden behaald. Dit is een knock out criterium Als het antwoord op de Wens een Matig of minder scoort, dan leidt tot uitsluiting van de aanbestedingsprocedure.

UE 63.	Na ondertekening van de Overeenkomst zal Opdrachtnemer in goed overleg daartoe binnen 10 (tien) Werkdagen een planning opstellen en na afstemming met Opdrachtgever binnen 10 (tien) Werkdagen een, op basis van het bij de Inschrijving ingediende concept Implementatieplan, definitief Implementatieplan opleveren. De vervolgbepalingen in de Overeenkomst gelden hierbij onverkort.

UE 64.	Het door Opdrachtnemer definitief opgeleverde Implementatieplan dient eerst door Opdrachtgever zoals omschreven in de Overeenkomst te zijn goedgekeurd. Pas na schriftelijke goedkeuring kan worden aangevangen met de Implementatie van de TBM-oplossing.

Competenties van de TBM experts tijdens de Implementatiefase

De Opdrachtgever vindt het belangrijk te weten over welke capaciteiten de experts beschikken die worden ingezet bij de uitrol en de inrichting van de TBM-oplossing. De reden is om er van overtuigd te zijn dat de uitrol en inrichting door gekwalificeerde medewerkers met een goed resultaat wordt uitgevoerd. Voor deze Wens wordt gekeken naar 2 experts die samen meer dan 75% van de werkzaamheden zullen uitvoeren. Per expert moet er minimaal 35% van de totale werkzaamheden worden uitgevoerd.

Voor onderstaande Wens geldt dat alleen de totalen van beide experts apart moeten worden aangegeven.

W 10	Geef voor de beste 2 TBM experts, die het volledige, of overgrote deel van de uitrol en inrichting van TBM bij de Opdrachtgever (ca. 1,5 FTE voor de periode van 1 jaar) gaan uitvoeren, aan over welke aantoonbare ervaring met betrekking tot de onderstaande punten zij beschikken: A. De TBM expert heeft een actieve rol gespeeld in TBM implementaties bij minimaal 2 verschillende opdrachtgevers; B. De TBM expert heeft meerdere trainingen gegeven over TBM aan groepen van meer dan 8 mensen; C. De TBM expert heeft operationele werkervaring als medewerker van het TBM team; D. De TBM expert beschikt over certificaten die specifieke expertise op TBM aantonen; E. De TBM expert heeft meerdere gebruikerstrainingen gegeven over de TBM-oplossing; F. De TBM expert heeft aantoonbare werkervering met de aangeboden TBM-oplossing; G. De TBM expert beschikt over aantoonbare kennis, door middel van certificering, in ITIL, IT4IT en FinOps en koppelt deze kennis aan TBM; H. De TBM expert heeft een projectleidersrol vervuld in TBM implementaties bij minimaal 1 opdrachtgever; I. De TBM expert heeft aantoonbare werkervaring in IT- en financiële rollen.

Onderstaande puntenverdeling geldt voor beide experts bij elkaar opgeteld.
De waardering voor deze Wens is als volgt:

Onderdeel	Criterium	Punten
A	Implementatie bij 1 opdrachtgever	0
	Implementaties bij 2 of 3 verschillende opdrachtgevers	12
	Implementaties bij 4 of 5 verschillende opdrachtgevers	16
	Implementaties bij meer dan 5 verschillende opdrachtgevers	19
B	0 tot en met 2 training gegeven	0
	3 tot en met 5 trainingen gegeven	12
	6 tot en met 10 trainingen gegeven	16
	Meer dan 10 trainingen gegeven	19
C	0 tot en met 2 jaar operationele werkervaring	0
	3 tot en met 4 jaar operationele werkervaring	12
	5 tot en met 8 jaar operationele werkervaring	16
	Meer dan 8 jaar operationele werkervaring	19
D	0 tot en met 2 certificaten	0
	3 tot en met 4 certificaten	6
	5 tot en met 6 certificaten	8
	Meer dan 6 certificaten	10
E	0 tot en met 2 gebruikerstrainingen	0
	3 tot en met 4 gebruikerstrainingen	12
	5 tot en met 9 gebruikerstrainingen	16
	Meer dan 9 gebruikerstrainingen	19
F	0 tot en met 2 jaar werkervaring	0
	3 tot en met 4 jaar werkervaring	17
	5 tot en met 7 jaar werkervaring	25
	Meer dan 7 jaar werkervaring	30
G	0 tot en met 2 certificaten	0
	3 tot en met 4 certificaten	6
	5 tot en met 6 certificaten	8
	Meer dan 6 certificaten	10
H	Geen implementatie in leidende rol	0
	1 implementatie in leidende rol	17
	2 implementaties in leidende rol	25
	Meer dan 2 implementaties in leidende rol	30

I	Werkervaring in alleen IT- of financiële rollen	0
	1 tot en met 2 jaar werkervaring in IT- en financiële rollen	12
	3 tot en met 4 jaar werkervaring in IT- en financiële rollen	16
	Meer dan 4 jaar werkervaring in IT- en financiële rollen	19

Op deze Wens kunnen maximaal 175 punten worden behaald.

Voor de beantwoording van deze Wens moet de Inschrijver de Bijlage IX Beantwoording Wens 10 Competenties.odt. gebruiken.

9.2. Documentatie, Opleiding en Consultancy

UE 65.	Opdrachtnemer levert gedurende de voorbereidings- en Implementatiefase van de Overeenkomst Documentatie, Opleiding en Consultancy conform de eisen zoals neergelegd in Hoofdstuk 8 'Documentatie, Opleiding en Consultancy'.

9.2.1. Opleiding

UE 66.	Opdrachtnemer geeft op aanvraag van Opdrachtgever aan iedere doelgroep, werkzaam in de organisatie van Opdrachtgever (een) passende Opleiding(en) bestaande uit concrete invulling, zoals opleiding, cursus, instructie, product sessies/seminars, etc.

UE 67.	In geval van uitstel of vertraging van de Implementatie van de Prestatie wordt uitgesteld of vertraagd, is Opdrachtgever gerechtigd tot wijziging van de tijdstippen, dan wel wijziging van het aantal personeelsleden te verlangen dat aan de Opleiding deelneemt.

Hoofdstuk 10. Operationele fase

10.1. Verantwoordelijkheden

De Opdrachtgever voorziet 2 soorten beheer; Technisch en Functioneel.

Opdrachtnemer is verantwoordelijk voor het Technisch beheer.

Opdrachtgever is verantwoordelijk voor het Functioneel beheer en voorziet wel dat hiervoor ondersteuning van Opdrachtnemer noodzakelijk is.

Functioneel beheer: betreft de activiteiten die door de Opdrachtgever worden uitgevoerd om de TBM-oplossing optimaal te laten aansluiten op de informatiebehoefte van de organisatie. Het richt zich op het gebruik, de inrichting en de ondersteuning van de functionaliteit van de oplossing, en omvat onder andere:

- Beheer van gebruikers en autorisaties binnen de TBM-oplossing;
- Inrichting en configuratie van rapportages, dashboards en datamodellen conform de interne informatiebehoefte;
- Afstemming met interne stakeholders over de toepassing en interpretatie van Gegevens;
- Testen en acceptatie van nieuwe functionaliteiten en releases;
- Ondersteuning bij gegevensvalidatie en datakwaliteit;
- Communicatie met de Opdrachtnemer over functionele wensen, incidenten en wijzigingsverzoeken.

Functioneel beheer vormt de schakel tussen de gebruikersorganisatie en de technische werking van de SaaS-dienst, en draagt bij aan een effectieve inzet van de TBM-oplossing binnen de bedrijfsvoering van de Opdrachtgever.

10.2. Logistieke kaders

UE 68.	Opdrachtnemer dient op alle communicatie betreffende orders het inkoopordernummer van de Opdrachtgever te vermelden.

Offerteproces

Voor het lichten van Keuze-elementen en/of herzieningsclausules zoals beschreven in paragraaf 2.5 van het Beschrijvend document wordt een Offertetraject gestart als Prijzen en/of Tarieven niet vaststaan. Na afronding van dit Offerteproces wordt conform artikel 15 een Aanvullende Overeenkomst gesloten. Indien er sprake is van een Wijziging, doorlopen Partijen eerst artikel 10 van de Overeenkomst alvorens - al dan niet - een Aanvullende Overeenkomst wordt aangegaan.

De werkwijze van een Offertetraject is in grote lijnen als volgt:

1. Het IUC Belastingdienst stuurt een aanvraag naar de Opdrachtnemer;
2. Na goedkeuring van de Opdrachtgever op de Offerte accepteert het IUC Belastingdienst de Offerte door middel van een Aanvullende overeenkomst op de Overeenkomst en een Inkoopopdracht.

Het bepaalde in artikel 15 van de Overeenkomst is van toepassing.

UE 69.	Opdrachtnemer conformeert zich aan de werkwijze van een Offertetraject zoals hierboven beschreven

UE 70.	Opdrachtnemer hanteert voor elke Offerte een geldigheidstermijn van minimaal 60 dagen.

UE 71.	Opdrachtnemer levert Offertes alléén via het Inkoopuitvoeringscentrum Belastingdienst aan.

10.3. Onderhoud & Support

Opdrachtnemer is gehouden tot het leveren van Onderhoud en Support ten behoeve van TBM-oplossing. Dit betekent onder andere dat Opdrachtnemer derde lijns Onderhoud en Support levert bij Incidenten. Het Onderhoud en Support in de eerste en tweede lijn wordt namelijk door de Opdrachtgever zelf uitgevoerd.

De Opdrachtgever sluit met de Opdrachtnemer een Service Level Agreement (SLA) af aangaande het te leveren Onderhoud en Support. De SLA bevat een beschrijving van de vastgestelde normen in de vorm van Service Levels.

In het SLA moeten, naast alle in de aanbestedingsstukken gevraagde Service Levels, de navolgende onderwerpen benoemd worden:

- Doel en scope van het document;
- Benoeming partijen, verantwoordelijkheden en werkingsgebied;
- Aanvang, looptijd, wijzigingsbeleid, vaststelling en ondertekening;
- Gerelateerde documenten;
- Beschrijving en scope van de dienstverlening;
- In het kader van informatiebeveiliging:
  - Servicedesk (melding en oppakken prio 1-security incidenten) 100%, Initieel terugkoppelmomenten prio 1 security incidenten, contactpersonen;
  - Change-en releasemanagement (waaronder security patches en significante juridische en infrastructurele wijzigingen);
  - Continuïteit (BCM): planning en excepties back-up/restore, calamiteiten;
  - Securitymanagement;
  - Incident- en problemmanagement (mede op basis van CVSS termijnen);
  - Audits, beveiligingstesten (A&P-testen, vulnerability scans) en continuïteitstesten (Back-up & Restore, Calamiteitentests) en beveiliging tijdens overige testen;
  - Monitoring, alerting en logging;
  - Veiligstellen van Gegevens en processen;
  - Certificering(en): <benoem de certificeringen> (of vergelijkbaar), audits en beveiligings-en continuïteitstesten (inclusief aanvraag, afstemming over en adresseren resultaten).
- Rapportage

Rapportage

Opdrachtnemer rapporteert maandelijks in ieder geval over het volgende:

- KPI opgeloste beveiligingsincidenten/-problems (openstaand en status, opgelost en cumulatief 14 maanden);
- 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;
- Verbeterplan (periodieke serviceniveaurapportage en voortgangscontrole uitstaande (oplos)trajecten, relevante wijzigingen in (onderliggende) Programmatuur).

Opdrachtnemer rapporteert jaarlijks in ieder geval over het volgende:

- Wijziging van de Statement of Applicability en/of ISO27001-certificering (of gelijkwaardig).

Opdrachtnemer communiceert jaarlijks de data wanneer onderstaande aspecten plaatsvinden:

- Audits;
- Beveiligingstesten (A&P-testen, kwetsbaarhedenscans);
- Continuïteitstesten (Back-up & Restore, Calamiteitentest).

UE 72.	Opdrachtnemer stelt in overleg met de Aanbestedende dienst na gunning én binnen 3 maanden na het tekenen van de Overeenkomst de SLA op waarin alle, in de aanbestedingsstukken gevraagde onderwerpen zijn opgenomen.

UE 73.	De SLA wordt binnen 3 maanden na het tekenen van de Overeenkomst tussen Opdrachtnemer en Opdrachtgever vastgesteld. Na vaststelling van de versie 1.0 zal deze jaarlijks 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 een Bijlage aan de Overeenkomst worden toegevoegd.

UE 74.	Opdrachtnemer verplicht zich om in overleg met de Opdrachtgever een Governance te beschrijven.

UE 75.	Opdrachtnemer verplicht zich om ten minste Onderhoud te verlenen op de voorlaatste (verse n-1) en nieuwste versie (versie n) van de TBM-oplossing

Dossier Afspraken & Procedures (DAP)

In het DAP moeten, naast alle in de aanbestedingsstukken gevraagde onderwerpen, de navolgende onderwerpen benoemd worden

- Doel en scope van het document;
- Benoeming partijen, verantwoordelijkheden en werkingsgebied;
- Aanvang, looptijd, wijzigingsbeleid, vaststelling;
- Standaard- en escalatiecommunicatiestructuur met rollen en contactgegevens;
- Afspraken en procedures (beveiligings- en privacy incidenten) betreffende:
  - Beschikbaarheid van de Servicedesk;
  - Prioriteriteitsbepaling, reactietijd en oplossingstijd;
  - Melding en afhandeling van incidenten, problems, common vulnerability disclosures en privacy gerelateerde incidenten;
  - Release-en patchmanagement. Releasekalender;
  - Werkwijze inzake Wijzigingen (Op- en afschalen van het gebruik van de TBM-oplossing gedurende de looptijd van de Overeenkomst);
  - Continuïteitstesten (Back-up & Restore, Calamiteitentest);
  - Beschikbaar stelling en afhandeling van rapportages van audits, beveiligingstesten en continuïteitstesten van de Opdrachtnemer;
  - Afspraken rond monitoring, logging en alerting;
  - Wijzigingen van beveiligingsstandaards (Forum van Standaardisatie);
  - Beschikbaar stellen van SLA-rapportages (SNR);
  - Beschikbaarstelling en gebruik van productiegegevens (Retransitie) buiten de Productie-omgeving;
  - Opstellen Verbeterplan;
  - Wijzigingen die de juridische status (bijvoorbeeld rond de AVG) wijzigen;
  - De procedures met betrekking tot Recovery Time Objective en Recovery Point Objective.

Ten aanzien van informatiebeveiliging moeten de onderstaande onderwerpen in het DAP worden beschreven:
- Standaard- en escalatiecommunicatiestructuur met rollen en contactgegevens;
- Afspraken en Procedures (beveiligings- en privacy incidenten) betreffende:
  - Contactpersonen (meldingen, terugkoppelingen en escalatie);
  - Beschikbaarheid van de Servicedesk (24/7);
  - Prioriteriteitsbepaling, reactietijd en oplossingstijd op basis van CVSS;

- Melding (uitgangspunt is wetgeving als AVG en NIS2) en afhandeling van incidenten, problems, common vulnerability disclosures en privacy gerelateerde incidenten;
- Release-en patchmanagement. Releasekalender;
- Uitvoeren van door Opdrachtnemer uitgevoerde beveiligingstesten (A&P, Vulnerability scans) en tests als Qualys SSL Labs, internet.nl en Securityheaders.com;
- Aanvraag, (resultaat van) uitvoering en afhandeling van audits, beveiligingstesten (A&P-test en Vulnerability scan) en continuïteitstesten (Back-up & Restore, Calamiteitentest);
- Beschikbaarstelling en afhandeling van rapportages van audits, beveiligingstesten en continuïteitstesten van de Opdrachtnemer. Afhandeling van het veiligstellen van Gegevens en processen (uitvoeren, herstellen);
- Afspraken rond monitoring, logging en alerting (analyse <afgelopen periode>, excepties (wat wel en niet direct melden);
- Wijzigingen van beveiligingsstandaards (Forum Standaardisatie);
- Beschikbaar stellen van ServiceNiveauRapportages (SNR), Verbeterplannen en Security Roadmaps;
- Beschikbaarstelling en gebruik van productiegegevens (bij onbeschikbaar maken van Gegevens, retransitie) buiten de Productie-omgeving;
- Wijzigingen in de TBM-oplossing (waaronder gebruikte (open source) Programmatuur;
- Wijzigingen die de juridische status wijzigen.

UE 76.	Opdrachtnemer stelt in overleg met de Aanbestedende dienst na gunning én binnen 3 maanden na het tekenen van de Overeenkomst een DAP op waarin alle, in de aanbestedingsstukken gevraagde onderwerpen, zijn opgenomen.

UE 77.	Opdrachtnemer neemt op verzoek deel aan een strategisch-, tactisch- en/of operationeel overleg deel.

10.3.1. Service Levels

10.3.1.1. 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 78.	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 79.	Kwetsbaarheden die leiden tot een Incident worden gekwalificeerd door middel van CVSS 4.0. Op basis van de CVSS 4.0 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.

10.3.1.2. Beschikbaarheid

PI	Service Level
Beschikbaarheid 7x24x365	Minimaal 99% per maand[1]

Tabel 1 Beschikbaarheid

Het is belangrijk te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én hoe snel de Gegevens beschikbaar zijn dan wel de TBM-oplossing weer volledig operationeel kan zijn, indien de onbeschikbaarheid toch groter mocht zijn dan gepland. Het gaat hierbij dus niet om de operationele beschikbaarheidseisen (waar het vooral draait om wanneer de TBM-oplossing wel of niet te gebruiken is), maar om de excepties als het mis gaat (Calamiteiten en Back-up & Restore).

Verwacht wordt dat de TBM-oplossing bij onbeschikbaarheid binnen bepaalde termijnen weer beschikbaar is zonder verlies van integriteit en vertrouwelijkheid.

UE 80.	De TBM-oplossing voldoet ten minste aan de Beschikbaarheid zoals opgenomen in Tabel 1 Beschikbaarheid.

10.3.1.3. 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. 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 TBM-oplossing bij de Opdrachtnemer beschouwd als daadwerkelijke Incidenten.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor • 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 • 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 2 Tabel Impact, Urgentie en Prioriteit

[1] Toelichting: voor gepland Onderhoud geldt maximaal 2 uur per maand.

Prestatie Indicator	Prioriteit	Service Level	Norm
Openstelling Helpdesk (Portal of email)	Incidenten	7 x 24 uur	100%
Openstelling Helpdesk (Telefonisch)	Incidenten	07:00 – 21:00 uur	100% op Werkdagen
Openstelling Helpdesk (Telefonisch, Portal of email)	Beveiligingsincidenten	7 x 24 uur	100% voor Prio 1
Aanmelden Service requests	Laag	Werkdagen van 08:00 – 17:00 uur	100%
REACTIETIJD			
Reactietijd	Prio 1	30 minuten	100%
Reactietijd	Prio 2	60 minuten	100%
Reactietijd	Prio 3	8 uur	100%
Reactietijd	Service request	1 Werkdag	100%
STREEFTIJD[2]			
Streeftijd	Prio 1	4 klokuur	100%
Streeftijd	Prio 2	1 Werkdag	100%
Streeftijd	Prio 3	3 Werkdagen	85%

Tabel 3 Service Levels Helpdeks en Incidentmanagement

UE 81.	Ten aanzien van de Openstelling van de Helpdesk wordt ten minste voldaan aan de Service Levels zoals opgenomen in Tabel 3 Service Levels Helpdeks en Incidentmanagement.

UE 82.	Ten aanzien van de afhandeling van Incidenten en Service requests wordt ten minste voldaan aan de Service Levels zoals opgenomen in Tabel 3 Service Levels Helpdeks en Incidentmanagement.

UE 83.	Indien een Incident niet binnen de Oplostijd wordt opgelost, wordt het Incident geëscaleerd naar de bovenliggende Prioriteit (Prio 3 wordt Prio 2 en Prio 2 wordt Prio 1).

UE 84.	Opdrachtnemer geeft ten aanzien van de afhandeling van beveiligingsincidenten minimaal het volgende aan: - De omvang; - De verwachte consequenties voor de Belastingdienst; - Getroffen en/of te nemen maatregelen. De procedures hiervoor worden in een DAP beschreven.

GUE 92.	De voertaal op de Helpdesk is Nederlands en/of Engels.

[2] Hierbij geldt dat tenminste de analyse en een beschikbare Workaround binnen de gestelde doelen plaatsvindt.

GUE 93.	Het is mogelijk om Incidenten en/of Problems via meerdere kanalen, bijvoorbeeld via de Self service portal of mail, aan te melden.

10.3.1.4. Release – en Patch management

GUE 94.	Inschrijver heeft Patchmanagement ingericht. De bedrijfsvoering is zodanig ingericht dat technische kwetsbaarheden adequaat worden ontdekt, geëvalueerd en geadresseerd.

UE 85.	Opdrachtnemer informeert Opdrachtgever periodiek over nieuwe Releases ten behoeve van het optimaal gebruik van de TBM-oplossing en de daarbij verwachte Impact voor Opdrachtgever.

UE 86.	Het doorvoeren van Releases en Patches ten behoeve van het optimaal gebruik van de TBM-oplossing wordt in overleg met Opdrachtgever ingepland.

UE 87.	Opdrachtnemer levert voorafgaand aan de Release ten behoeve van het optimaal gebruik van de TBM-oplossing de releasenotes ten behoeve van Acceptatie(test).

UE 88.	Gedurende de Overeenkomst is er voor Opdrachtgever een actuele Release kalender van de TBM-oplossing beschikbaar.

UE 89.	Opdrachtnemer informeert Opdrachtgever minimaal 1 jaar voorafgaande aan de datum wanneer (delen van) de TBM-oplossing EOD en/of EOL en/of EOS zijn. In het DAP worden afspraken gemaakt op welk tijdstip Opdrachtgever hierover geïnformeerd wordt.

GUE 95.	De TBM-oplossing beschikt over een geautomatiseerd voortbrengingsmechanisme t.b.v. Functionele Inrichtingen. Voorbeeld: In de Testomgeving wordt bijvoorbeeld een workflow ontwikkelt; deze kan dan geautomatiseerd worden voortgebracht naar de productie omgeving.

10.3.1.5. Business Continuity management (BCM)

In geval van Calamiteiten wordt van Opdrachtnemer verwacht dat de TBM-oplossing bij onbeschikbaarheid binnen bepaalde termijnen weer beschikbaar is zonder verlies van integriteit en vertrouwelijkheid. Het gaat hierbij dus niet om de operationele beschikbaarheidseisen (waar het vooral draait om wanneer de TBM-oplossing wel of niet te gebruiken is), maar om de excepties als het mis gaat (Calamiteiten). Zie ook Tabel 3.

UE 90.	De TBM-oplossing voldoet aan onderstaande eisen betreffende de operationele continuïteit in geval van een Calamiteit (crisis): • Recovery Time Objective (RTO): De TBM-oplossing is binnen 24 (vierentwintig) klokuren weer volledig functioneel beschikbaar; • Recovery Point Objective (RPO): Er is maximaal 24 (vieren twintig) klokuren verlies van Gegevens toegestaan.

UE 91.	Opdrachtnemer test minimaal jaarlijks of na een grote wijziging om de goede werking van de TBM-oplossing te waarborgen in geval van Calamiteiten.

10.3.1.6. Verbeterplan

UE 92.	Indien de TBM-oplossing voor een periode van drie (3) maanden niet voldoet aan één of meerdere Service Levels levert Opdrachtnemer hiervoor een Verbeterplan, inclusief een bijbehorend implementatievoorstel, 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.

UE 93.	Opdrachtnemer conformeert zich dat in een Verbeterplan met betrekking tot Informatiebeveiliging, waarin alle niet conform standaard afspraken opgeloste beveiligingszaken opgenomen zijn, in ieder geval onderstaande onderwerpen worden opgenomen: - Naam van Verbeterpunt; - Beschrijving; - Startdatum; - Geplande einddatum; - Beoogde aanpak (kort, inclusief risico's en benodigde toestemmingen); - Status; - Beschreven oplossing/Lessons learned; - Archief van afgesloten verbeterpunten; - Wijziging in het Verbeterplan; deze wordt direct gecommuniceerd.

10.3.2. Rapportage

UE 94.	Opdrachtnemer levert maandelijks een Service Level rapportage op aan de Opdrachtgever met minimaal de volgende inhoud: • Helpdesk: Reactietijden per Prio; • Beschikbaarheid; • KPI incident management; • KPI Helpdesk; • Performance rapportage; • Licentie gebruik.

UE 95.	Opdrachtnemer overlegt minimaal eenmaal per jaar aan Opdrachtgever het schriftelijk bewijs dat zij aan haar verplichtingen heeft voldaan betreffende het nemen van de gestelde securitymaatregelen en de geëiste verbeteracties (zoals gedefinieerd in dit document). Als bewijs hiervoor kunnen certificeringen en/of uitkomsten van kwetsbaarheidsonderzoeken, A&P testen en/of calamiteitstesten dienen.

UE 96.	Met betrekking tot informatiebeveiliging rapporteert Opdrachtnemer periodiek over onderstaande onderwerpen: - KPI opgeloste beveiligingsincidenten/-problems;

	- Status, voortgang en afhandeling van openstaande en opgeloste; 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 trendanalyse; - Resultaat van tests als: Qualsys SSL Labs, internet.nl en securityheaders.com. Opdrachtnemer conformeert zich verder inzage te geven in de geplande datum en het resultaat van: - Audits, ISO 27001-certificering (of gelijkwaardig); - Wijziging van de Statement of Applicability); - Beveiligingstesten (A&P-testen, Vulnerabilty scans); - Continuïteitstesten (Back-up & Restore, Calamiteitentest).

10.4. Documentatie, Opleiding en Consultancy

UE 97.	Opdrachtnemer levert gedurende de operationele fase van de Overeenkomst Documentatie, Opleiding en Consultancy conform de eisen zoals neergelegd in Hoofdstuk 8 'Documentatie, Opleiding en Consultancy'.

10.5. 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 leverancierspportaal.

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/

Leverancierspportaal

U kunt ook gebruik maken van het e-factuurportaal van de Rijksoverheid, het leverancierspportaal. 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 leverancierssportaal. Het huidige leverancierssportaal van DigiInkoop wordt vervangen. U wordt tijdig geïnformeerd over de overgang naar het nieuwe leverancierssportaal.

UE 98.	De Opdrachtnemer voldoet, conform Bijlage 5 Bijsluiter e-factureren juli 2022, aan de vereisten van e-facturatie via het leverancierssportaal of een geautomatiseerde koppeling met de DigiPoort (toekomstig E-procurementpoort) of het Peppol netwerk met daarin de referentie naar de inkooporder en de inkooporderregel. Zie ook https://www.helpdesk-efactureren.nl/bijsluiter voor de meest actuele informatie.

UE 99.	Kosten die voortkomen uit het realiseren van de koppeling voor elektronische berichten uitwisseling met de Rijksoverheid worden gedragen door de Opdrachtnemer.

UE 100.	Opdrachtnemer vermeldt het inkooporderнummer als referentie op elke pakbon en factuur aan Opdrachtgever. Zonder dit Inkooporderнummer kan Opdrachtgever de levering of de factuur weigeren.

UE 101.	Opdrachtnemer is verantwoordelijk voor de implementatie aan haar zijde. Op verzoek van Opdrachtgever kunnen wijzigingen in het implementatieplan en/of implementatie worden aangebracht die invloed hebben op het bestelproces. Hieronder valt in ieder geval het inzetten van extra expertise.

UE 102.	Opdrachtnemer accepteert dat er gedurende de looptijd van de Overeenkomst nieuwe-/verbeterde versies van de programmatuur van het leverancierssportaal in gebruik genomen kunnen worden.

10.6. Kaders voor (re)transitie

10.6.1. Inleiding

In geval van (tussentijdse) beëindiging of afloop van de Overeenkomst van de TBM-oplossing, dient de Opdrachtnemer te 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.

Een en ander hierover wordt, conform art 38.3 van de Overeenkomst, in een Retransitieplan vastgelegd.

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

Hierbij zal in ieder geval het maximaal aantal uren of dagen benodigd voor de Retransitie worden overeengekomen tussen de Opdrachtnemer en Opdrachtgever. De geldende Prijs is gebaseerd op de aangeboden Prijzen voor Additionele diensten in de vorm van Consultancy, zoals ingevuld in Bijlage VIII Prijzenformulier en toegelicht in Bijlage VIIIb Toelichting Prijzenformulier.

10.6.2. Documentatie en Gegevens(overdracht)

UE 103.	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, noodzakelijk is voor een succesvolle Retransitie waarbij de continuïteit van de Prestatie gewaarborgd blijft. Hierbij wordt, indien noodzakelijk, een Retransitieplan opgesteld door de Partijen, waarvoor de (Uitvoerings)eisen uit het hoofdstuk leidend zijn.

UE 104.	Opdrachtnemer verleent volledige medewerking aan de Retransitie en verstrekt daarbij alle relevante Documentatie aan Opdrachtgever c.q. opvolgende opdrachtnemer.

UE 105.	Aanlevering van de Documentatie gebeurt via een beveiligde verbinding. Opdrachtgever draagt zorg voor deze verbinding.

UE 106.	De ter beschikking gestelde Gegevens dienen te zijn voorzien van een zodanige functionele - en technische beschrijving dat in de toekomst een datamigratie naar een nieuwe oplossing kan plaatsvinden zonder verdere tussenkomst van de Opdrachtnemer.

UE 107.	Opdrachtnemer verstrekt op verzoek van de Opdrachtgever gewenste Gegevens in een voor de Opdrachtgever bruikbaar (digitaal) formaat voor verdere verwerking. De procedure hiervoor moet worden beschreven in een DAP met de Belastingdienst.

UE 108.	Na ontvangst van bevestiging dat de Gegevens in goede orde zijn ontvangen, zal de Opdrachtnemer overgaan tot vernietiging van onder hem bevindende Gegevens, waarbij de vernietigingshandelingen gedocumenteerd zullen worden.

UE 109.	Opdrachtnemer zorgt dat binnen één (1) maand na afloop van de Retransitie, alle Gegevens in verband met deze Overeenkomst van haar systemen zijn verwijderd, zodat de vertrouwelijkheid van deze Gegevens gewaarborgd blijft.

UE 110.	De rapportage van de vernietigingshandelingen is in overeenstemming met wettelijke vereisten ter zake en wordt door Opdrachtnemer aan Opdrachtgever ter hand gesteld.

UE 111	Op eerste verzoek van Opdrachtgever overlegt Opdrachtnemer een door een onafhankelijk IT-auditor of accountant gecertificeerde verklaring van vernietiging waaruit blijkt dat alle Gegevens in verband met deze Overeenkomst zijn gewist. In de verklaring is aangegeven hoe de Gegevens zijn vernietigd (bijvoorbeeld: twee keer overschreven met vaste Gegevens en één keer met random gegevens of met Programmatuur zoals beschreven op: https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten. De procedure moet worden beschreven in het DAP.

UE 112.	Naar de Belastingdienst herleidbare domeinnamen en URL's worden onbeschikbaar gemaakt op het internet en domeinnamen worden –zo mogelijk- overgedragen aan de Belastingdienst.

UE 113.	Hergebruik van de domeinnamen en URL's is niet toegestaan zonder nadrukkelijke toestemming van de Opdrachtgever.

10.6.3. (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 114.	Bij overgang naar een nieuwe opdrachtnemer moet de Prestatie voor een periode van 12 maanden tegen gelijkblijvende condities (naar rato), voor Opdrachtgever beschikbaar blijven.

UE 115.	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 116.	Opdrachtnemer houdt voldoende gekwalificeerd personeel beschikbaar voor de Retransitie.

UE 117.	Opdrachtnemer verleent medewerking aan een Audit betreffende de inhoud en de kwaliteit van de informatie die Opdrachtnemer in het kader van Retransitie beheerd.

UE 118.	Opdrachtnemer dient inzage te geven in de gebruikte middelen en processen tijdens de periode van Retransitie.

UE 119.	Opdrachtnemer dient onder meer de verbindingen te verbreken, eventuele Licenties te verstrekken ten aanzien van TBM-oplossing die noodzakelijk is om de omgeving in stand te houden/te blijven beheren; en elektronische sleutels aan Opdrachtgever ter beschikking te stellen.