Bijlage 2

(Marktconsultatie HR loopbaantesten)

Non Functionele eisen en wensen

versie	**1.0**
datum	**3 september 2018**

Inhoud

1 Non functionele eisen

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Kwaliteit					
	De kwaliteit van de Oplossing wordt bepaald op basis van de ISO25010-norm. De hierin genoemde kwaliteitsnormen zijn gerangschikt naar de daarin genoemde kwaliteitskenmerken. Vanuit de kwaliteitskenmerken zijn eisen en wensen geformuleerd. De norm is aangevuld met specifieke eisen en wensen die voor de Belastingdienst, of rijksoverheden in het algemeen, gelden. Er is voor gekozen om alleen de meest relevante kwaliteitseigenschappen te formuleren. Uitgangspunt hierbij is dat van de Oplossing minimaal een marktconforme kwaliteit wordt verwacht. Zo begrijpt iedereen dat de Responsetijd van een gebruikersactie niet in een ordegrootte van tientallen seconden ligt. De Belastingdienst wil dat de Oplossing logisch uit één geheel bestaat en dat te allen tijde de Inschrijver verantwoordelijk is voor alle functionele en non-functionele gedragingen van de Oplossing. Dit laat onverlet dat de Inschrijver delen van de Oplossing kan en mag onder-uitbesteden naar derden.	De Inschrijver levert de Oplossing als één integraal werkend systeem. Als de Oplossing bestaat uit deeloplossingen dan is de integratie van deze oplossingen de verantwoordelijkheid van de Inschrijver. De Inschrijver garandeert dat, bij gebruik van (deel)oplossingen van eventuele onderaannemers, ook deze partijen en hun (deel)oplossingen aan de in de Aanbestedingsstukken gestelde Kwaliteitsnormen en (Security)eisen voldoen.	X	X	

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Gebruik					
	Onder Gebruik verstaan we de kwaliteit van de prestatie (performance), presentatie en interactie van de Oplossing. Voor wat betreft de prestatie wordt van de Inschrijver gevraagd aan te geven hoe objectief kan worden gemeten dat de prestatie van de Oplossing constant blijft gedurende de looptijd van de Overeenkomst.	De Oplossing kent minimaal 2 normwaarden (bijvoorbeeld Responsetijd van een specifieke veelgebruikte actie) waaraan de prestatie van de Oplossing wordt gemeten. Deze normwaarden worden opgenomen in de concept SLA van de Inschrijver en dienen mede als referentie voor de prestatie van de Oplossing bij vermoedelijke toekomstige problemen omtrent de prestatie van de Oplossing. Over de actuele waarden wordt minimaal eens per kwartaal gerapporteerd.	X	X	X
	De Oplossing zal gebruikt worden door personen met een functiebeperking. De Belastingdienst is verplicht om hier rekening mee te houden. De Oplossing moet hier in zekere mate op ingesteld zijn.	De Oplossing biedt een intuïtieve, marktconforme gebruikersinterface in tenminste de Nederlandse taal.	X	X	
	De Oplossing zal gebruikt worden door personen met een functiebeperking. De Belastingdienst is verplicht om hier rekening mee te houden. De Oplossing moet hier in zekere mate op ingesteld zijn.	De gebruikersinterface voldoet aan de EN 301 549* standaard en biedt hiermee oplossingen voor Gebruikers met een functiebeperking.	X	X	
	De Belastingdienst hecht waarde aan een gelijke presentatie van alle applicaties die door de gebruikers van de Belastingdienst worden gebruikt. De Rijkshuisstijl geldt hierbij als leidraad.	De presentatie aan de Gebruikers is conform de Nederlandse Rijkshuisstijl ingericht (zie www.rijkshuisstijl.nl).	X	X	

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Gebruik					
	Om de Oplossing te kunnen gebruiken is het wenselijk dat er zo min mogelijk aanpassingen op het gebruikersapparaat nodig zijn. De gebruikersapplicatie heeft bij voorkeur een ‘zero-client footprint’, waarbij de volledige toegang via een standaard browser verloopt, zonder het gebruik van applicatie-specifieke toevoegingen (bijv. plug-ins en/of dongles).	Er is geen additionele software nodig, naast een standaard browser, nodig op de gebruikersapparaten nodig om alle gevraagde functionaliteit van de Oplossing te kunnen benaderen.	X	X	
	De Oplossing zal worden gebruikt op een diversiteit van apparaten, besturingssystemen en browsers. Een brede ondersteuning voor de toegang via deze gebruikersapparaten is nodig.	De Oplossing is te gebruiken op gangbare apparaten: desktops, laptops, tablets en smartphones. De Oplossing ondersteunt minimaal de huidige en de voorgaande versie van het Besturingssysteem welke nog actief wordt ondersteund door de leverancier van het Besturingssysteem. De Oplossing ondersteunt de vier meest gangbare web browsers: Google Chrome, Microsoft Internet Explorer/Edge, Mozilla Firefox en Apple Safari. De versies die ondersteund worden zijn gelijk aan de versies die nog actief ondersteunt worden door de leverancier van de web browser. Dit is van toepassing voor de Levensduur van de Oplossing.	X	X	

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Beveiliging					
	De Oplossing van de Inschrijver zal ten aanzien van het beveiligingscertificaat en de configuratie ervan aan een QuickScan worden onderworpen. Deze QuickScan wordt uitgevoerd via de website van Qualsys SSL Labs. Een status van minimaal ‘A’ wordt door de Belastingdienst gezien als een aanvaardbaar veilige Oplossing.	De Oplossing behaalt een A-status (A-, A, A+) bij de SSL/TLS-test van Qualsys SSL Labs. Deze status wordt periodiek, minimaal eens per kwartaal, bevestigd gedurende de Levensduur van de Oplossing.	X		X

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
(Persoons-) Gegevens					
	De Belastingdienst hecht veel belang aan de beveiliging van de (persoons-)Gegevens. De Belastingdienst heeft een taak en verantwoordelijkheid om er voor te zorgen dat (persoons-) Gegevens nooit in onbevoegde handen valt of kan vallen. De Inschrijver dient alle passende en nodige maatregelen te hebben getroffen en te treffen om de Belastingdienst in staat te stellen deze taak uit te voeren en haar verantwoordelijkheid te kunnen nemen. Op basis van de Wet bescherming persoonsgegevens (Wbp), dataclassificaties, een Privacy Impactanalyse (PIA) en een Business Impactanalyse (BIA) zijn eisen geformuleerd ten aanzien van de inrichting, levering en het gebruik van de Oplossing. De Privacy Impact Assessment (PIA) legt in de eerste plaats de risico's bloot die te maken hebben met privacy en dragen bij aan het vermijden of verminderen van deze privacy risico's. Op basis van de antwoorden van de PIA is op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van betrokkene wordt geschaad, hoe hoog deze is en op welke gebieden dit is. De PIA doet dit op gestructureerde wijze door: • de mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen; en • de risico's voor de betrokken personen en organisaties zo veel mogelijk te lokaliseren. Op basis van de uitkomsten van de PIA kunnen gericht acties ondernomen worden om deze risico's te verminderen. Een belangrijk kader in de te nemen beveiligingsmaatregelen is de vigerende wetgeving en standaarden ten aanzien van ICT-beveiliging.	De Oplossing voldoet aan de algemene vigerende Nederlandse Wet- en regelgeving, waaronder de Algemene verordening gegevensbescherming (AVG). De Oplossing voldoet aan de Baseline Informatiebeveiliging Rijksoverheid (BIR) en voldoen aan –daar waar relevant- het Pas-toe-of-leg-uitprincipe dat van toepassing is op organisaties in de publieke sector. Dit betekent dat voldaan wordt aan de Pas-toe-of-leg-uit-lijst van het Forum Standaardisatie. De Oplossing voldoet aan de meest recente beveiligingsprotocollen en algoritmen, waaronder minimaal de ICT-beveiligingsrichtlijnen voor web-applicaties van het National Cyber Security Centre (NCSC). Dit is van toepassing gedurende de Levensduur van de Oplossing.	X	X	X

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
(Persoons-) Gegevens					
	Door ISO 27001 certificering kunt u aantonen dat uw informatiebeveiliging managementsysteem voldoet aan alle normeisen op het gebied van informatiebeveiliging.	De Inschrijver is ISO 27001 gecertificeerd of een minstens gelijkwaardige norm en toont dit jaarlijks aan door middel van een audit dat door een onafhankelijk en algemeen erkend bureau wordt uitgevoerd. De resultaten van de audits worden gedeeld met een door de Belastingdienst aangewezen Contractmanager.	X	X	X
	Door ISO 27001 certificering kunt u aantonen dat uw informatiebeveiliging managementsysteem voldoet aan alle normeisen op het gebied van informatiebeveiliging.	De organisatie(s) die de ICT-voorzieningen van de Oplossing levert en beheert, de datacentra, zijn ISO 27001 of gelijkwaardig gecertificeerd.	X		X
	De Inschrijver zal er op toezien dat maatregelen worden genomen om ononderbroken de beveiliging van de Gegevens te kunnen waarborgen. Hiertoe zal regelmatig worden getoetst of de Oplossing veilig genoeg is en zullen, wanneer de beveiliging moet worden verbeterd, de nodige maatregelen ter verbetering worden uitgevoerd.	De Belastingdienst heeft het recht om minimaal 1 keer per jaar een audit uit te laten voeren om de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de Oplossing te toetsen. De Belastingdienst kiest hierbij zelf welk onafhankelijk en algemeen erkend bureau de audit uitvoert. De resultaten van de audits worden, in de vorm van een Third Party Memorandum, gedeeld met een door de Inschrijver aangewezen Security Officer.	X	X	

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
(Persoons-) Gegevens					
	Een grote bedreiging voor beveiliging van de Gegevens komt van derden, die ongeautoriseerd en ongewenst toegang krijgen tot de Oplossing en/of de Gegevens in deze Oplossing. Door regelmatig een Attack en Penetration test uit te voeren, kan tijdig worden onderkend of de Oplossing voldoende beschermd is tegen deze ongewenste toegang. Daarnaast zal bij elke wijziging een risicoanalyse op het gebied van informatiebeveiliging moeten plaatsvinden. Op basis van de uitkomsten van deze analyse wordt bepaald of naar aanleiding van de wijziging een extra Attack en Penetration moet worden uitgevoerd.	Inschrijver laat minimaal één keer per jaar én bij iedere risicovolle wijziging van de Oplossing op het gebied van informatiebeveiliging een A&P-test uitvoeren door een onafhankelijk en algemeen erkend bureau om de beveiliging te testen. De resultaten van de testen worden gedeeld met een door de Belastingdienst aangewezen Security Officer. De Belastingdienst heeft het recht om een A&P test uit te laten voeren om de beveiliging te testen. De Belastingdienst kiest hierbij zelf een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. De resultaten van de testen worden, in de vorm van een Third Party Memorandum, gedeeld met een door de Inschrijver aangewezen Security Officer.	X	X	X

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
(Persoons-) Gegevens					
	Het inperken van de risico's dat onbevoegden gebruik kunnen maken van kwetsbaarheden in de Oplossing.	Conform beleid van de Belastingdienst is het niet toegestaan dat er kwetsbaarheden, gekwalificeerd door het bureau dat een A&P-test voor de Inschrijver of de Belastingdienst, als Kritisch (Critical) of Hoog (High risk) in Productie staan. Kritische bevindingen dienen per direct te worden weggenomen door de Inschrijver. Voor Hoge risicobevindingen geldt dat deze binnen uiterlijk een maand zijn weggenomen door de Inschrijver. Voor kwetsbaarheden die geclassificeerd zijn als Gemiddeld en Laag worden termijnen van respectievelijk drie en zes maanden gehanteerd. De Security Officer van de Belastingdienst heeft de bevoegdheid om toegang tot (relevante delen van) de oplossing te blokkeren. Dit wordt het Stekkermandaat genoemd. De Gegevens van de Belastingdienst wordt veilig gesteld en ontoegankelijk gemaakt. Inschrijver werkt mee aan het implementeren van een Alternatieve werkstroom om het uit te voeren proces zoveel als mogelijk doorgang te laten vinden. Het deblokkeren van (delen van) de Oplossing mag alleen na toestemming van de Security Officer van de Belastingdienst. Bij deze Reinstate werkt de Leverancier mee aan het weer in Productie nemen van de Oplossing, inclusief integratie van Gegevens die ontstaan is door de noodgedwongen uitwijk naar een Alternatieve werkstroom.	X	X	X

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
(Persoons-) Gegevens					
	Het voorkomen dat er enkel op basis van de A&P test van de leverancier een kwetsbare Oplossing naar productie wordt gebracht.	De Belastingdienst heeft het recht om een A&P-test uit te voeren als onderdeel van de Acceptatietest voor in Productiename van de Oplossing.	X	X	
	Het detecteren van nieuwe kwetsbaarheden en vaststellen dat bestaande kwetsbaarheden zijn opgelost. Dit aanvullend op de eisen t.a.v. de andere Attack and Penetration tests.	De Belastingdienst heeft het recht om – onaangekondigd- minimaal één keer per kwartaal een Vulnerability scan op de Oplossing uit te laten voeren door het Security Operation Center (SOC) van de Belastingdienst. Indien noodzakelijk geacht door de Belastingdienst worden Vulnerability scans ad-hoc uitgevoerd. Er is geen beperking op het aantal Vulnerability scans per jaar. De Bevindingen worden gedeeld en besproken met de Chief Security Officer (CSO) van de Inschrijver. Gevonden Kwetsbaarheden worden opgelost. Inschrijver werkt kosteloos mee aan de Vulnerability scans die namens de Belastingdienst worden uitgevoerd.	X	X	

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
(Persoons-) Gegevens					
	In de ongewenste situatie dat onbevoegden toegang krijgen tot de Oplossing op een wijze, anders dan via de door de Belastingdienst toegekende identificatie en autorisatie, zullen de Gegevens in deze Oplossing ontoegankelijk moeten zijn. Hiertoe zullen alle Gegevens in alle toestanden, zijnde in ieder geval opslag en transport te allen tijde moeten worden geëncrypt met een door NIST of NCSC aanbevolen encryptie-algoritmes van 128 bits en bij voorkeur 256 bits. http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#Approved Algorithms Een goede versleuteling van Gegevens verkleint het risico dat (persoons-)Gegevens ongewenst in handen komt van derden. Hierbij is het van belang dat: • de Gegevens versleuteld worden opgeslagen; • het transport van de Gegevens door middel van een versleutelde verbinding loopt; • de Gegevens zelf tijdens transport versleuteld zijn.	Gegevens waarmee in de Oplossing wordt gewerkt, worden versleuteld opgeslagen. Gegevens die tussen de Oplossing en andere ICT-services worden verzonden, dienen versleuteld te zijn. Versleuteling van de Gegevens geschiedt met een door NIST of NCSC aanbevolen encryptie-algoritmes van 128 bits en bij voorkeur 256 bits.	X	X	
	De Belastingdienst hecht veel belang aan de bescherming van haar Gegevens. Toegang van onbevoegden tot deze gegevens is niet toelaatbaar. De architectuur van de Database waarin de Gegevens worden opgeslagen geeft extra zekerheid over de waarborging van de bescherming van de Gegevens.	Gegevens van de Belastingdienst worden fysiek gescheiden van Gegevens van andere klanten van de Inschrijver opgeslagen.	X		

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
(Persoons-) Gegevens					
	Voldoen aan Rijksbeleid.	Gegevens van de Belastingdienst worden binnen de Europese Economische Ruimte (EER) opgeslagen. Gedurende de levenscyclus van de Gegevens, blijven deze Gegevens binnen de EER	X		

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Autorisatie en Authenticatie					
	Om te waarborgen dat alleen geautoriseerde Gebruikers gebruik maken van de Gegevens in de Oplossing, moet elke Gebruiker een eigen unieke gebruikersidentificatie krijgen. Door het gebruikersaccount te herleiden naar één en uitsluitend één natuurlijk persoon kan misbruik van een gebruikersaccount beter worden bestreden.	Elke Gebruiker van de Oplossing krijgt een unieke gebruikersidentificatie (gebruikersaccount). Het gebruikersaccount is altijd één op één herleidbaar naar een Natuurlijk Persoon. De Belastingdienst beheert de gebruikersaccounts en bepaalt welke accounts opgevoerd of verwijderd moeten worden. De Oplossing biedt uitsluitend en alleen toegang tot Gegevens aan Gebruikers, die daarvoor expliciet geautoriseerd zijn door de Belastingdienst.	X	X	
	Gezien de vertrouwelijkheid van de Gegevens is het wenselijk dat de Oplossing two-factor authentication ondersteunt.	De Oplossing biedt een mechanisme voor Two-factor authentication aan. Voor beheerders van de Oplossing is gebruik verplicht.	X	X	
	De Oplossing maakt gebruik van één Identity Management Systeem, waardoor Gebruikers (ongeacht hun rol en autorisaties) maar één keer hoeven te authentiseren om alle aan hun toegewezen functionaliteiten van de Oplossing te kunnen gebruiken.	De Gebruiker hoeft zich eenmalig aan te melden om gebruik te maken van de integrale functionaliteit van de Oplossing. Het beheer van toegangsrechten voor de Oplossing, inclusief de bewaking van functiescheiding, geschiedt vanuit één (logisch) Identity Managementsysteem (IMS).	X	X	

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Autorisatie en Authenticatie					
	De Belastingdienst werkt aan een Identity Bridge waarmee SSO (Single Sign-on) met derde partijen mogelijk wordt. Voorwaarde is daarbij wel, dat authenticatie op basis van SAML 2.0 gebeurt. Van de Inschrijver wordt gevraagd een Oplossing te leveren die SAML 2.0 ondersteunt, zodat SSO kan worden gerealiseerd wanneer de Identity Bridge van de Belastingdienst hiervoor geschikt is gemaakt.	Het Identity Managementsysteem (IMS) van de Oplossing ondersteunt federatieve authenticatie op basis van SAML 2.0	X	X	

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Koppelingen					
	De Oplossing zal in meer of mindere mate in staat moeten zijn om te koppelen met Oplossingen van derden. Dit moet het mogelijk maken om in de toekomst gegevens tussen andere autonome systemen en de Oplossing uit te kunnen wisselen.	Alle relevante API's van de Oplossing ten aanzien van koppelingen en gegevensuitwisseling met andere autonome systemen van derden zijn gedocumenteerd. Deze informatie is actueel, correct en wordt beschikbaar gesteld aan de Contractmanager.	X	X	

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Logging en monitoring					
	Voldoen aan Rijksbeleid (BIR).	Alle mutaties die leiden tot wijziging van (persoons)Gegevens moeten worden gelogd en zijn te raadplegen door de Functioneel beheerder van de Belastingdienst. De logging bevat per mutatie minimaal de mutatie zelf, de Gebruiker die de mutatie uitvoert en de datum en het tijdstip van de mutatie.	X	X	
	Zicht krijgen op afwijkingen om herstelacties te kunnen formuleren.	De Oplossing wordt volcontinu gemonitord op beveiligingsaspecten, capaciteit, performance en beschikbaarheid. Afwijkingen worden gelogd en gerapporteerd aan de Contractmanager.	X	X	X

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Herstelbaarheid					
	Van de Oplossing wordt verwacht dat deze hoog beschikbaar is en nagenoeg geen ongeplande onbeschikbaarheid kent. De inschrijver dient daarbij voorbereid te zijn op de uitzonderlijke situatie dat de Oplossing dusdanig beschadigd raakt dat voor herstel de back-up van de Gegevens nodig zijn.	De Oplossing dient na een ernstige calamiteit binnen 48 klokuren zonder verlies van Gegevens weer volledig functioneel beschikbaar te zijn. Indien voor dit herstel de back-up van de Gegevens benodigd zijn, is maximaal 24 klokuren verlies van Gegevens toegestaan.	X		**X**

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
SLA					
	Inschrijver levert bij inschrijving een concept SLA Inschrijver dat in elk geval onderstaande aspecten bevat: Wijze waarop invulling wordt gegeven aan 3e lijns support; Een aanpak die er voor zorgt dat de Belastingdienst altijd vrij kan beschikken over een op basis van Open Standaarden opgebouwde digitale recente (1 Kalenderdag) kopie van de Gegevens en de metadata van de Oplossing.	De Oplossing dient na een ernstige calamiteit binnen 48 klokuren zonder verlies van Gegevens weer volledig functioneel beschikbaar te zijn. Indien voor dit herstel de back-up van de Gegevens benodigd zijn, is maximaal 24 klokuren verlies van Gegevens toegestaan.	X		**X**

Categorie	Doelstelling	Eis	SaaS	On premise	SLA
Algemeen					
	Aansluiten op de standaard werkwijzen en techniek van het datacenter van de Belastingdienst.	De oplossing wordt on premise gehost, conform de aansluitvoorwaarden		X	
	Beleid van Belastingdienst.	Domeinnamen zijn eigendom van de Belastingdienst.	X	X	
	Het anonimiseren en/of pseudonimiseren van deze informatie heeft een positief effect op de zwaarte van de beveiligingseisen, die gesteld worden aan de koppelingen. De Belastingdienst hecht daarom veel waarde aan het kunnen anonimiseren en/of pseudonimiseren van persoonsgegevens.	De Oplossing kan (persoons)Gegevens bij verzending kan anonimiseren en/of pseudonimiseren.	X	X	
	De Gegevens zijn onder andere onderhevig aan de Wet Bescherming Persoonsgegevens en Archiefwet. Technische mogelijkheden in de Oplossing kunnen het eenvoudiger maken om aan deze Wetten te conformeren.	De Oplossing biedt de mogelijkheid om het archiveren en verwijderen van geclassificeerde Gegevens, bij voorkeur automatisch, uit te voeren.	X	X	

2 Non functionele wensen

Categorie	Doelstelling	Wens	SaaS	On premise	SLA
Beveiliging					
	De beveiliging van de Gegevens kan op allerlei manieren worden gerealiseerd. De wijze waarop dit gebeurt, geeft een goed beeld van de volwassenheid van de Oplossing ten aanzien van (ICT-) beveiliging.	Geef aan op welke wijze de vertrouwelijkheid, integriteit en onweerlegbaarheid van Gegevens van de Belastingdienst gedurende de gehele data lifecycle (maken, gebruiken, transmissie, verwerking, opslag, archivering en vernietiging) in de Oplossing gewaarborgd blijft op het in de SLA overeengekomen beveiligingsniveau. Beoordelingscriterium: De mate waarin Inschrijver bovenstaande elementen heeft uitgewerkt en aangetoond. Er wordt onder andere gekeken naar procedurele-, technische- en fysieke maatregelen.	X	X	X

Categorie	Doelstelling	Wens	SaaS	On premise	SLA
(Persoons-) Gegevens					
	Omdat de versleuteling geen waarde heeft indien de sleutel in verkeerde handen komt of wordt gebruikt voor niet door de Belastingdienst gewenste doeleinden, is het wenselijk dat het beheer van de sleutel door de Belastingdienst wordt uitgevoerd. Gezien de voordelen die hiermee zijn te behalen op het gebied van compliance ten aanzien van privacy van persoonsgegevens wordt aan eigen sleutelbeheer veel waarde gehecht.	Geef aan in hoeverre de Oplossing eigen sleutelbeheer door de Belastingdienst ondersteunt en wat de eventuele meerkosten zijn. Beoordelingscriterium: De beoordeling geschiedt op basis van de meerkosten, de haalbaarheid, de benodigde implementatie activiteiten voor de Belastingdienst en de onderhoudbaarheid van het eigen sleutelbeheer.	X	X	

Categorie	Doelstelling	Wens	SaaS	On premise
Koppelingen				
	Beleid van de Belastingdienst om aan Open Standaarden te voldoen van het Forum Standaardisatie. www.formumstandaardisatie.nl	Geef aan in hoeverre de Oplossing Open Standaarden ondersteunt om informatie van en naar autonome systemen van derden te transporteren. Beoordelingscriterium: Score 0: Geen ondersteuning; Score 6: 1 open standaard wordt ondersteund; Score 8: 2 tot 4 Open Standaarden worden ondersteund; Score 10: minimaal 5 Open Standaarden worden ondersteund.	X	X
	Geeft inzicht in de koppelbaarheid en de beveiliging daarvan. Dit tussen de Oplossing en partijen die geen onderdeel zijn van de Oplossing.	Beschrijf de mate van koppelbaarheid van de Oplossing. In uw beschrijving dient u in ieder geval de volgende aspecten uit te werken: De aanwezigheid van gedocumenteerde koppelvlakken; Gebruik van marktconforme standaarden voor gegevensuitwisseling; De beveiligingsmaatregelen die onbedoelde en/of ongeautoriseerde toegang tot de Gegevens in transport, opslag en bewerking verhinderen; De aanwezigheid van een ontwikkelomgeving met representatieve testgegevens. Beoordelingscriterium: De mate waarin wordt voldaan aan bovenstaande aspecten. Alle aspecten wegen even zwaar."	X	X

Begrippen- en afkortingenlijst

In onderstaande tabel wordt aangegeven wat met de begrippen en afkortingen wordt verstaan. Begrippen en afkortingen beginnen met een hoofdletter.

Begrip	Betekenis
Acceptatietest	-
Algemene verordening gegevensbescherming	-
Alternatieve werkstroom	-
anonimiseren	-
API	-
Archiefwet	-
Attack en Penetration	-
Baseline Informatiebeveiliging Rijksoverheid	-
Business Impactanalyse	-
Chief Security Officer	-
Contractmanager	-
Database	-
dataclassificaties	-
Europese Economische Ruimte	-
Forum Standaardisatie	-
Gebruik	-
Gebruiker	De Gebruiker is de aanduiding voor een willekeurige functionaris in de Oplossing die geautoriseerd is om gebruik te maken van de Oplossing.
Identity Managementsysteem	-
ISO 27001	-
ISO25010-norm	-
Kwaliteitsnormen	-
Levensduur van de Oplossing	-
National Cyber Security Centre	-
Natuurlijk Persoon	-
Open Standaarden	-
Pas-toe-of-leg-uit	-
PIA	-
Productie	-
Productiename	-

Begrip	Betekenis
pseudonimiseren	-
Qualsys SSL Labs	-
QuickScan	-
Reinstate	-
Responsetijd	De tijd tussen melding van een Incident/vraag en het moment dat gestart wordt met het oplossen c.q. beantwoorden van een Incident/vraag.
Rijkshuisstijl	
SAML 2.0	Responsetijd
Security eisen	-
Security Officer	-
Security Operation Center	-
Single Sign-on	-
SSL/TLS	-
Third Party Memorandum	-
Two-factor authentication	-
Wbp	Wet bescherming persoonsgegevens.
zero-client footprint	-

Begrip	Betekenis
Beheer en Onderhoud	Alle activiteiten van Opdrachtnemer gericht op het verbeteren, herstellen, waaronder het uitvoeren van service- en onderhoudswerkzaamheden en/of in aanvaardbare werkbare (operationele) situatie houden van de Diensten conform het gestelde in de Aanbestedingsstukken. Dit alles met inbegrip van de (eventuele) nieuwe functionaliteiten en/of nieuwe Diensten na Implementatie, gericht op het in operationele staat brengen en houden van de Oplossing, evenals de helpdesk activiteiten in de vorm van Support. onder Onderhoud wordt tenminste verstaan adaptief, additief, correctief, preventief en perfectief.
Additionele Dienst(en)	Aanvullende diensten welke door middel van een opdracht op incidentele basis aan Opdrachtnemer zijn en/of worden verstrekt. Indien Opdrachtnemer in het kader van de levering van een Additionele Dienst eveneens product(en) moet leveren, wordt in een dergelijk geval voor het toepassen en lezen van deze Overeenkomst onder het begrip Additionele Dienst eveneens onlosmakelijk met deze Additionele Dienst te leveren product(en) begrepen, tenzij de aard en inhoud van de bepaling zich daartoe verzet.
Oplossing	De Oplossing betreft het voor Gebruikers ingerichte, geteste en door de Belastingdienst geaccepteerde werkende samenstel van alle gevraagde ICT componenten die ondersteuning bieden aan de .. aandachtsgebieden ……. en conform de overeengekomen Specificaties functioneert.
Specificaties	Het onderdeel van de Aanbestedingsstukken en/of Offerteaanvraag, betreffende de huidige technische en functionele infrastructuur en/of gewenste technische en functionele behoefte beschreven in de Aanbestedingsstukken en/of de technische en functionele eisen van het Beheer en Onderhoud van de te verwerven Diensten eventueel vermeerderd met de Specificaties benodigd voor de verwerving van Additionele Diensten .
Support	Ondersteuning bieden aan de Belastingdienst conform de bepalingen zoals neergelegd in de SLA als onderdeel van de Overeenkomst.
Overeenkomst	Als bedoeld in art. 1.24 van de Voorwaarden.
Voorwaarden	De Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT) bestaande uit deze Algemene bepalingen en alle Bijzondere bepalingen.
Service Level Agreement Opdrachtnemer (SLA)	Een aanhangsel van de Overeenkomst dat na parafering door Partijen onderdeel van de Overeenkomst uitmaakt. Het betreft een beschrijving van de vastgestelde normen in de vorm van Service Levels voor de Diensten.
Service Levels	Ten aanzien van Beheer en Onderhoud overeengekomen vormen van dienstverlening in de Overeenkomst met inbegrip van het Beschrijvend Document en Specificaties en eveneens nader uitgewerkt in de SLA Opdrachtnemer als onderdeel van de Overeenkomst.
Inschrijver	Een natuurlijk of rechtspersoon (of een combinatie van rechtspersonen) die naar aanleiding van het Beschrijvend Document en de Nota(s) van Inlichtingen een Inschrijving heeft ingediend en waarmee al dan niet een Overeenkomst wordt gesloten.
Aanbestedingsstukken	Alle documenten in de aanbestedingsprocedure verwoord in het Beschrijvend Document.
Nota’s van Inlichtingen	Nadere inlichtingen op het Beschrijvend Document, welke integraal deel uitmaken van de Aanbestedingsstukken.
Beschrijvend Document	Het document met kenmerk IUC18-XXX, op basis waarvan de Inschrijver een Inschrijving heeft ingediend in het kader van de Europese aanbesteding.