



BIJLAGE A SPECIFICATIE VAN DE OPDRACHT

Europese aanbesteding

“IT Service Management-oplossing”

Versie : 1.1
Kenmerk : IUC 21-055
Datum : 20-01-2023

INHOUDSOPGAVE

Hoofdstuk 1. Inleiding	4
1.1. On-premises versus Cloud eisen en wensen	4
1.2. De IST-situatie	4
1.3. De SOLL-situatie	4
1.4. Offerteproces	7
1.5. Samenwerken conform Agile / aanpak installatie, configuratie en migratie	7
Hoofdstuk 2. Functionals	10
2.1. Algemeen	10
2.2. Archiveren	10
2.3. Rapportage	10
2.4. Selfservice	11
2.5. Proces inrichting	12
2.6. Technische interface integratie	12
2.7. Koppelingen	12
2.8. Forum Standaardisatie	13
2.9. Eisen en Wensen aan best practices	14
Hoofdstuk 3. IV kaders	16
3.1. Non-functionals	16
3.2. Infrastructuur	20
3.3. Beveiliging	24
Hoofdstuk 4. Integriteit	36
4.1. Business Etiquette	36
Hoofdstuk 5. Maatschappelijk Verantwoord Inkopen (MVI)	37
5.1. Energie & Klimaat	37
5.2. Welzijn & Gezondheid	38
5.3. Social Return on Investment	38
5.4. Internationale sociale voorwaarden	39
Hoofdstuk 6. Juridische kaders	41
Hoofdstuk 7. Prijsstelling	42
7.1. Algemene eisen ten aanzien van Prijzen	42
7.2. Toelichting Prijscomponenten in Bijlage VIII 1.1 "Prijzenformulier"	42
7.3. Specifieke eisen ten aanzien van Prijzen	44
7.4. Indexering Prijs	44
Hoofdstuk 8. Documentatie, Opleiding en Consultancy	46

8.1.	Documentatie.....	46
8.2.	Opleiding	46
8.3.	Consultancy	47
Hoofdstuk 9. Voorbereiding- en Implementatiefase		48
9.1.	Installatie & Integratie	48
9.2.	Documentatie, Opleiding en Consultancy.....	49
Hoofdstuk 10. Beheer en Onderhoud & Support		50
10.1.	Technisch Beheer & Consultancy	50
10.2.	Onderhoud & Support	50
10.3.	Documentatie, Opleiding en Consultancy.....	57
10.4.	Factureren en bestellen	57
10.5.	Kaders voor (re)transitie	58

Hoofdstuk 1. Inleiding

Dit document beschrijft de eisen en wensen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding met kenmerk IUC 21-055. Dit document maakt integraal onderdeel uit van het Beschrijvend Document.

In dit document zijn een aantal teksten blauw en groen gearceerd; deze dienen als extra hulp c.q. aandachtspunt.

De blauwe arcering betreffen Eisen waarop ook met NVT geantwoord mag worden; de groene arcering betreffen zaken die in het DAP moeten worden beschreven.

1.1. On-premises versus Cloud eisen en wensen

Zoals in paragraaf 2.4. van het Beschrijvend Document aangegeven wordt de ITSM-oplossing primair on-premises gebruikt en vindt er een gefaseerde overgang naar Cloud plaats. Dit heeft tot gevolg dat er per platform aparte Eisen en Wensen zijn gedefinieerd, maar dat er ook Eisen en Wensen zijn die voor beide platforms gelden.

Daar waar een Eis of een Wens specifiek voor on-premises of Cloud geldt, is dat expliciet aangegeven. (In de Eis is **[OP]** of **[CI]** opgenomen als de betreffende Eis alleen voor de on-premises of Cloud variant van de ITSM-oplossing geldt.)

Alle overige Eisen en Wensen gelden voor beide platformen.

1.2. De IST-situatie

De huidige ITSM-oplossing is op basis van ITIL®3 voor de in paragraaf 2.4 van het Beschrijvend document ingericht op basis van IBM ICD en Flexera. In Bijlage 6 Beschrijving van de ingerichte IST-situatie is door verschillende afdelingen zo goed mogelijk beschreven hoe zij hun werk met ITIL®3 uitvoeren. Deze informatie is voor Inschrijver bedoeld om zich een goed beeld te kunnen vormen van het huidige gebruik én op welke wijze een Migratie van Gegevens naar de nieuwe ITSM-oplossing zo goed mogelijk kan verlopen.

Omvang van de huidige omgeving

In de huidige ITSM-oplossing worden voor de op 2 na in paragraaf 2.4 van het Beschrijvend document genoemde best practices Gegevens bewaard. Aangezien er op dit moment 2 verschillende instanties (voor IV en NHD) naast elkaar draaien, is de behoefte voor de migratie van Gegevens verschillend.

Te migreren objecten voor IV:

Vanuit de huidige oplossing (ICD) moeten Gegevens van openstaande objecten naar de ITSM-oplossing gemigreerd worden. In Bijlage VIII Prijzenformulier 1.1, tabblad Dimensionering is een overzicht gegeven. Het aangegeven aantal objecten is een momentopname van juli 2022; de verwachting is dat deze aantallen veranderen.

1.3. De SOLL-situatie

De directie IV van de Belastingdienst heeft drie hoofddoelstellingen geformuleerd om samen met de business voor informatievoorziening te zorgen die bijdraagt aan een financieel gezond en veilig Nederland, te weten:

- Top 3 IT-werkgever van Nederland zijn voor engineers (bouwers): medewerkers zijn trots om voor IV te werken;
- Tijdige en kort-cyclische levering: features worden afgerond volgens met de business overeengekomen plannen en kennen een korte cycle time. De IV-oplossingen voldoen aan de vraag van de business;
- 99,9% beschikbaarheid: een grote mate van stabiliteit en continuïteit voor de business binnen service windows en een hoge standaard van cyberveiligheid.

De nieuwe ITSM-oplossing is randvoorwaardelijk voor bovengenoemde doelstellingen en levert hieraan een bijdrage door middel van:

- Sterk verbeterde gebruikers ervaring (selfservice portaal en chat robots);

- Reductie van manueel of herhaaldelijk werk (automatisering van workflow en taken het inzetten van Artificial Intelligence, mobiel benaderen van de ITSM oplossing;
- Efficiënter werken: meer doen met minder mensen;
- Meer verantwoordelijkheid naar de Eindgebruikers om zelf zaken op te (kunnen) lossen (door middel van API-toegang tot de ITSM-oplossing)
- Een eenduidige architectuur, die toekomstige ontwikkelingen als de beweging naar DevOps voortbrenging maximaal faciliteert en waarvan de onderhoudsinspanning minimaal is.

In de SOLL-situatie zijn de IT-beheerprocessen van de IV Organisatie van de Belastingdienst op basis van ITIL®4 ingericht.

De IT-beheerprocessen worden ondersteund door de ITSM-oplossing, waarbij configuratie van de ITSM-oplossing zo dicht mogelijk bij de "out of the box" implementatie van de Opdrachtnemer blijft.

Dit stelt Opdrachtgever in staat om beter in control te zijn over het voortbrengingsproces IV in termen van juiste, tijdige en efficiënte uitvoering.

Deze situatie wordt niet ineens bereikt, maar fasegewijs. Hiervoor zal een roadmap worden opgesteld.

In de eerste fase zal het huidige tool, IBM Control Desk (ICD), worden vervangen. Dit betekent dat eerst alle IT-beheerprocessen die de Opdrachtgever nu kent en geïmplementeerd zijn in ICD, in deze fase worden gemigreerd naar de nieuwe ITSM-oplossing. Uitgangspunt is dat we de best practices van de Opdrachtnemer volgen en de onderlinge samenhang van de processen borgen.

Naast de technische inrichting van de ITSM-oplossing zullen gebruikers en organisatie meegenomen moeten worden in de veranderingen die worden doorgevoerd. Dit is geen onderdeel van deze aanbesteding.

Voor de volgende best practices is de implementatie ingevuld met een koppeling met bestaande producten:

- Monitoring en Event Management: koppelvlak met NetCool Operations Insight;
- IT Asset Management: koppelvlak met Flexera;
- Portfolio Management: koppelvlak met Fortes Change Cloud.

De SOLL-situatie voor de eerste fase is bereikt als:

- Genoemde eerste 13 best practices zijn geïnstalleerd, geïmplementeerd en geconfigureerd in de nieuwe ITSM-oplossing;
- De performance en de werking van de ITSM-oplossing is geaccepteerd door gebruikers;
- De migratie van aangewezen gegevens is afgerond (zie voor aangewezen gegevens paragraaf 1.5);
- Eindgebruikers en Behandelaren de nieuwe ITSM-oplossing gebruiken;
- DevOps teams de mogelijkheid hebben om te integreren met de ITSM-oplossing;
- De oude ITSM-oplossing (ICD) niet meer gebruikt wordt en is uit gefaseerd;
- Een scenario is uitgewerkt waarbij migratie naar een Cloud-oplossing (in een latere fase) mogelijk is.

Na deze eerste fase zullen de overige processen aan bod komen (voor een volledig overzicht van de best practices zie het Beschrijvend Document, par. 2.4.1).

De SOLL-situatie voor de volgende fases is bereikt als:

- Onder de opties afgenomen best practice(s) is/zijn geïnstalleerd, geïmplementeerd, geconfigureerd of met een bestaande oplossing binnen de Belastingdienst is geïntegreerd;
- Eindgebruikers en Behandelaren de opties gebruiken;
- De oude oplossing voor de opties niet meer gebruikt wordt en is uit gefaseerd.

1.3.1. De transitie naar de SOLL-situatie

De IV-organisatie zit in een meerjarige periode van strategische transitie naar een dienstverlenende organisatie die op Agile & DEVOPS wijze werkt en levert.

De IV-organisatie zet over een periode van meerdere jaren in op een transitie naar een Agile manier van werken en het verder automatiseren van de automatisering, waarbij de implementatie van DEVOPS een belangrijk onderdeel is.

Na de verwerving van de nieuwe ITSM-oplossing zal de besturing van de transitie van 'oud' naar 'nieuw' ITSM plaatsvinden vanuit een centraal programma. De samenstelling van dit programma is IV-breed.

Naast de feitelijke besturing wat in welke volgorde vormgegeven moet worden aan de best practices zal ook verandermanagement vanuit dit programma worden vormgegeven.

De eerste transitiestap zal bestaan uit het zodanig inrichten van de verworven ITSM-oplossing dat de huidige implementaties in ICD kunnen worden uit gefaseerd. Hierbij is het de bedoeling dat de nieuwe ITSM-oplossing zo wordt ingericht dat er een geïntegreerde oplossing staat die standaard (dus geen maatwerk) is ingericht. De ITSM-oplossing moet voorbereid zijn op de integratie van de ontwikkelomgeving die door DEVOPS teams worden gebruikt.

Met behulp van deze integratie moeten resultaten uit het DEVOPS proces worden geregistreerd in de ITSM-oplossing. Het is de bedoeling om de ITSM-oplossing door middel van zo klein mogelijke wijzigingen in overzichtelijke releases beschikbaar te stellen aan de organisatie. De eerste release waar daadwerkelijk productie mee gedraaid wordt, zal enige tijd duren, daar de geïmplementeerde processen minimaal ondersteund moeten worden.

De huidige implementatie van de Nationale Helpdesk Douane in ICD zal eveneens gemigreerd moeten worden naar een (logisch) gescheiden instantie van de nieuwe ITSM-oplossing. Hierbij is het uitgangspunt dat de implementatie door middel van de standaard functionaliteit van de ITSM-oplossing geschiedt. Voor de Nationale Helpdesk Douane wordt niet voorzien dat er, in relatie tot de IST-situatie (paragraaf 16 van Bijlage 6), additionele practices benodigd zijn.

De Opdrachtnemer zal als supplier actief deelnemen in de programmaorganisatie. Van de Opdrachtnemer wordt naast de inbreng in de feitelijke installatie en configuratie van de ITSM-oplossing, verwacht dat zij de Belastingdienst adviseert over inrichtingskeuzes, aanpak en volgorde van inrichting.

Na de definitieve gunning van de opdracht zal een kick-off met de Opdrachtnemer worden georganiseerd waar de verdere samenwerking en besturing vorm gegeven worden en gezamenlijk de inhoudelijke aanvliegroute worden bepaald.

1.3.2. Inzet van de best practices

Van de 34 best practices die in scope van de opdracht zijn, zijn er een aantal die, indien deze worden verworven, functioneel volledig worden ingezet. Er zijn ook een aantal best practices die bij afname enkel en alleen ingezet worden met als doel te integreren met bestaande (die niet vervangen worden) en/of toekomstige applicaties. Met behulp van die best practices worden in dat geval naadloze en betrouwbare koppelingen tussen de ITSM-oplossing en de betreffende applicaties gerealiseerd.

Een voorbeeld hiervan is Flexera. (Op dit moment wordt Flexera ingezet als Software Asset Management oplossing omdat deze door grote softwareleveranciers wordt geaccepteerd om licentiebeheer uit te voeren.)

De best practice IT Asset Management (Software Asset Management Integratie) dient in dit specifieke voorbeeld als integratiestuk tussen Flexera en de ITSM-oplossing.

In de onderstaande tabel is aangegeven van welke best practices de functionaliteit bij afname volledig worden geïmplementeerd en welke alleen voor integratie worden gebruikt:

Best Practice	Doel	Best Practice	Doel
Change Enablement	Volledig	Problem Management	Volledig
Deployment Management	Volledig	Release Management	Volledig
Incident Management	Volledig	Service Catalog Management	Volledig
IT Asset Management	Integratie ¹	Service Configuration Management	Volledig
Knowledge Management	Volledig	Service Desk	Volledig
Monitoring and Event Management	Integratie	Service Request Management	Volledig
Portfolio Management	Volledig		

¹ Voor Software Asset Management wordt primair Flexera gebruikt, vandaar integratie. Voor Hardware Assetmanagement zal de best practice van de ITSM-oplossing worden gebruikt.

Best Practice	Doel	Best Practice	Doel
Capacity and performance management	Volledig	Infrastructure and platform management	Volledig
Measurement and reporting	Volledig	Service continuity management	Volledig
Relationship management	Volledig	Service design	Volledig
Risk management	Volledig	Service financial management	Integratie
Service level management	Volledig	Architecture management	Integratie
Service validation and testing	Integratie	Business analysis	Volledig
Software development and management	Integratie	Organizational change management	Volledig
Supplier management	Integratie	Project management	Volledig
Availability management	Volledig	Strategy management	Volledig
Continual improvement	Volledig	Workforce and talent management	Integratie
Information security management	Volledig		

Tabel 1 overzicht best practices t.b.v. Integratie of volledige inzet

1.4. Offerteproces

Voor het lichten van opties zoals beschreven in paragraaf 2.4.1. van het Beschrijvend document, Uitbreidingen, Additionele Diensten in de vorm van consultancy en/of Opleidingen wordt een Offertetraject gestart als Prijzen en/of Tarieven niet vaststaan.

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

1. Het IUC Belastingdienst stuurt een aanvraag naar de Opdrachtnemer;
2. De Opdrachtnemer stuurt de Offerte, inclusief met de originele door de Fabrikant en/of toeleverancier afgegeven Offerte retour aan het IUC Belastingdienst;
3. Na goedkeuring van de Opdrachtgever op de Offerte accepteert het IUC Belastingdienst de Offerte door middel van een addendum op de Overeenkomst en een Inkoopopdracht.

De Aanbestedende dienst kan in een Offertetraject de Fabrikant en/of toeleverancier dezelfde Wensen voorleggen als die nu in deze aanbesteding aan de Inschrijver worden gevraagd.

Van de Offerte moet de oorsprong vast te stellen te zijn en te herleiden naar de Fabrikant en/of toeleverancier. Hiervan is bijvoorbeeld sprake indien de Offerte op briefpapier van de Fabrikant wordt aangeleverd. Offertes in pdf van de Fabrikant of doorgestuurde e-mails van de Fabrikant behoren ook tot de mogelijkheden zolang de oorsprong vastgesteld kan worden.

UE 1. Opdrachtnemer conformeert zich aan de werkwijze van een Offertetraject zoals beschreven in paragraaf 1.4.

UE 2. Opdrachtnemer hanteert voor elke Offerte een geldigheidstermijn van minimaal 60 dagen.

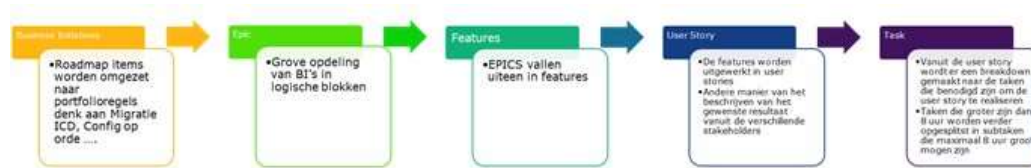
UE 3. Opdrachtnemer levert Offertes alléén via het Inkoopuitvoeringscentrum Belastingdienst aan.

1.5. Samenwerken conform Agile / aanpak installatie, configuratie en migratie

De initiële inrichting/configuratie, migratie en de doorontwikkeling van de door u aangeboden ITSM-oplossing, wordt op een Agile wijze ingericht. Hierbij wordt zoveel mogelijk aangesloten bij SAFe (de standaard binnen de Belastingdienst voor Agile werken).

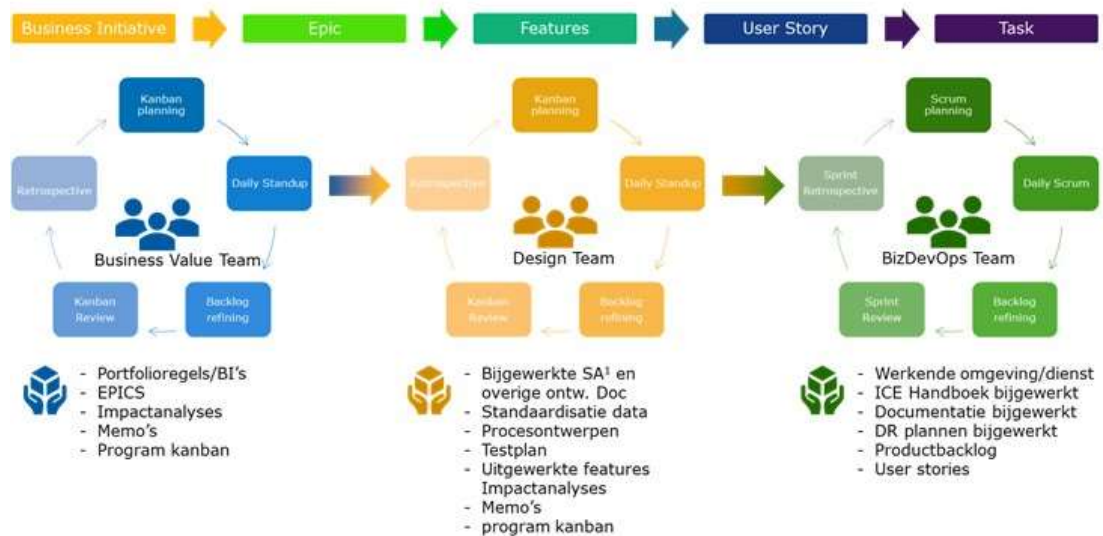
De verwachting is dat voor de inrichting, migratie en doorontwikkeling kan worden volstaan met de "essential" inrichting van SAFe.

De methode van werken voor de inrichting van de nieuwe aan te schaffen ITSM-oplossing is hieronder weergegeven, als mede de teams en de functies die daarvoor ingevuld dienen te worden.



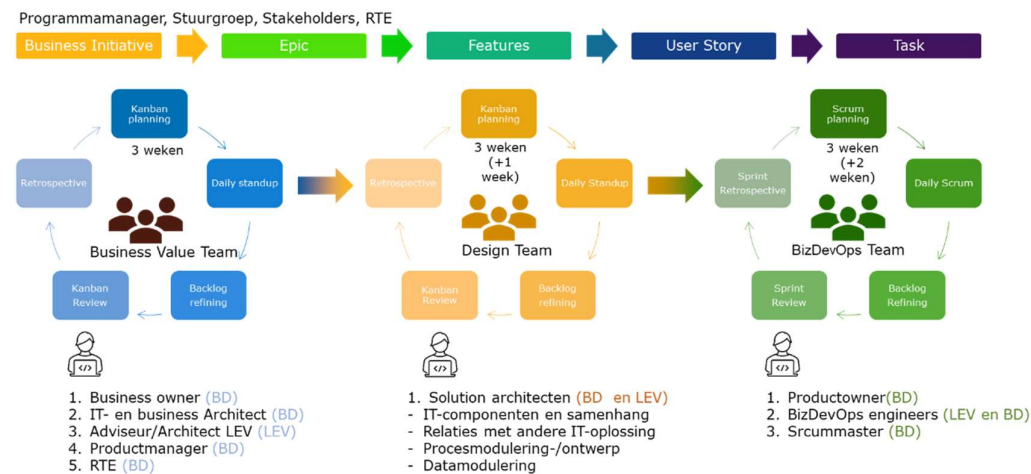
Figuur 1 Werkverdeling

Daarbij worden de volgende teams geformeerd:



Figuur 2 Samenstelling teams

Binnen deze teams zijn de volgende rollen onderkend:



Figuur 3 Rollen²

Voor een succesvolle implementatie moet er achter de business owner nog een organisatie worden ingericht om de met de implementatie noodzakelijk business change succesvol te implementeren. Dit zal worden opgepakt vanuit een programma dat is opgezet bij de Belastingdienst. De rollen die hiervoor nodig zijn (denk aan programma-/projectmanagement, verandermanagement, procesmanagement en diepgaander kennis van ITIL4/IT4IT aan business zijde, functioneel beheer aan business zijde) worden

² BD betreft medewerkers van de Belastingdienst; LEV betreft medewerkers van/via de Opdrachtnemer.

door de Belastingdienst zelf ingevuld en indien nodig vindt inhuur plaats de inhuurmantels die de Belastingdienst heeft. Deze rollen zijn dus geen onderdeel van deze aanbesteding.

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

- Voor het business value team een Adviseur-/Architect;
- Voor het designteam de rol van solution architect vanuit de Opdrachtnemer;
- Voor het BizDevOps team BizDevOps engineers die de ITSM-oplossing configureren, waarbij één engineer in staat moet zijn de rol van scrummaster in te vullen. De verwachting is dat de Belastingdienst deze rol na migratie overneemt. Dit zal een parttime rol zijn die gecombineerd wordt met die van BizDevOps engineer.

Er wordt met bovenstaande opzet van teams begonnen. Gaande het proces van inrichten, migreren en optimaliseren zal deze opzet verder geëvalueerd worden met de betrokken medewerkers en, indien nodig, worden aangepast.

Na contractering wordt begonnen met Business Value team en het Designteam. Het BizDevOps team start pas nadat de ITSM-oplossing technisch in de OTA(P) is ingericht. De engineers kunnen immers pas starten met configureren als de ITSM-oplossing technisch ingericht is.

Zie voor de dimensionering van de inzet Bijlage VIII 1.1 Prijzenformulier, tabblad 3 Additionele Diensten.

De beschrijvingen waaraan elke rol moet voldoen is beschreven in Bijlage 7 Rolbeschrijvingen 1.1.

UE 4.	Opdrachtnemer conformeert zich aan de werkwijze zoals beschreven in paragraaf 1.5.
-------	--

Hoofdstuk 2. Functionals

2.1. Algemeen

GUE 1.	De ITSM-oplossing biedt de mogelijkheid voor verschillende (interne) klanten een logisch gescheiden omgeving in te richten.
GUE 2.	In aanvulling op GUE 1 is het in de ITSM-oplossing is het mogelijk om voor verschillende (interne) klanten, op minimaal het niveau van Helpdesk tickets, Gegevens tussen de verschillende logisch gescheiden omgevingen uit te wisselen.
GUE 3.	De ITSM-oplossing ondersteunt alle huidige 34 ITIL® best practices.

Back-up & Recovery

GUE 4.	[OP] De ITSM-oplossing is in staat om een back-up van de omgeving te maken en deze te herstellen vanaf deze back-up omgeving. Hierbij maakt de ITSM-oplossing gebruik van één van de storage diensten van de Belastingdienst: - File storage dienst: zie Bijlage 12 Aansluitvoorwaarden NAS of - Back-up & Recovery dienst: zie Bijlage 13 Aansluitvoorwaarden back-up en recovery.
--------	--

2.2. Archiveren

GUE 5.	De ITSM-oplossing biedt de mogelijkheid om Gegevens die niet meer actueel zijn (denk hierbij aan bijvoorbeeld aan afgestoten CI's Assets, gesloten Incidenten, Changes etc.) te archiveren.
--------	---

2.3. Rapportage

GUE 6.	De ITSM-oplossing beschikt over een rapportage framework.
GUE 7.	Het rapportage framework bevat standaard sjablonen voor/bij alle best practices.
GUE 8.	Het rapportage framework beschikt over role-based toegang.
GUE 9.	Alle opgeslagen Gegevens in de ITSM-oplossing kunnen in een rapportage worden opgenomen.

W 1	Beschrijf in maximaal 4 pagina's welke mogelijkheden het rapportage framework biedt: De beoordelingscriteria voor deze Wens zijn: - Welke rapportage is standaard in de ITSM-oplossing aanwezig; - Kan elke gebruiker zijn/haar eigen rapportage samenstellen? - Kan elke gebruiker in de eigen rapportage teksten toevoegen? - Kunnen rapportage instellingen gedeeld worden? - Kunnen rapportages per tijdseenheid automatisch samengesteld en gemaild worden? - Kunnen rapportages op onderwerp en/of organisatieonderdeel worden gegenereerd? - Hoe flexibel is het framework bij bijvoorbeeld aanpassingen in de organisatie? - Kan elke gebruiker d.m.v. slepen van velden de rapportage zelf, zonder programmeercodering samenstellen? - Welke presentatie mogelijkheden (bijvoorbeeld, maar niet limitatief, xls, xlsx), html en/of pdf biedt de rapportage tool t.b.v. publicatie van rapportages op het intranet van de Belastingdienst? Voor deze Wens geldt de volgende waardering: <table> <tr> <td>0</td><td>Zeer slecht;</td></tr> <tr> <td>13</td><td>Slecht;</td></tr> <tr> <td>67</td><td>Matig;</td></tr> <tr> <td>111</td><td>Voldoende;</td></tr> <tr> <td>289</td><td>Goed;</td></tr> <tr> <td>444</td><td>Uitstekend.</td></tr> </table>	0	Zeer slecht;	13	Slecht;	67	Matig;	111	Voldoende;	289	Goed;	444	Uitstekend.
0	Zeer slecht;												
13	Slecht;												
67	Matig;												
111	Voldoende;												
289	Goed;												
444	Uitstekend.												

2.4.

Selfservice

ITSM Selfservice portal

Een Selfservice portal is een moderne gebruikersinterface die vanaf elk apparaat vanaf elke locatie toegankelijk is en een onderdeel van de ITSM-oplossing.

Medewerkers bezoeken de Selfservice portal om bijvoorbeeld een oplossing voor hun problemen en/of vragen te vinden. De Selfservice portal maakt het vinden van oplossingen op vragen eenvoudig door directe toegang tot een Knowledge database.

GUE 10.	De ITSM-oplossing beschikt over een Selfservice portal.
GUE 11.	Vanuit de Selfservice portal is toegang tot de Knowledge database.
GUE 12.	De Selfservice portal beschikt over een Chat(ro)bot functie.
GUE 13.	De Chat(ro)bots met virtuele assistenten kunnen dienen als proxy tussen een gebruiker en de Servicedesk.
GUE 14.	De ITSM-oplossing biedt de mogelijkheid de service catalog (logisch) te rubriceren.
GUE 15.	Een Eindgebruiker ziet alleen items van de service catalog waartoe hij/zij rechten heeft.
GUE 16.	De ITSM-oplossing biedt de mogelijkheid om vanuit de Selfservice portal een melding naar de (interne) Helpdesk te sturen.
GUE 17.	De ITSM-oplossing biedt de mogelijkheid om vanuit de selfservice Request Full Fillment bestellingen te plaatsen en volgen.

GUE 18. De ITSM-oplossing biedt de mogelijkheid de status van meldingen en/of bestellingen op te vragen.

2.5. Proces inrichting

GUE 19. De ITSM-oplossing bevat voor gedefinieerde sjablonen, blueprints en workflows van de ITIL practices die kunnen worden aangepast.

2.6. Technische interface integratie

GUE 20. De ITSM-oplossing ondersteunt voor alle onderdelen van de ITSM-oplossing een functionele ontsluiting via een REST-API.

GUE 21. Inschrijver heeft een beschrijving van de REST-API interface beschikbaar.

GUE 22. De ITSM-oplossing ondersteunt een interface die in staat is minimaal 100.000 items per uur te importeren en/of updaten.

GUE 23. De ITSM-oplossing ondersteunt bulkimport van in ieder geval .csv, .xls en fixed lenght.

In de huidige situatie zijn een groot aantal systemen met ICD gekoppeld. Deze koppelingen zijn ook in de ITSM-oplossing noodzakelijk. Het heeft de voorkeur dat de Inschrijver over standaard koppelingen beschikt om deze systemen te koppelen.

W 2	Geef aan of uw ITSM-oplossing uitgewerkte koppelingen heeft met:	
	IBM Netcool CEM omgeving t.b.v. van het melden van Events & Incidenten	89 punten;
	IBM Netcool CEM omgeving t.b.v. het monitoren van de ITSM-oplossing zelf	89 punten;
	Flexera Flexnet Manager	89 punten;
	IBM Tivoli Application Dependency Discovery Manager(TADDM);	89 punten;
	SAP, gecertificeerd, t.n.v. HR, Artikelen, exemplaren van artikelen en Contracten	89 punten;
	SAP, ongecertificeerd, t.n.v. HR, Artikelen, exemplaren van artikelen en Contracten	89 punten;
	VMWare Workspace One	27 punten;
	Azure DevOps	27 punten;
	Atlassian JIRA	27 punten;
	HCL Big Fix	27 punten;
	Koppelingen met systemen anders dan hierboven genoemd.	24 punten.
	Op deze Wens kunnen maximaal 666 punten worden behaald.	

GUE 24. De ITSM-oplossing bevat een interface naar SMTP en IMAP.

2.7. Koppelingen

Een oplossing staat zelden op zichzelf. Ook niet als het in de Cloud staat. Oplossingen zijn vaak met andere ICT-systemen binnen de Belastingdienst gekoppeld. Denk ook aan de kantooromgeving van de Belastingdienst. Of aan gebruikers van buiten de Belastingdienst die de Belastingdienst toegang wil verlenen tot, in dit geval, de ITSM-oplossing.

Hetzelfde geldt voor on-premises oplossingen. In alle gevallen zullen er Aansluitvoorwaarden van toepassing zijn.

De Aanbestedende dienst stelt hiervoor specifieke Eisen op die er op gericht zijn organisatorisch en technisch aan te sluiten op de infrastructuur van de Belastingdienst

Medewerkers van de Aanbestedende dienst werken 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 Aanbestedende dienst een zero-footprint client.

In de praktijk betekent dat dat er gebruik wordt gemaakt van een web browser als clientprogramma. De Aanbestedende dienst ondersteunt op de eigen werkplek Google Chrome.

GUE 25. De ITSM-oplossing ondersteunt de laatste versies van de ondersteunde webbrowsers.

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

Gegevens in transitie worden versleuteld. Versleuteling is gebaseerd volgens de richtlijnen van het NCSC. In Bijlage 20 ICT-beveiligingsrichtlijnen-voor-Transport-Layer-Security-v2 zijn in hoofdstuk 4 richtlijnen en voorwaarden beschreven. Op de website van het NCSC is altijd de meest recente richtlijn te vinden. Voor de ITSM-oplossing geldt dat deze aan elke richtlijn moet voldoen aan het criterium 'Goed'.

Zie ook: <https://www.ncsc.nl/onderwerpen/verbodingsbeveiliging/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>.

GUE 26. **[CL]** De ITSM-oplossing voldoet aan Elke genoemde in hoofdstuk 4 van Bijlage 20 ICT-beveiligingsrichtlijnen-voor-Transport-Layer-Security-v2 genoemde TLS-versie, cryptografische algoritme, sleutellengte, keuze van groepen en overige en opties die met een 'Goed' wordt gewaardeerd.

GUE 27. Vervallen

UE 5. Opdrachtnemer is verantwoordelijk dat koppelingen tussen de ITSM-oplossing en systemen van derden beveiligd zijn.

2.8. 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 Belastingdienst overigens vastgesteld dat Inschrijver deze moet toepassen (dus zonder Leg-uit-mogelijkheid).

Zie ook: <https://www.forumstandaardisatie.nl/open-standaarden/verplicht>.

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.

Voor de ITSM-oplossing zijn onderstaande standaarden verplicht:

GUE 28. De ITSM-oplossing biedt de mogelijkheid om voor alle webverbindingen van de ITSM-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 29.	[CL] De ITSM-oplossing biedt de mogelijkheid web- en maildomeinen waar de ITSM-oplossing gebruik van beschikbaar te maken via zowel IPv4 als IPv6 (dual stack). In het gebruik, in de breedste zin van het woord, tussen IPv4 en IPv6 is geen verschil.
GUE 30.	[CL] De ITSM-oplossing biedt de mogelijkheid om voor elke domeinnaam van de ITSM-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.
GUE 31.	De ITSM-oplossing ondersteunt SAML.

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 6.	Opdrachtnemer gaat akkoord om in overleg te treden als de lijst Open Standaarden wijzigt.
-------	---

2.9. Eisen en Wensen aan best practices

W 3	Het is de wens om binnen Incidentmanagement de meldingen in te kunnen delen in verschillende categorieën; denk hierbij onder ander aan bijvoorbeeld verlies en diefstal, menselijke fout, configuratiefout, aanval, hack, phishing. Daarbij is het wenselijk dat, als dit bovenstaande mogelijk is, deze zelf te beheren. Beschrijf of bovenstaande in de ITSM-oplossing mogelijk is. De beoordelingscriteria voor deze Wens zijn: <table> <tr> <td>Wel mogelijk in te kunnen delen in verschillende categorieën én het is mogelijk deze zelf te beheren</td><td>148 punten;</td></tr> <tr> <td>Wel mogelijk in te kunnen delen in verschillende categorieën maar het is niet mogelijk deze zelf te beheren</td><td>44 punten;</td></tr> <tr> <td>Niet mogelijk in te kunnen delen in verschillende categorieën</td><td>0 punten.</td></tr> </table>	Wel mogelijk in te kunnen delen in verschillende categorieën én het is mogelijk deze zelf te beheren	148 punten;	Wel mogelijk in te kunnen delen in verschillende categorieën maar het is niet mogelijk deze zelf te beheren	44 punten;	Niet mogelijk in te kunnen delen in verschillende categorieën	0 punten.
Wel mogelijk in te kunnen delen in verschillende categorieën én het is mogelijk deze zelf te beheren	148 punten;						
Wel mogelijk in te kunnen delen in verschillende categorieën maar het is niet mogelijk deze zelf te beheren	44 punten;						
Niet mogelijk in te kunnen delen in verschillende categorieën	0 punten.						
GUE 32.	Het is mogelijk bij iedere best practice van de ITSM-oplossing bijlages (zoals Word-documenten en/of afbeeldingen) toe te voegen.						
GUE 33.	Elke best practice binnen de ITSM-oplossing heeft de mogelijkheid voor opmaak van tekst; dit betekent het aan kunnen passen van bijvoorbeeld lettertype, lettergrootte, opsommingstekens etc.						
W 4	Sommige Incidenten moeten behandeld worden door functionarissen van zowel binnen als buiten de Belastingdienst. Overdracht en terugkoppeling vindt nu via de mail plaats, waarbij functionarissen van IV eigenaar van het Incident blijven. Geef aan of het mogelijk is om vanuit de ITSM-oplossing geautomatiseerd Incidenten aan te melden bij de derde partij, updates van het Incident te ontvangen en te verwerken vanuit een oplossing van een derde partij. Dit zou ook andersom moeten kunnen; een derde partij kan geautomatiseerd een melding indienen, waarbij updates vanuit de ITSM-oplossing geautomatiseerd worden doorgegeven aan de oplossing van een derde partij. De beoordelingscriteria voor deze Wens zijn: <table> <tr> <td>Ja, dit is mogelijk</td><td>555 punten;</td></tr> <tr> <td>Nee; dit is niet mogelijk</td><td>0 punten.</td></tr> </table>	Ja, dit is mogelijk	555 punten;	Nee; dit is niet mogelijk	0 punten.		
Ja, dit is mogelijk	555 punten;						
Nee; dit is niet mogelijk	0 punten.						

GUE 34	De ITSM-oplossing toont de status van de voortgang binnen een proces van de betreffende geïmplementeerde best practice.
--------	---

Hoofdstuk 3. IV kaders

Vanuit IV zijn de navolgende Eisen en Wensen gedefinieerd.

3.1. Non-functionals

Ontwerp van de ITSM-oplossing

De Opdrachtgever wil inzicht hebben wat door de Opdrachtgever aan infrastructuur beschikbaar gesteld moet worden om de ITSM-oplossing on premises (intern als dienst) beschikbaar te kunnen stellen. Dit voor de eerste 13 practices met de dimensionering zoals die in Bijlage VIII 1.1 Prijzenformulier is geschetst voor het derde jaar.

In het ontwerp wordt minimaal beschreven:

- Hoe wordt de ITSM-oplossing gemapped op de in infrastructuur zoals beschreven in paragraaf 3.2 infrastructuur. Hierbij moet niet alleen worden weergegeven welk deel van de oplossing op welk hostingplatform land, maar ook hoeveel capaciteit nodig is van het hosting platform in termen van aantal benodigde hosts en per host:
 - Hoeveelheid benodigde cores;
 - Hoeveelheid benodigde geheugen;
 - Hoeveelheid benodigde opslag.
- Van welke diensten (zoals een koppeling met de Active Directory) de werking van de ITSM-oplossing afhankelijk is en
- Welke netwerkverbindingen nodig zijn om een werkende ITSM-oplossing te krijgen.

Daarnaast zal het ontwerp gebruikt worden om te toetsen of aan de volgende gunningseisen wordt voldaan:

Uit het ontwerp moet blijken dat de architectuur van de aangeboden ITSM-oplossing een level 4 implementatie is van IT4IT (GUE 36).

Uit het ontwerp moet blijken hoe ingericht is dat de ITSM-oplossing beschikbaar blijft bij het uitvallen van een heel datacenter (GUE 130).

Uit het ontwerp moet blijken hoe ingericht is dat bij het doorvoeren van releases en patches de ITSM-oplossing voor gebruikers beschikbaar blijft (GUE 136).

De ITSM-oplossing geen andere hostingplatformen nodig heeft dan Red Hat Linux 7 of hoger, Windows Server 2022 of hoger, IaaS Virtualisatie platform op basis van VW Ware en/of Container platform (GUE 53)

Ten slotte wordt dit ontwerp in de fase van gunningstest gebruikt om exact af te spreken wat de belastingdienst beschikbaar stelt aan infrastructuur op locatie van de belastingdienst. Het testplan ITSM-oplossing (Bijlage 19) beschrijft de testen. Voor de uitvoering van de gunningstesten mag alleen infrastructuur worden ingezet welke in het ontwerp is beschreven.

GUE 35.	Inschrijver dient bij de Inschrijving op basis van bovenstaande tekst het ontwerp van de ITSM-oplossing als Bijlage XII bij GUE 35 in.
GUE 36.	Inschrijver toont op verzoek aan dat de ITSM-oplossing een aantoonbaar level 4-implementatie van IT4IT (zie https://pubs.opengroup.org/it4it/refarch20/chapo4.html) heeft voor de navolgende best practices: Servicedesk, incl. service portal, Incident Management, Service Request Management, Service Configuration Management, IT Asset Management, Problem Management, Change Enablement, Deployment Management, Release Management, Service Catalog Management, Service Catalog Management, Knowledge management, Capacity and Performance Management, Infrastructure and Platform Management, Continual Improvement, Measurement and Reporting, Availability Management, Service Design, Business Analysis, Organisational Change Management, Strategy Management, Project Management
GUE 37.	Alle in de ITSM-oplossing geproduceerde data is en blijft eigendom van de Aanbestedende dienst.

Gebruikersinterface

GUE 38	De user interface van de ITSM-oplossing voldoet aan WCAG 2.1 AA richtlijn.				
GUE 39	Behandelaars zijn in staat, om na het lezen van gebruikersinstructies en/of een opleiding van maximaal 1 dag, zelfstandig aan de slag te gaan met de ITSM-oplossing.				
GUE 40	De user interface van de ITSM-oplossing is minimaal beschikbaar in de Nederlandse en Engelse taal.				
GUE 41	De gebruiker heeft de mogelijkheid om m.b.t. de user interface binnen de ITSM-oplossing zelf de keuze te maken voor de Nederlandse en/of Engelse taal.				
GUE 42	De ITSM-oplossing ondersteunt het configureren van het startscherm op basis van rollen.				
GUE 43	De ITSM-oplossing ondersteunt voor elke gebruiker de mogelijkheid om de eigen startpagina in te richten / in te stellen.				
W 5	Geef aan of de ITSM-oplossing een Natural Language Query ondersteunt. De beoordelingscriteria voor deze Wens zijn: <table> <tr> <td>Ja</td><td>74 punten;</td></tr> <tr> <td>Nee</td><td>0 punten.</td></tr> </table>	Ja	74 punten;	Nee	0 punten.
Ja	74 punten;				
Nee	0 punten.				
GUE 44	De web interface m.b.t de ITSM-oplossing voldoet aan Responsive Web design; dit houdt in dat de interface zich aanpast aan het Device waarop het wordt aangeroepen.				

Performance

GUE 45	Bij het aanmaken van een nieuw Incident in de ITSM-oplossing is het betreffende scherm binnen maximaal 5 seconden beschikbaar om Gegevens in te voeren.
--------	---

Autorisaties

GUE 46	De ITSM-oplossing ondersteunt een RBAC model voor zowel data als functionaliteit.
GUE 47	De ITSM-oplossing kent verschillende autorisaties niveaus.
GUE 48	Een gebruiker mag in zijn/haar GUI geen opties zien waarvoor die niet is geautoriseerd.

Abonnementen

GUE 49	De ITSM-oplossing geeft inzicht in het licentiegebruik van de ITSM-oplossing.
GUE 50	[OP] De ITSM-oplossing ondersteunt tevens het gebruik om de licentiepositie en/of het gebruik van abonnementen van de ITSM-oplossing met Flexera te bepalen.

Acceptatietest

UE 7.	[OP] Opdrachtnemer conformeert zich dat Opdrachtgever het recht heeft een Acceptatietest uit te voeren om (onderdelen van) de ITSM-oplossing, waarbij geïdentificeerde bevindingen worden door Opdrachtnemer opgelost, tenzij de Opdrachtgever anders besluit. Opdrachtnemer werkt hier kosteloos aan mee. Acceptatietesten vinden plaats na omvangrijke wijzigingen én voor in productie name van nieuwe Releases van de ITSM-oplossing. De Opdrachtgever bepaalt de acceptatiemomenten.
-------	--

Installeerbaarheid

GUE 51.	[OP] De ITSM-oplossing heeft tijdens het starten en in gebruik nemen geen actieve internetverbindingen, om bijvoorbeeld licenties te controleren, benodigd.
GUE 52.	[OP] Het servercomponent van de ITSM-oplossing kan worden gebruikt op virtuele Apparatuur welke gebaseerd is op VMware (Intel).)
GUE 53.	[OP] De ITSM-oplossing ondersteunt installatie zonder aanpassingen op de onderstaande platformen: - Red Hat Enterprise Linux versie 7 en hoger (inclusief Logische opvolgers) en/of - Windows Server 2022 en hoger en/of - IAAS virtualisatie platform op basis van VM Ware en/of - Container platform.
GUE 54.	[OP] Opdrachtgever moet de ITSM-oplossing, conform handleiding, zelf op het genoemde platform kunnen installeren.
GUE 55.	[OP] De installatie en het updaten van de Programmatuur van de ITSM-oplossing vindt plaats vanaf lokale media zonder (directe) internettoegang. In de productieomgeving van het Datacenter is geen rechtstreekse internettoegang.
GUE 56.	[OP] De Programmatuur van de ITSM-oplossing is niet afhankelijk van externe Apparatuur zoals bijvoorbeeld een dongle.
GUE 57.	[OP] De installatie van de ITSM-oplossing moet zonder tussenkomst van handmatige handelingen uitgevoerd kunnen worden. Dit door gebruik te maken van het packageformaat behorend bij de genoemde platformen zoals genoemd in GUE 53.
GUE 58.	[OP] De ITSM-oplossing is geschikt om op de genoemde platformen zoals genoemd in GUE 53 te draaien en is onafhankelijk van de onderliggende Apparatuur. En kan dus naar andere Apparatuur gemigreerd worden.
GUE 59.	[OP] Het servercomponent van de ITSM-oplossing moet worden gebruikt op virtuele Apparatuur welke gebaseerd is op VMware (Intel).
GUE 60.	[OP] Inschrijver dwingt niet af om naar een hogere versie van Pakket Hosting te gaan als de 'oude' versie nog ondersteund wordt.
GUE 61.	[OP] Nieuwe functionaliteiten in de ITSM-oplossing (of nieuwe versies van de gehele ITSM-oplossing) van Inschrijver zijn beschikbaar voor alle op dat moment door Inschrijver in GUE 53.

	ondersteunde platformen. Met “ondersteunen” wordt bedoeld dat alle bestaande features van de ITSM-oplossing op dat betreffende platform probleemloos werken en dat de Inschrijver op dat platform ondersteuning verleent.
--	---

Generieke aansluitvoorwaarden

GUE 62	De ITSM-oplossing voldoet aan Bijlage 8 IDWOR (interoperabiliteitskader voor digitale werkomgevingen in de rijksdienst)
GUE 63	[OP] De ITSM-oplossing voldoet aan Bijlage 9 Aansluitvoorwaarden Netwerkaansluitdiensten Datacenter.
GUE 64	[OP] De ITSM-oplossing voldoet aan Bijlage 10 Aansluitvoorwaarden Web proxy - v1.0.
GUE 65	[OP] De ITSM-oplossing voldoet aan Bijlage 11 aansluitvoorwaarden externe leveranciers x86 OS-en.

3.2. Infrastructuur

Het Overheids Data Center van de Belastingdienst (ODC-BD) bestaat uit twee datacenter locaties die redundant, met eigen glasvezelverbindingen, met elkaar gekoppeld zijn. De productieomgeving van de ITSM-oplossing moet zo ingericht worden dat hij blijft doordraaien als één van de datacenters niet meer bereikbaar is vanwege een calamiteit. De ITSM-oplossing kan worden gehost op één van de volgende hostingdiensten van de het ODC-BD:

- Hosting op VM (Virtuele appliance); zie paragraaf 3.2.1;
- Pakket hosting (o.b.v. Windows of Linux); zie paragraaf 3.2.2
- Container Hosting zie paragraaf 3.2.3.

Afhankelijk van de hostingsdienst gelden de navolgende Eisen.

3.2.1. Virtuele Appliance

Een Virtual Appliance is een virtual machine die bestaat uit een image van Programmatuur van een voor geïnstalleerde virtuele server (inclusief besturingssysteem en applicatie). Een Virtual Appliance is bedoeld om de kosten en benodigde tijd voor installatie, configuratie en onderhoud van complexe Programmatuur te verminderen.

Als de ITSM-oplossing (voor een deel uit) een Virtual Appliance bestaat dan gelden de navolgende Eisen. Als dit niet het geval is, dan kunnen de navolgende Eisen met 'NVT' worden beantwoord.

GUE 66	[OP] De Virtual Appliance van de ITSM-oplossing is gebaseerd op virtuele Apparatuur van VMware (Intel). Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met het gebruik op een Virtuele Appliance wordt aangeboden.
GUE 67	[OP] De Virtual Appliance van de ITSM-oplossing wordt als importeerbare set van één of meerdere bestanden geleverd in OVF of OVA formaat. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met het gebruik op een Virtuele Appliance wordt aangeboden.
GUE 68	[OP] De Virtual Appliance van de ITSM-oplossing maakt gebruik van een VXMNET3 netwerkadaptor. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met het gebruik op een Virtuele Appliance wordt aangeboden.
GUE 69	[OP] De Virtual Appliance van de ITSM-oplossing maakt gebruik van een Paravirtual SCSI storage adaptor. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met het gebruik op een Virtuele Appliance wordt aangeboden.

3.2.2. Pakket Hosting

Bij een Pakket Hosting oplossing wordt de ITSM-oplossing geïnstalleerd op pakkethosting diensten van de Belastingdienst: Windows of Linux. Een algemene beschrijving van de taken en verantwoordelijk heden van de dienst (providerfunctie van de Belastingdienst) en de afnemer (de leveranciers verantwoordelijk voor het gedrag en functioneren van de ITSM-oplossing) wordt beschreven in Bijlage 14 Gebruikersovereenkomst LPH 2.0; deze is van toepassing indien de ITSM-oplossing op basis van windowspakket hosting wordt aangeboden.

Als de ITSM-oplossing (voor een deel uit) een Pakket Hosting bestaat dan gelden de navolgende Eisen. Als dit niet het geval is, dan kunnen de navolgende Eisen met 'NVT' worden beantwoord.

Installeerbaarheid

GUE 70.	[OP] De ITSM-oplossing ondersteunt installatie zonder aanpassingen op de onderstaande platformen: - Red Hat Enterprise Linux versie 7 en hoger (inclusief Logische opvolgers) en/of - Windows Server 2022 en hoger. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.
GUE 71.	[OP] Opdrachtgever moet de ITSM-oplossing, conform handleiding, zelf op het genoemde platform kunnen installeren. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.
GUE 72.	[OP] De installatie van de ITSM-oplossing moet zonder tussenkomst van handmatige handelingen uitgevoerd kunnen worden. Dit door gebruik te maken van het packageformaat behorend bij het platform O.S. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.
GUE 73.	[OP] De ITSM-oplossing is geschikt om op een gevirtualiseerd OS te draaien en is onafhankelijk van de onderliggende Apparatuur. En kan dus naar andere Apparatuur gemigreerd worden. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.
GUE 74.	[OP] Het servercomponent van de ITSM-oplossing kan worden gebruikt op virtuele Apparatuur welke gebaseerd is op VMware (Intel). Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.

Virusscanner

GUE 75.	[OP] De ITSM-oplossing functioneert in de omgeving waar op Windows Server een virusscanner verplicht en actief is, zonder deze virusscanner te hoeven her configureren (momenteel is dit de Symantec virusscanner). Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Windows Server 2022 wordt aangeboden.
---------	--

Linux Security

GUE 76.	[OP] De ITSM-oplossing functioneert normaal, indien geïnstalleerd op een Linux Server, ook als selinux in die omgeving actief is en op 'enforcing' staat. Het is niet noodzakelijk eigen selinux policies mee te leveren; de ITSM-oplossing zelf mag in de unconfined selinux context draaien. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux wordt aangeboden.
---------	---

Admin rechten

GUE 77.	[OP] De ITSM-oplossing draait geen services of daemons met netwerkconnectiviteit onder een high privileged account (root, local admin of domain admin). Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.
---------	--

Licentiemanagement

GUE 78.	[OP] De ITSM-oplossing functioneert in een omgeving waarin een licentie management agent verplicht en actief is (momenteel is dit de Flexera agent). Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.
---------	---

Firewall en integratie

GUE 79.	[OP] De ITSM-oplossing vereist niet dat de hostbased firewall op Linux moet worden uitgezet om te kunnen functioneren; de ITSM-oplossing functioneert met een actieve hostbased firewall. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met het gebruik in combinatie met Pakket Hosting wordt aangeboden.
---------	---

Nieuwe releases van het platform

GUE 80.	[OP] In aanvulling op GUE 60 ondersteunt Opdrachtnemer de platformversies totdat deze vanuit de leverancier van het betreffende platform End-of-Support zijn. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.
GUE 81.	[OP] De ITSM-oplossing wordt door Inschrijver ondersteund op de meest recente security patches van het onderliggende operating system. Met andere woorden: de ITSM-oplossing mag niet verhinderen dat de laatste security patches van het operating system worden geïnstalleerd. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.
GUE 82.	[OP] Bij het beschikbaar komen van een nieuwe versie van een platform levert de Inschrijver binnen 6 maanden na beschikbaar komen daarvan, een werkende versie van haar ITSM-oplossing voor dat platform. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Pakket Hosting op Red Hat Enterprise Linux en Windows Server 2022 wordt aangeboden.

3.2.3. Container Hosting

De Belastingdienst container-hosting-dienst is een platform waarop containers gehost kunnen worden. Het platform biedt daartoe een marktconforme run-time omgeving voor containers inclusief container management. Deze dienst is gebaseerd op Red Hat Open Shift technologie.

Als de ITSM-oplossing (voor een deel uit) een Container Hosting oplossing bestaat dan gelden de navolgende Eisen.

Als dit niet het geval is, dan kunnen de navolgende Eisen met 'NVT' worden beantwoord.

Installeerbaarheid server

GUE 83	[OP] De ITSM-oplossing wordt zonder aanpassing geïnstalleerd op het container platform van de Belastingdienst. Op dit moment is dat Red Hat OpenShift Container Platform versie 4. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie Container Hosting wordt aangeboden.
--------	---

GUE 84	[OP] De installatie van de ITSM-oplossing moet zonder tussenkomst van handmatige handelingen uitgevoerd kunnen worden. Dit door gebruik te maken van het packageformaat behorend bij het Container Platform. Dit zijn bij voorkeur operators en anders Helm charts. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie Container Hosting wordt aangeboden.
--------	---

Opslag

GUE 85	[OP] De ITSM-oplossing mag behalve tijdelijke gegevens geen gegevens in de lokale container opslaan. De ITSM-oplossing maakt voor permanente opslag van gegevens gebruik van de persistant storage, zoals geleverd wordt door het container platform of maakt gebruik van opslag buiten het platform, zoals een DBMS of gedeelde opslag faciliteiten. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	---

Netwerk

GUE 86	[OP] Er is beschreven welke poorten en protocollen voor de ITSM-oplossing benodigd zijn. Dit geldt zowel voor de firewall in het netwerk als de hostbased firewall. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	---

Container security

GUE 87	[OP] Het is niet toegestaan dat de ITSM-oplossing containers bevat, die Security Content Constraints (hierna SCC) nodig hebben, waardoor deze draaien als root en/of root toegang en/of privilege escalation hebben. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	--

GUE 88	[OP] De ITSM-oplossing draait geen services of daemons met netwerkconnectiviteit onder een high privileged account (root, local admin of domain admin). Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	---

Onderhoud platform

GUE 89	[OP] De correcte werking van de ITSM-oplossing wordt niet beïnvloed als het Container Hosting Platform een container van de Programmatuur stopt en op een andere worker node start. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	---

GUE 90	[OP] De correcte werking van de ITSM-oplossing wordt niet beïnvloed door het stoppen van een worker node, waarop een container van de Programmatuur draait. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	--

Nieuwe releases van het platform

GUE 91	[OP] Opdrachtnemer ondersteunt de platformversies totdat deze vanuit de Fabrikant van het betreffende platform End-of-Support zijn. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	--

GUE 92	[OP] De ITSM-oplossing wordt door Inschrijver ondersteund op de meest recente security patches van het Container Hosting Platform. Met andere woorden: de Programmatuur mag niet verhinderen dat altijd de laatste security patches worden geïnstalleerd. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	--

GUE 93	[OP] Bij het beschikbaar komen van een nieuwe versie van een platform levert de Inschrijver binnen 6 maanden na beschikbaar komen daarvan, een werkende versie van haar ITSM-oplossing voor dat platform. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	--

GUE 94	[OP] Nieuwe functionaliteiten in de ITSM-oplossing (of nieuwe versies van de gehele ITSM-oplossing) van Inschrijver zijn beschikbaar voor alle op dat moment door Inschrijver ondersteunde platformen. Met “ondersteunen” wordt bedoeld dat alle bestaande features van de ITSM-oplossing op dat betreffende platform probleemloos werken en dat de Inschrijver op dat platform ondersteuning verleent. Toelichting: Opdrachtgever wil beschikken over actuele platformversies, maar Opdrachtgever wil geen gedwongen upgrades naar hogere platformversies om bij te blijven in de life cycle van de ITSM-oplossing van Inschrijver zolang het platform niet end-of-support is. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	---

GUE 95	[OP] Releases van de ITSM-oplossing kunnen worden geïnstalleerd zonder handmatige migratieacties. Op deze GUE mag met NVT worden geantwoord als de ITSM-oplossing niet in combinatie met Container Hosting wordt aangeboden.
--------	--

3.3. Beveiliging

3.3.1. Privacy

GUE 96	De ITSM-oplossing voldoet aan AVG wetgeving.
--------	--

GUE 97	De ITSM-oplossing is gebouwd conform privacy by design.
GUE 98	De ITSM-oplossing is gebouwd conform privacy by default.
GUE 99	De ITSM-oplossing biedt de mogelijkheid om persoonsgegevens af te schermen.
GUE 100	De ITSM-oplossing biedt de mogelijkheid om bepaalde velden versleuteld op te slaan zodat de informatie niet toegankelijk is voor bijvoorbeeld Technisch Beheer.
UE 8.	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. In geval toont Opdrachtnemer aan welke Gegevens om welke reden(en) strikt noodzakelijk zijn.

Gegevens die te relateren zijn aan de Belastingdienst of haar medewerkers mogen zonder expliciete toestemming van de Opdrachtgever niet buiten de ITSM-oplossing verwerkt worden. Dat geldt uiteraard ook voor Persoonsgegevens. 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.

UE 9.	Opdrachtnemer conformeert zich, conform bovenstaande alinea, aan dat bij testen van de ITSM-oplossing geen gebruik wordt gemaakt van: - Productiegegevens; - Naar natuurlijke personen herleidbare Gegevens. Indien het voor het testen van de ITSM-oplossing noodzakelijk is om Productiegegevens te gebruiken of Gegevens die herleidbaar zijn naar natuurlijk personen, 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.
-------	---

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 ITSM-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 ingezetenen 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 10.	Opdrachtnemer overlegt voorafgaande aan uit te voeren werkzaamheden van de betreffende medewerker(s) een geldige Verklaring Omtrent Gedrag (hierna VOG.)
--------	--

3.3.2. Gegevens

In het geval van Cloud geldt dat Gegevens van de Belastingdienst gescheiden worden verwerkt (waaronder opgeslagen) van andere klanten van Opdrachtnemer; de Belastingdienst heeft geen zicht in Gegevens van andere klanten van de Opdrachtnemer en andere klanten hebben geen zicht in die van de Belastingdienst. Medewerkers van Opdrachtnemer hebben alleen toegang tot de Gegevens van de Belastingdienst voor zover dat noodzakelijk is voor het uitvoeren van de Overeenkomst.

GUE 101.	[CL] Gegevens van de Belastingdienst worden gescheiden opgeslagen van de Gegevens van andere klanten van de Inschrijver.
----------	---

GUE 102.	[CL] Toegang tot Gegevens van de Belastingdienst is beperkt voor medewerkers van de Belastingdienst en medewerkers van de Inschrijver voor zover dit noodzakelijk is voor de uitvoering van de Overeenkomst.
----------	---

Voor de Eisen GUE 101 en GUE 102 geldt dat deze onderdeel zijn van een Acceptatietest indien de optie tot verwerving van een Cloud variant wordt gelicht. Als een optie de Acceptatietest in dat geval niet goed doorstaat, zal de betreffende best practice niet worden verworven.

UE 11.	Opdrachtnemer zal geen Gegevens voor eigen doeleinden delen dan wel verwerken, behalve na expliciete toestemming van de Opdrachtgever.
--------	--

UE 12.	Opdrachtnemer zal, in navolging van UE 11, aangeven welke Gegevens in een dergelijk geval als noodzakelijk worden geacht voor de uitvoering van de Overeenkomst.
--------	--

De Aanbestedende dienst maakt bij voorkeur gebruik van versleutelde Gegevens bij opslag (encryption-at-rest). Eén van de voordelen is dat als de Gegevens op ongecontroleerde wijze buiten de ITSM-oplossing terecht komen, andere partijen geen gebruik kunnen maken van deze Gegevens.

GUE 103.	[CL] De ITSM-oplossing ondersteunt encryption-at-rest.
----------	---

UE 104.	[CL] Met betrekking tot GUE 103 geldt dat de private key zowel bij de Opdrachtgever dienst als de Opdrachtnemer in beheer moet kunnen worden gegeven.
---------	--

3.3.3. Beveiligingsincidenten

Dit zijn Incidenten die een vermoedelijk 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;
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, bedrijfstak- of sectorgerichte CERT) en
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 3.1). Oplostermijnen die hier aan gekoppeld zijn, zijn:

- Kritisch risico (Critical risk, score 9.0 – 10.0); per direct (voor lifegang van een nieuwe oplossing is dit belemmerend). Voor de Opdrachtgever is dit een incident;

- Hoog risico (High risk, score 7.0 – 8.9): per direct, na afstemming maximaal 1 maand (voor lifegang van een nieuwe oplossing is dit belemmerend). Voor de Opdrachtgever is dit een incident;
- Gemiddeld risico (Medium risk, score 4.0 – 6.9): 3 maanden. Voor de Opdrachtgever is dit een probleem en
- Laag risico (Low risk, 0.1 – 3.9): 6 maanden. Voor de Opdrachtgever is dit een probleem.

Voordat de ITSM-oplossing in productie kan gaan, wordt de beveiliging van de ITSM-oplossing getest ter Acceptatie. Daarna gebeurt dat periodiek (minimaal jaarlijks).

Gemiddeld- en Laagrisico bevindingen worden afgehandeld conform het Pas-toe-of-Leg-uitprincipe. Dit laatste, een Leg uit (Explain), betekent dat er besloten is dat de Kwetsbaarheid niet weggenomen wordt of dat adresseren ervan meer tijd gaat kosten dan de standaard Oplostijd. Opdrachtnemer onderbouwt in een dergelijk geval haar 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.

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

Het Stekkermandaat (zie ook paragraaf 3.3.7 **Stekkermandaat**) wordt in gang gezet als een ICT-oplossing reeds in productie staat. Staat een ICT-oplossing nog niet in productie, dan zal dat ook niet mogen totdat de Kritische-en Hoge risicobevindingen zijn weggenomen

UE 13.	Uit bovenstaande volgt daarom de Eis dat Opdrachtnemer zich conformeert, gedurende de looptijd van de Overeenkomst, aan de door de Opdrachtgever gebruikte methode (CVSS) om beveiligingsincidenten te kwalificeren en heeft haar organisatie zodanig ingericht dat de door de Opdrachtgever onderkende typen Beveiligingsincidenten voor (onderdelen) van de ITSM-oplossing binnen gestelde termijnen, als onderdeel van het Onderhoud & Support, opgepakt en opgelost worden.
UE 14.	Bij het constateren van Kwetsbaarheden met een niveau van kritisch (critical) of hoog (high), conform CVSS 3.1, wordt de Opdrachtgever daarover binnen één (1) uur door Opdrachtnemer geïnformeerd.
UE 15.	Kwetsbaarheden die leiden tot een Incident worden gekwalificeerd door middel van CVSS 3.1. Op basis van de CVSS 3.1 kwalificaties gelden voor de Opdrachtnemer de volgende streeftijden om deze op te lossen: • 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.
GUE 105	In de ITSM-oplossing gebruikte Open Source-code en/of libraries van andere toeleveranciers bevatten geen bekende Kwetsbaarheden. Er wordt gebruik gemaakt van de meest recente veilige versies uit betrouwbare bron. Op deze GUE mag met alleen NVT worden geantwoord als in de ITSM-oplossing géén Open Source-code en/of libraries van andere toeleveranciers is/zijn verwerkt.

Opdrachtgever gaat er van uit dat Opdrachtnemer de ITSM-oplossing ook levert of gaat leveren aan derden. Indien in dergelijke instances zich inbreuken op beveiliging en/of privacy voordoen, die zich ook kunnen voordoen in de aan de Opdrachtgever geleverde ITSM-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 Incidenten, maar ook om mogelijke toekomstige 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 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 Incident aangeven, de verwachte consequenties voor de Opdrachtgever, alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken. **Het proces hiervoor moet worden beschreven in een DAP met de Belastingdienst.**

UE 16.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. inbreuken op beveiliging en/of privacy in de ITSM-oplossing bij derden.
--------	---

Indien Opdrachtgever (op basis van een risico-inschatting) het noodzakelijk acht een A&P-test uit te laten voeren dan staat Opdrachtnemer dat toe en werkt daar conform afspraken aan mee. De precieze invulling van de A&P-test is afhankelijk van de situatie. Het kan een A&P-test zijn binnen de keten waar de ITSM-oplossing onderdeel van is of op de ITSM-oplossing zelf.

Het organiseren van deze A&P-test gebeurt door Opdrachtgever; het uitvoeren van de A&P-test zelf is voor rekening van Opdrachtgever.

Eventuele Kwetsbaarheden worden opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer werkt hier als onderdeel van Onderhoud & Support aan mee.

UE 17.	[CL] Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. inbreuken op beveiliging en/of privacy in de ITSM-oplossing bij derden.
--------	---

3.3.4. Datalek

De Belastingdienst handelt als verwerkingsverantwoordelijke conform de wettelijke kaders als primaire partij Data incidenten af. De verwerkingsverantwoordelijke moet de Autoriteit Persoonsgegevens (AP) binnen 72 klokuren op de hoogte stellen van een Datalek en eist van Opdrachtnemer onverwijld, doch uiterlijk binnen 24 klokuren op de hoogte te worden gesteld van een door Opdrachtnemer geconstateerd Datalek. Een (potentieel) Datalek is het gevolg van een beveiligingsincident en moet ook als zodanig worden geregistreerd en afgehandeld. Melding aan AP en afhandeling van het corresponderende beveiligingsincident kan parallel plaatsvinden.

Bij het informeren over een Datalek moet de omvang worden aangegeven alsmede de getroffen en/of te nemen maatregelen om de gevolgen te adresseren. In afstemming wordt bepaald welke partij primair analyse en afhandeling uitvoert. Verwerkingsverantwoordelijke en Opdrachtnemer houden elkaar op de hoogte.

UE 18.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. het omgaan met van een Datalek in de ITSM-oplossing. Procedures hier omtrent worden vastgelegd in een DAP met de Belastingdienst.
--------	---

3.3.5. Coordinated Vulnerability Disclosure

De Aanbestedende dienst heeft een Coördinated Vulnerability 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>.

UE 19.	Opdrachtnemer conformeert zich aan bovengenoemde werkwijze m.b.t. het afhandelen van CVD-meldingen. Procedures hier omtrent worden vastgelegd in een DAP met de Belastingdienst.
--------	--

3.3.6. Malware

GUE 106.	[OP] De ITSM-oplossing voldoet aan de beheersmaatregelen, conform aan Bijlage 10 Aansluitvoorwaarden Web proxy - v1.0, tegen malware (detectie, preventie en herstel) die Opdrachtgever heeft geïmplementeerd.
----------	---

3.3.7. Stekkermandaat

Opdrachtgever kent het principe van het Stekkermandaat. Opdrachtgever kan opdracht geven dat de ITSM-oplossing (inclusief de Gegevens) van de Belastingdienst onbeschikbaar gemaakt wordt voor (minimaal) toegang vanaf het internet. Effectief zal dit betekenen dat:

- Gegevens van de Belastingdienst voor derden ontoegankelijk worden gemaakt en/of
- (Relevante delen van) de ITSM-oplossing voor derden onbeschikbaar worden gemaakt.

Het Stekkermandaat wordt uitgevoerd op het moment dat de beveiliging van de ITSM-oplossing (inclusief Gegevens) in gevaar is. Dat is het geval als er zich een beveiligingsincident met een score van Kritisch of Hoog risico voordoet waarbij de onderliggende Kwetsbaarheid niet tijdig kan worden weggenomen. De ITSM-oplossing wordt weer in productie (online) gebracht na toestemming van de Security Officer van de Belastingdienst.

Opdrachtnemer werkt, daar waar relevant, kosteloos mee bij:

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

Het proces en de afspraken hiervoor worden beschreven in een DAP met de Belastingdienst.

UE 20.	[CL] Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. het omgaan met van het Stekkermandaat in relatie tot de ITSM-oplossing. Hierbij geldt dat tussen het inroepen van het Stekkermandaat en het afronden van de uitvoering maximaal 4 uur zit. Het startmoment begint als het verzoek om Data veilig te stellen door Opdrachtnemer is ontvangen.
--------	---

UE 21.	[OP] Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. het omgaan met van het Stekkermandaat in relatie tot de ITSM-oplossing.
--------	---

Bij (langdurige) uitval van de ITSM-oplossing krijgt de Opdrachtgever de beschikking over de meest recente Gegevens. Aanlevering gebeurt via een afgestemd veilig kanaal en conform afspraken conform (machine leesbaar) formaat.

UE 22.	[CL] Opdrachtnemer levert op aanvraag en conform afspraken een voor de Belastingdienst bruikbare digitale kopie van de meest actuele Gegevens en haar structuur. Vertrouwelijkheid en integriteit blijven geborgd.
--------	---

De afspraken hierover worden in een DAP met de Belastingdienst vastgelegd.

Reinstate

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

Hierbij geldt de speciale aandacht voor de situatie dat Gegevens van vóór het stopzetten van de ITSM-oplossing samengevoegd moeten worden met de Gegevens die in de tussentijd, zijn gegenereerd. Integriteit en Vertrouwelijkheid van de Gegevens blijven te allen tijde geborgd.

Opdrachtnemer werkt met betrekking tot bovenstaande alinea's als onderdeel van het Onderhoud & Support mee met het opnieuw in gebruik nemen van de ITSM-oplossing.

De afspraken hierover worden in een DAP met de Belastingdienst vastgelegd.

UE 23.	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. de Reinstate van de ITSM-oplossing.
--------	---

3.3.8. 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.

Er worden periodiek of rond een omvangrijke release beveiligingstesten uitgevoerd op een internet-facing ICT-oplossing. Het betreffen zowel Attack & Penetration testen als Vulnerability scans. De partij waar primair de hosting plaatsvindt, is de eerst verantwoordelijke om deze beveiligingstesten uit te voeren. Meestal is dat de Opdrachtnemer.

Beveiligingstesten die (aanvullend) uitgevoerd worden door de Opdrachtgever vervangen niet de beveiligingstesten van de Opdrachtnemer. Beveiligingstesten 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 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 daarover.

Bevindingen 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 ITSM-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?);
- 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 3.0) is gebruikt. Bij voorkeur met de statusaanduiding, bijvoorbeeld "In behandeling" (met plandatum) of "Opgelost (en hertest)".

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.

Aanvullende uitgangspunten bij A&P-testen die door of namens de Opdrachtgever worden uitgevoerd. Hierbij geldt dat:

- Er getest wordt in de Acceptatieomgeving welke technisch gelijk is aan en voorzien is van dezelfde beveiligingsmaatregelen als de Productie-omgeving; voor noodzakelijke afwijkingen is toestemming van de Opdrachtgever vereist;
- Er wordt géén gebruik gemaakt van Productiegegevens; voor noodzakelijke afwijkingen is toestemming van de Opdrachtgever vereist;
- Er is sprake van een freeze-periode in de omgeving wordt getest; alleen in samenspraak met het A&P-testbedrijf, bijvoorbeeld om een patch uit te voeren om een Kwetsbaarheid weg te nemen, kan hier van worden afgeweken;
- Kwetsbaarheden gekwalificeerd als Kritisch of Hoog risico worden zo mogelijk tijdens de A&P-test opgelost en hertest.

Opdrachtgever voert jaarlijks of na een significante release een A&P-test uit conform de hierboven beschreven richtlijnen van de Belastingdienst. De precieze invulling van de A&P-test is afhankelijk van de situatie.

Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.

UE 24. **[CL]** Opdrachtnemer conformeert zich aan bovenstaande, onder het kopje **Inleiding** genoemde, alinea's m.b.t. Beveiligingstesten in relatie tot de ITSM-oplossing.

UE 25. **[OP]** Opdrachtgever voert vóór in productie name, jaarlijks of ná een significante Release van de ITSM-oplossing een A&P-test uit conform beschreven richtlijnen van de Opdrachtgever. Dit kan ook een A&P-test zijn in een keten waarvan de ITSM-oplossing een deel is. De precieze invulling van de A&P-test is afhankelijk van de situatie en wordt bepaald door de Opdrachtgever. Eventuele Kwetsbaarheden die binnen de scope van de Opdrachtnemer vallen worden als onderdeel van Onderhoud & Support opgelost door Opdrachtnemer. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtgever conformeert zich aan, onder het kopje **Inleiding** genoemde, bovenstaande tekst.

A&P test vanuit Opdrachtgever

Als de Opdrachtgever het noodzakelijk vindt om de sterkte van de beveiligingsmaatregelen van de ITSM-oplossing te (laten) toetsen wenst Opdrachtgever hiervoor een onafhankelijk A&P-testbedrijf in te zetten. Opdrachtnemer accepteert en werkt hier aan mee; hiervoor is het nodig dat de Opdrachtnemer een Vrijwaringsverklaring af geeft.

De precieze invulling van de A&P-test is afhankelijk van de situatie. Het kan een A&P-test zijn binnen de keten waar de ITSM-oplossing onderdeel van is.

Het organiseren van deze A&P-test gebeurt door de Opdrachtgever en het uitvoeren van de A&P-test zelf is voor rekening van de Opdrachtgever.

Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.

UE 26. **[CL]** Opdrachtnemer conformeert zich aan het meewerken aan een toets en hierboven, onder het kopje **Inleiding** genoemde, beschreven werkwijze.

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 ITSM-oplossing ge-update wordt en aan de andere kant hackers en beveiligingsonderzoekers constant op zoek zijn naar nieuwe Kwetsbaarheden.

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

UE 27. **[CL]** Opdrachtnemer voert minimaal maandelijks een Vulnerability scan uit op de ITSM-oplossing conform bovenstaande.

Hierbij geldt dat de gebruikte tooling, waar Opdrachtnemer zelf in dient te voorzien, gebruik maakt van up-to-date kwetsbaarheidendefinitiebestanden.

	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 28.	[CL] In aanvulling op UE 27 geldt dat de gebruikte tooling, waar Opdrachtnemer zelf in dient te voorzien, gebruik maakt van up-to-date kwetsbaarheiddefinitiesbestanden. 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. Opdrachtnemer conformeert zich hier aan.
--------	--

Belastingdienst voert ook minimaal maandelijks een Vulnerability scan uit op de ITSM-oplossing conform haar eigen richtlijnen. Eventuele Kwetsbaarheden worden conform de richtlijnen van de Belastingdienst opgelost; Opdrachtnemer werkt hier kosteloos aan mee.

UE 29.	[OP] Opdrachtnemer conformeert zich aan bovenstaande alinea m.b.t. de uitkomsten van een Vulnerability scan.
--------	---

UE 30.	[CL] Als Opdrachtgever het noodzakelijk acht, op basis van een risico inschatting, een vulnerability scan uit te laten voeren op de ITSM-oplossing, dan staat Opdrachtnemer dat toe. De kosten van het uitvoeren van de Vulnerability scan worden gedragen door de Opdrachtgever. Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer conformeert zich hier aan.
--------	---

Beveiligingstestbeleid

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

GUE 107	[CL] Inschrijver voegt als Bijlage XIII documentatie bij de Inschrijving in die in bovenstaande informatiebehoefte voorziet.
---------	---

3.3.9. Continuïteit en continuïteitstesten

Opdrachtgever vindt het van belang te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én mocht onbeschikbaarheid toch groter zijn dan gepland, hoe snel de Gegevens beschikbaar zijn dan wel de ITSM-oplossing weer volledig operationeel kan zijn. Het gaat hierbij dus niet om de beschikbaarheidseisen waar het vooral draait om wanneer de ITSM-oplossing wel of niet te gebruiken is, maar om de excepties dat het mis gaat.

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

3.3.10. Back-up & Restore Test / Disaster Recovery Test

Het is voor de Opdrachtgever van belang te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én hoe snel de Gegevens beschikbaar zijn dan wel de ITSM-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 ITSM-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 Oplossing bij onbeschikbaarheid binnen bepaalde termijnen weer beschikbaar is zonder verlies van integriteit en vertrouwelijkheid.

De Opdrachtgever wil de garantie dat het proces doorgang kan vinden met de afgesproken beschikbaarheid. Verstoringen en Calamiteiten zijn beheersbaar en mitigerende maatregelen worden periodiek getest. De scope is de Productie-omgeving en eventuele ondersteunende omgevingen/processen die de beschikbaarheid van de Productie-omgeving kunnen degraderen. Er worden twee continuïteitstesten voorzien: Back-up & Restore en Calamiteitentest.

Back-ups zijn bedoeld om Gegevens, Programmatuur en Configuratiegegevens periodiek veilig te stellen, op een zodanige wijze dat deze gebruikt kunnen worden om Gegevens, Programmatuur of Configuratiegegevens bij onbeschikbaarheid binnen afgesproken termijnen al dan niet op hetzelfde systeem te herstellen.

Gegevens opgeslagen in back-ups zijn minimaal op het zelfde niveau beveiligd als Productiegegevens. Back-up buiten de ITSM-oplossing zijn niet te gebruiken om de Gegevens te verwerken anders dan via het reguliere Restoreproces binnen de ITSM-oplossing te brengen.

In geval van on-premises geldt dat bestanden met Gegevens, Programmatuur en de Configuratiegegevens zijn door de Back-upfunctionaliteit van de ITSM-oplossing veilig gesteld (moeten) worden.

Bovengenoemde toelichting geldt voor de 4 onderstaande Uitvoeringseisen.

UE 31.	[OP] De back-up functionaliteit betreffende de Gegevens in de ITSM-oplossing wordt aangesloten op de bestaande back-upfaciliteit van de Opdrachtgever en voldoet conform Bijlage 12 Aansluitvoorwaarden NAS of Bijlage 13 Aansluitvoorwaarden back-up en recovery.
--------	---

Opdrachtgever voert periodiek een Back-up & Restore Test uit. Afwijkingen worden indien voor Opdrachtnemer relevant gemeld. Opdrachtnemer werkt, als onderdeel van Onderhoud & Support mee aan het implementeren van eventuele verbeterpunten die van toepassing zijn op de ITSM-oplossing zelf. Deze worden opgenomen in het Verbeterplan en van daar uit opgelost.

UE 32.	[CL] Opdrachtnemer conformeert zich aan bovenstaande alinea m.b.t. het uitvoeren van een periodieke Back-up & Restore Test.
--------	--

UE 33.	[OP] Opdrachtnemer conformeert zich aan bovenstaande alinea m.b.t. het uitvoeren van een periodieke Back-up & Restore Test.
--------	--

UE 34.	[OP] Opdrachtnemer werkt in aanvulling op UE 33 mee aan het implementeren van eventuele verbeterpunten.
--------	--

Calamiteit

Een Calamiteit kan optreden als de Productie-omgeving, of de Gegevens daarop, volledig onbeschikbaar worden. In een dergelijke situatie mag er geen sprake zijn van inbreuk op Integriteit en Vertrouwelijkheid van de Gegevens. Opdrachtnemer is hierop voorbereid door het opstellen van een Calamiteitenplan (Disaster Recovery Plan).

Het is noodzakelijk minimaal 1x per jaar een test uit te voeren om te controleren of de ITSM-oplossing naar aanleiding van gesimuleerde noodsituaties kan worden hersteld en daarna kan blijven functioneren, zoals overeengekomen.

Opdrachtnemer werkt mee aan het implementeren van eventuele verbeterpunten die van toepassing zijn op de ITSM-oplossing zelf.

Afspraken hierover worden in een DAP met de Belastingdienst vastgelegd.

UE 35.	Opdrachtnemer conformeert zich aan bovenstaande alinea m.b.t. het uitvoeren en de uitkomsten van een Disaster Recovery Test.
--------	--

3.3.11. Monitoring, Alerting & Logging

De Opdrachtgever wil zicht hebben op afwijkingen op de werking van de ITSM-oplossing om herstelacties te kunnen formuleren en zo mogelijk in de toekomst te voorkomen. Denk aan (ongeautoriseerde) toegang tot de ITSM-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.

De ITSM-oplossing (inclusief raakvlaksystemen en tooling) wordt volcontinu gemonitord op verstoringen en 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.

Excepties, zoals bijvoorbeeld in geval van blokkerende applicatieve fouten, worden gelogd.

Beveiligingsinbreuken worden daarnaast gelogd voor forensisch onderzoek.

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

Logregels bevatten minimaal:

- 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 gelogd moeten worden zijn:

- Authenticatie/autorisatie pogingen, inloggen en uitloggen;
- Acties die betrekking hebben op gebruikersprofielen, bestanden en databases of systeemservices;
- Transacties tussen systemen;
- Activatie en/of de-activering van beveiligingsfunctionaliteit;
- Niet gespecificeerd gedrag van systemen en applicaties (uitzonderingen, fouten en storingen);
- Beveiligingsincidenten.

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 ITSM-oplossing gecompromitteerd kan worden

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. Procedures voor kennisgeving en afhandeling sluiten aan op die van de Belastingdienst; zie hiervoor Bijlage 16 Aansluitvoorwaarden Operational Intelligence.

Afspraken hiervoor moeten worden beschreven in een DAP met de Belastingdienst.

GUE 108.	[CL] De ITSM-oplossing voldoet aan de voorwaarden zoals beschreven in bovenstaande alinea's, inclusief de voorwaarden van Bijlage 16 Aansluitvoorwaarden Operational Intelligence.
GUE 109.	[OP] In aanvulling op GUE 108 geldt dat de ITSM-oplossing volcontinu wordt gemonitord en excepties worden gelogd conform Bijlage 18 20200127-Standaard-Technische-beveiligings-logging-IV. De logfunctie van de ITSM-oplossing moet gekoppeld worden aan de centrale logvoorziening van de Opdrachtgever; zie hiervoor Bijlage 16 Aansluitvoorwaarden Operational Intelligence. Afspraken hiervoor moeten worden beschreven in een DAP met de Belastingdienst.
GUE 110.	De ITSM-oplossing ondersteunt het instellen van loglevels en onderscheidt hier minimaal info-, error- en fatal-meldingen in.
GUE 111.	De ITSM-oplossing biedt de mogelijkheid voor functioneel beheerders om na een foutsituatie Gegevens te herstellen zodat de gebruiker zijn/haar werk kan hervatten.

3.3.12. Autorisatie & Authenticatie

GUE 112.	[OP] De ITSM-oplossing voldoet aan de aansluitvoorwaarden van Bijlage 17 Aansluitvoorwaarden LTB 1.0.
GUE 113.	Voor authenticatie sluit de ITSM-oplossing aan op de Belastingdienst Active Directory via een van volgende opties: 1. Een SAMLv2/OpenID Connect aansluiting op de Federated Identity Hub* die vertaling doet van het Kerberos token naar een SAML token of 2. Native Windows authenticatie aansluiting op Belastingdienst Active Directory of 3. Secure LDAP bind naar de Belastingdienst Active Directory. Ad 2) Er mag alleen gebruik gemaakt worden van door Microsoft ondersteunde en actuele protocollen. Dit betekent bijvoorbeeld dat SMB v1 (en binnenkort SMB v2), LM/NTLM non-secure LDAP, SSLv3 en WINS niet zijn toegestaan. Inschrijver geeft in een toelichting aan in hoeverre en op welke wijze de ITSM-oplossing authenticatie via de Belastingdienst authenticatiediensten ondersteunt. De toelichting wordt bij de Inschrijving ingediend als Bijlage XIV, toelichting op GUE 113. *Ping Federate is de standard federation service van de Belastingdienst en heeft de voorkeur boven ADFS.
GUE 114.	De communicatie over het netwerk van de wachtwoorden van gebruikers in relatie met de ITSM-oplossing is versleuteld.
Toegang tot ITSM-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 ITSM-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 ITSM-oplossing is technisch zodanig ingericht zodat deze principes zijn voldaan.	
GUE 115.	De ITSM-oplossing voldoet aan wat in bovenstaande alinea is beschreven.
GUE 116.	[CL] De ITSM-oplossing voorziet in een multi-factor authenticatiemechanisme voor gebruikers met verhoogde rechten. Denk hierbij bijvoorbeeld aan Beheerders.
GUE 117.	De ITSM-oplossing bevat maatregelen om ongeautoriseerde toegang tot de ITSM-oplossing uit te sluiten

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 36.	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, behoeftebestellers en leveranciers begeleiden in het vormgeven van de duurzaamheidsaspecten in producten en diensten op het vlak van bedrijfsvoering, bij aanbestedingen en gedurende de looptijd van de contracten (maatschappelijk verantwoord inkopen).

Maatschappelijk Verantwoord Inkopen (MVI) binnen de overheid is een uitvloeisel van een politiek besluit. Sinds 2010 is de rijksoverheid verplicht 100% duurzaam in te kopen. Door gelijktijdig milieu-, sociale- en economische afwegingen in alle aankopen mee te nemen leidt dit tot winst voor de belastingbetaler, de overheidsorganisatie en de samenleving.

Het nieuwe regeerakkoord stelt dat de overheid zijn inkoopkracht beter gaat benutten voor het versnellen van duurzame transities, inschakelen van kwetsbare groepen en om innovatief in te kopen.

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

5.1. Energie & Klimaat

Onder dit thema vallen onder andere:

- Energiegebruik;
- CO₂ reductie en
- Duurzame energie opwekking

100% CO₂-compensatie dienstreizen

Nederland moet voor 2030 de helft minder CO₂ 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 CO₂-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 CO₂ vanwege dienstreizen van medewerkers van de Inschrijver voor 100% te compenseren.

W 6	Geef aan of alle vrijgekomen CO₂ vanwege dienstreizen van medewerkers van de Inschrijver 100% gecompenseerd wordt. Aleen CO₂-credits worden geaccepteerd waarvoor de CO₂-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: <table> <tr> <td>Alle vrijgekomen CO₂ vanwege dienstreizen wordt 100% gecompenseerd</td><td>15 punten</td></tr> <tr> <td>Niet alle vrijgekomen CO₂ vanwege dienstreizen wordt 100% gecompenseerd</td><td>0 punten</td></tr> </table> De Inschrijver toont met een onderstaande mogelijke bewijsmiddelen aan dat aan het criterium is voldaan:	Alle vrijgekomen CO ₂ vanwege dienstreizen wordt 100% gecompenseerd	15 punten	Niet alle vrijgekomen CO ₂ vanwege dienstreizen wordt 100% gecompenseerd	0 punten
Alle vrijgekomen CO ₂ vanwege dienstreizen wordt 100% gecompenseerd	15 punten				
Niet alle vrijgekomen CO ₂ vanwege dienstreizen wordt 100% gecompenseerd	0 punten				

- Een Gold Standard certificaat (Informatie over Gold Standard is verkrijgbaar via goldstandard.org (Engelstalig));
- Een ander gelijkwaardig certificaat;
- Een ander gelijkwaardig bewijsmiddel.

Duurzame energieopwekking

Op de website van PIANOo zijn voorbeelden gegeven met betrekking tot het gebruik van energie uit duurzame bronnen: <https://www.piano.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 ITSM-oplossing gehost wordt CO² neutraal is. Het beoordelingscriterium voor deze Wens is: <table> <tr> <td>Van 96 % tot en met 100%</td><td>222 punten;</td></tr> <tr> <td>Van 91 % tot 95%</td><td>133 punten;</td></tr> <tr> <td>Van 81 % tot 90%</td><td>89 punten;</td></tr> <tr> <td>Van 71 % tot 80%</td><td>56 punten;</td></tr> <tr> <td>Van 61 % tot 70%</td><td>33 punten;</td></tr> <tr> <td>Van 51 % tot 60%</td><td>11 punten;</td></tr> <tr> <td>Van 41 % tot 50%</td><td>4 punten;</td></tr> <tr> <td>Van 0 % tot 40%</td><td>0 punten.</td></tr> </table> De Inschrijver toont dit met een bewijs aan waaruit blijkt dat aan dit criterium is voldaan.	Van 96 % tot en met 100%	222 punten;	Van 91 % tot 95%	133 punten;	Van 81 % tot 90%	89 punten;	Van 71 % tot 80%	56 punten;	Van 61 % tot 70%	33 punten;	Van 51 % tot 60%	11 punten;	Van 41 % tot 50%	4 punten;	Van 0 % tot 40%	0 punten.
Van 96 % tot en met 100%	222 punten;																
Van 91 % tot 95%	133 punten;																
Van 81 % tot 90%	89 punten;																
Van 71 % tot 80%	56 punten;																
Van 61 % tot 70%	33 punten;																
Van 51 % tot 60%	11 punten;																
Van 41 % tot 50%	4 punten;																
Van 0 % tot 40%	0 punten.																

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: <table> <tr> <td>Medezeggenschap van de medewerker is geregeld</td><td>43 punten;</td></tr> <tr> <td>Er zijn stimulerende maatregelen getroffen die bijdragen aan de gezondheid van de werknemer</td><td>20 punten;</td></tr> <tr> <td>Geen van bovengenoemde onderdelen</td><td>0 punten.</td></tr> </table> Op deze Wens kunnen maximaal 63 punten worden behaald.	Medezeggenschap van de medewerker is geregeld	43 punten;	Er zijn stimulerende maatregelen getroffen die bijdragen aan de gezondheid van de werknemer	20 punten;	Geen van bovengenoemde onderdelen	0 punten.
Medezeggenschap van de medewerker is geregeld	43 punten;						
Er zijn stimulerende maatregelen getroffen die bijdragen aan de gezondheid van de werknemer	20 punten;						
Geen van bovengenoemde onderdelen	0 punten.						

5.3. Social Return on Investment

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

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

De gehele overheid (Rijk, provincies, waterschappen en gemeenten) doet de laatste jaren steeds meer ervaring op met het leveren van een bijdrage aan deze doelstelling. Door social return op te nemen in aanbestedingen binnen de categorie 'werken' en 'diensten' met een loonsom hoger dan € 250.000,00 exclusief BTW, wil de Rijksoverheid een extra impuls geven aan social return.

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

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

UE 37.	Tijdens de looptijd van de Overeenkomst besteedt de Opdrachtnemer gedurende de looptijd van de Overeenkomst minimaal 5% van het totaal betaalde (technisch) Beheer en afgenomen Consultancy ex. BTW per jaar aan extra werk(ervarings)plaatsen voor mensen uit genoemde social return doelgroepen.
UE 38.	Na het tekenen van de Overeenkomst stemmen Partijen met elkaar af over de wijze waarop invulling wordt gegeven aan social return.
UE 39.	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 40.	Wanneer op basis van de periodieke verantwoordingsformulieren de Opdrachtgever constateert dat de Opdrachtnemer gedurende de looptijd van de Overeenkomst twee maal achtereenvolgend niet aan de verplichting voldoet zoals beschreven in UE 37, dan kan de Opdrachtnemer in overleg kan treden met Opdrachtnemer. 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 41.	Bij het niet nakomen van de verplichting genoemd in UE 37, kan de Opdrachtgever naar rato van de bijdrage social return die de Opdrachtnemer moest doen, betalingen inhouden of storeren op de waarde van de Overeenkomst, met uitzondering in die situaties dat het voldoen aan de verplichting genoemd in UE 37 buiten de schuld van de Opdrachtnemer om niet lukt(e). De bewijslast rust te allen tijde bij de Opdrachtnemer.

5.4. Internationale sociale voorwaarden

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.

GUE 118.	Inschrijver zal 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 42.	Opdrachtnemer dient rekening te houden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2 Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: • Opdrachtgever, www.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.

Hoofdstuk 6. Juridische kaders

Concept Overeenkomst

De in Bijlage X 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 119.	Inschrijver gaat akkoord met de concept Overeenkomst met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen zoals genoemd in deze paragraaf.
----------	--

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.

Hoe de Opdrachtnemer en de Opdrachtgever samenwerken wordt vastgelegd in een Dossier Afspraken en Procedures (DAP). 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 op te stellen. In paragraaf 10.2 staat hierover meer informatie.

GUE 120	Inschrijver gaat akkoord met de werkwijze om pas na gunning gezamenlijk een SLA en DAP inclusief gevraagde procedures op te stellen.
---------	--

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.

Gegevens dienen verwerkt (onder andere: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen) te worden in de EU en landen waarvan de Europese Commissie bepaald heeft dat in deze landen een passend beveiligingsniveau is.

Zie hiervoor: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu#hoe-weet-ik-of-een-derde-land-een-passend-beschermingsniveau-heeft-1752>

GUE 121.	[CL] Inschrijver verklaart 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. Inschrijver levert het bewijs aan als Bijlage XV van de Inschrijving.
----------	---

UE 43.	[CL] Opdrachtnemer heeft (technische) maatregelen getroffen om te voorkomen dat Gegevens van de Aanbestedende dienst geleverd (kunnen) worden aan andere partijen die niet onder Nederlandse of Europese wetgeving vallen.
--------	---

Hoofdstuk 7. Prijsstelling

7.1. Algemene eisen ten aanzien van Prijzen

In de in Bijlage VIII 1.1 “Prijzenformulier” geoffeerde Prijzen dienen alle kosten voor de ITSM-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;
- Het verstrekken van de benodigde toegangscodes voor gebruik van de ITSM-oplossing;
- Materialen en Documentatie vereist voor het gebruik van de ITSM-oplossing.

UE 44.	Kosten die niet in de Inschrijving genoemd worden en niet verdisconteerd zijn in de Prijzen, maar toch noodzakelijk blijken te zijn voor een optimaal functioneren van de Prestatie conform de in de Aanbestedingsstukken gestelde eisen én de in de Inschrijving opgenomen beantwoording van de wensen, kan Opdrachtnemer niet in rekening brengen bij Opdrachtgever.
GUE 122.	Eventuele valutarisico's zijn volledig voor rekening van Opdrachtnemer en worden geacht in de geoffeerde Prijzen te zijn verwerkt.
GUE 123.	Alle geoffeerde tarieven met betrekking tot Technisch Beheer, Consultancy en Opleidingen zijn inclusief reis- en verblijfkosten.
UE 45.	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 1.1 “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

De Aanbestedende dienst beseft dat het onmogelijk is Prijzen en/of Tarieven voor 20 jaar af te geven. Voor het bepalen van de Vergelijkingswaarde moet Inschrijver bij het invullen van het Prijzenformulier uitgaan van de huidige Prijzen en/of Tarieven.

Tabblad Samenvatting

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

Tabblad ITSM versus best practices

In dit tabblad vult de Inschrijver in de gele velden voor de on-premises en de Cloud variant in welke onderdelen van de ITSM-oplossing de betreffend best practice is opgenomen. Uit de eerder gehouden RFI is naar voren gekomen dat hier verschillen in zitten.

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 Behandelaren in de Ontwikkel-, Test- en Acceptatieomgeving genoemd, dezelfde unieke Behandelaren zijn als in de Productieomgeving. Voor jaar 1 geldt dus het totaal aantal Behandelaren over de gehele OTAP maximaal 500 is.

Tabblad 1a Gebruiksrecht – On-premises (Best Practices 1 tot en met 13)

In dit tabblad vult Inschrijver op basis van de dimensionering in dit tabblad én de overige dimensionering van het tabblad Dimensionering in de gele cellen de kosten per jaar en een eventueel kortingspercentage in.

Voor de jaren 3 tot en met 6 is er de mogelijkheid een kortingspercentage aan te geven vanwege mogelijk gebruik van de ITSM-oplossing in de On-premises én Cloud variant.

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

Tabblad 1b Gebruiksrecht – Cloud (Best Practices 1 tot en met 21)

In dit tabblad vult Inschrijver op basis van de dimensionering in dit tabblad én de overige dimensionering van het tabblad Dimensionering in de gele cellen de kosten per jaar en een eventueel kortingspercentage in.

Voor de jaren 3 tot en met 6 is er de mogelijkheid in de gele cellen een kortingspercentage aan te geven vanwege mogelijk gebruik van de ITSM-oplossing in de On-premises én Cloud variant.

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

Tabblad 1c Gebruiksrecht – Cloud (Best Practices 22 tot en met 34)

In dit tabblad vult Inschrijver op basis van de dimensionering in dit tabblad én de overige dimensionering van het tabblad Dimensionering in de gele cellen de kosten per jaar en een eventueel kortingspercentage in.

Omdat het hier om Best Practices die eventueel pas ná jaar 8 worden afgenomen is er voor gekozen om de kosten per jaar op basis van de huidige prijzen te vragen, maar deze niet voor de volledige looptijd door te berekenen. Voor de Best Practices 22 tot en met 34 worden de kosten voor 3 meegenomen in de Vergelijkingswaarde.

Mocht uit ‘**Tabblad ITSM versus best practices**’ bijvoorbeeld naar voren komen dat Best Practice 23, 25 en 27 als één geheel wordt aangeboden, dan vult Inschrijver alleen de cellen onder Best Practice 23 in.

De Opdrachtgever behoudt zich het recht voor om, op het moment dat één of meerdere van deze genoemde Best Practices afgenomen gaan worden, de dan geldende Prijzen te toetsen bij een onafhankelijke partij zoals Gartner, Forrester o.i.d.

Tabblad 2 Diensten Beheer

Inschrijver vult het tarief per jaar in.

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

Tabblad 3 Additionele Diensten

Consultancy

Inschrijver vult m.b.t. de Consultancy een dagtarief.

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

Opleiding

Inschrijver vult m.b.t. de Opleiding op gegevens van een opleiding/training in voor 10 functioneel beheerders.

Doel is deze medewerkers bekend te maken met in 1e instantie de eerste 13 best Practices van de aangeboden ITSM-oplossing.

Inschrijver heeft hierbij de mogelijkheid een kortingspercentage aan te bieden, de groepsgrootte en het aantal sessies te bepalen. De voorkeur gaat uit naar één sessie.

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 EMVI-grafiek

Inschrijver kan 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

Omdat in het Prijzenformulier voor de Abonnementen alleen de kosten per jaar moeten worden aangegeven, is er geen inzicht in het afrekenmodel van de Inschrijver. Omdat de Overeenkomst lang loopt en niet meteen de volle omvang van de dimensionering wordt afgenomen én deze informatie wel gewenst is, wordt van Inschrijver verwacht uit toelichting bij de Inschrijving in te dienen.

In de toelichting moeten de navolgende zaken beschreven worden:

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

GUE 124. Inschrijver levert op basis van bovenstaande als Bijlage XVI een toelichting bij het Prijzenformulier (Bijlage VIII.1.1) bij de Inschrijving in.

Zowel tekstueel als rekenkundig moet expliciet en duidelijk en eenduidig herleidbaar te zijn hoe de jaarbedragen in verhouding staan met de genoemde dimensionering en de in het tabblad "Dimensionering" gegeven uitgangspunten. Hierbij moet onder andere gedacht worden aan de grondslag(en) van de aangeboden Abonnementen/Gebruiksrechten, de gebruikte staffels met aantallen, prijsstellingen per eenheden (staffel) en de benodigde aantallen en hoe deze correleren met de aangegeven dimensionering. Hierbij is ook een mogelijkheid om een Abonnement/Gebruiksrecht, aan te beiden voor bijvoorbeeld Onbeperkt gebruik.

GUE 125. Het is niet toegestaan om negatieve Prijzen die de gehanteerde berekeningen frustreren of die bij voorbaat objectief niet afzonderlijk kunnen worden nagekomen, te offren.

7.4. Indexering Prijs

De door Inschrijver geoffreerde Prijzen zoals opgegeven in het spreadsheet Prijzenformulier, Bijlage VIII.1.1, mogen vanaf 2024 jaarlijks en steeds per jaarlijkse verlengdatum geïndexeerd worden op basis van de CBS tabel 'CAO-lonen, contractuele loonkosten en arbeidsduur, indexcijfers (2010 = 100)'; onderwerp: CAO- lonen incl. bijz. beloningen; SBI2008: M-N Zakelijke dienstverlening, of de opvolger van deze index, conform de volgende webpagina:

<https://opendata.cbs.nl/statline/#/CBS/nl/dataset/82838NED/table?dl=74C6F>

De door Inschrijver geoffreerde Prijzen voor het Gebruiksrecht zoals opgegeven in het spreadsheet Prijzenformulier, Bijlage VIII.1.1, in tabbladen '1a...' '1b...' en '1c...' mogen vanaf 2024 jaarlijks en steeds jaarlijkse verlengdatum geïndexeerd worden op basis van de CBS-tabel Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2015 = 100 (CPA2008, kwartaalindex), of de opvolger van deze index, conform de volgende webpagina:

<https://opendata.cbs.nl/#/CBS/nl/dataset/83760NED/table?dl=74C78>

Prijsaanpassingen dienen uiterlijk twee maanden voor het verlengingsmoment aan de contractmanager ter goedkeuring te worden aangeboden, waarbij het op dat moment – door het CBS – meest recent beschikbare en gepresenteerde indexcijfer, Jaarmutatatie 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 voor de tarieven van Consultancy op 1 september 2022 geïndexeerd had mogen worden, was de prijsindexatie 2,8% geweest (jaarmutatatie DPI 2e kwartaal 2022, op dat moment meest recent beschikbare indexcijfer).

UE 46. De door de Opdrachtnemer geoffreerde Prijzen mogen jaarlijks per 15 juni geïndexeerd worden conform paragraaf 7.4. De eerste indexering vindt plaats niet eerder dan 2 jaar na ingaan van de Overeenkomst.

UE 47.	Opdrachtnemer dient 2 maanden voorafgaande aan de genoemde momenten van indexering, een schriftelijk verzoek in met bijbehorende onderbouwing om voor de indexering in aanmerking te komen.
--------	---

Hoofdstuk 8. Documentatie, Opleiding en Consultancy

8.1. Documentatie

UE 48.	Opdrachtnemer zal Opdrachtgever tijdig voorzien van actuele en volledige Documentatie in elektronische vorm met betrekking tot Installatiewerkzaamheden en/of het gebruik van de Prestatie. Hierbij is de Documentatie over de eigenschappen en gebruiksmogelijkheden van de ITSM-oplossing in de Nederlandse en/of Engelse taal.
UE 49.	De Documentatie dient zodanig te zijn dat zij een juiste, volledige en gedetailleerde beschrijving geeft van de door Opdrachtnemer te leveren ITSM-oplossing en de functies daarvan, zodat Eindgebruikers op eenvoudige wijze van alle mogelijkheden van de ITSM-oplossing gebruik kunnen maken.
UE 50.	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 ITSM-oplossing.
UE 51.	Opdrachtgever mag de Documentatie voor gebruik binnen de eigen organisatie reproduceren en wijzigen.
UE 52.	Opdrachtnemer zal de door hem geleverde Documentatie zo spoedig mogelijk vervangen, wijzigen of aanpassen indien op enig tijdstip tijdens het gebruik door Opdrachtgever van de Prestatie, blijkt dat de Documentatie onjuiste informatie bevat of anderszins onvolledig, onvoldoende, onduidelijk en/of verouderd is.
UE 53.	Opdrachtnemer is verantwoordelijk dat Documentatie na een nieuwe Release actueel blijft. Na oplevering van een nieuwe Release wordt de geactualiseerde Documentatie digitaal beschikbaar gesteld.
UE 54.	Opdrachtnemer geeft in de Documentatie de in de Release opgenomen aanpassingen duidelijk weer.

8.2. Opleiding

UE 55.	Opdrachtnemer levert relevante Opleidingen, inclusief Documentatie, inzake het gebruik van de ITSM-oplossing, alsmede het functioneel, technisch en applicatie beheer van de ITSM-oplossing.
UE 56.	Opleidingen vinden plaats op locatie van de Opdrachtgever tenzij nadrukkelijk anders overeengekomen.
UE 57.	De Opleidingen vinden plaats in Nederland in de Nederlandse taal.
UE 58.	Opdrachtnemer stelt voor de Eindgebruikers de goedgekeurde gebruikersinstructie online beschikbaar gedurende de looptijd inclusief verlengingsopties van de Overeenkomst en houdt deze actueel.
UE 59.	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 60.	Lesmateriaal voor Eindgebruikers is in de Nederlandse of Engelse taal beschikbaar.

8.3. Consultancy

UE 61.	Opdrachtnemer spant zich in om binnen 1 maand na opdrachtverstrekking tot het leveren van Consultancy een geschikte consultant voor de Aanbestedende dienst beschikbaar te hebben.
--------	--

Hoofdstuk 9. Voorbereiding- en Implementatiefase

9.1. Installatie & Integratie

Na het contracteren moet als eerste stap de ITSM-oplossing op de infrastructuur van de Belastingdienst geïnstalleerd te worden. Opdrachtgever stelt één van haar platformen beschikbaar. Inschrijver heeft in de Inschrijving aangegeven op welk platform het de ITSM-oplossing aanbiedt.

Dit resulteert uiteindelijk in een OTAP-straat waarop de ITSM-oplossing is geïnstalleerd en gereed is voor het functioneel inrichten voor de fase van initiële configuratie, migratie en doorontwikkeling.

De ITSM-oplossing is na afronding van deze fase geïntegreerd in de infrastructuur van de Opdrachtgever (inclusief aangesloten op de monitoring, logvoorziening en AD van de Belastingdienst) én voldoet aan de SLA-eisen. De Acceptatie vindt plaats door medewerkers van team Tooling en de technische Beheerders die u beschikbaar stelt voor de operationele fase.

De Opdrachtgever wil hierbij (zo veel mogelijk) geadviseerd worden in het op de beste en meest efficiënte manier van installeren, integreren, inrichten van de aangeboden ITSM-oplossing op de infrastructuur van de Opdrachtgever voor de 1^e 13 practices en de migratie van ICD naar de aangeboden ITSM-oplossing.

W 9	Met betrekking tot bovenstaande alinea's vraagt Opdrachtnemer een plan van aanpak waarin Inschrijver schetst hoe deze de installatie, integratie, inrichting van de ITSM-oplossing op de infrastructuur van Opdrachtgever aanpakt evenals de migratie van ICD naar de aangeboden ITSM-oplossing, inclusief een uitgebreide en betrouwbare inschatting gemaakt van de realisatie en acceptatie. Het plan bevat minimaal de volgende onderwerpen: - Een duidelijk fasering die een beheerste control op de voortgang mogelijk maakt; - Een duidelijk opzet t.a.v. projectgovernance; - Inhoudelijke aanpak om te komen tot een werkende ITSM-oplossing op de infrastructuur van de Belastingdienst; - Verwachte bijdrage van Opdrachtgever om de installatie en integratie van de infrastructuur van de Opdrachtgever succesvol uit te kunnen voeren; - Inschatting van de benodigde inzet (projectmanagement, architect, beheerder, BizDevOps engineer) per deliverable/projectonderdeel, waarbij tevens doorlooptijden worden aangegeven; - Beschrijving van een helder acceptatie proces, waarbij acceptatie altijd door Opdrachtgever gebeurt op basis van positief verlopen acceptatietesten; - Blijk geven dat de Inschrijver de problematiek van Opdrachtgever heeft begrepen en de Opdrachtgever daadwerkelijk helpt bij de installatie, integratie, inrichting en migratie gegeven de meegeven IST situatie en geschetste aanpak zoals beschreven in paragraaf 1.5. Het plan van aanpak is, exclusief voorblad, inhoudsopgave en afbeeldingen, maximaal 5 pagina's. Hyperlinks en/of verwijzingen naar andere documenten en/of websites zijn niet toegestaan. Voor deze Wens geldt de volgende waardering: <table> <tr> <td>0</td><td>Zeer slecht;</td></tr> <tr> <td>52</td><td>Slecht;</td></tr> <tr> <td>261</td><td>Matig;</td></tr> <tr> <td>435</td><td>Voldoende;</td></tr> <tr> <td>1.130</td><td>Goed;</td></tr> <tr> <td>1.739</td><td>Uitstekend.</td></tr> </table> 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.	0	Zeer slecht;	52	Slecht;	261	Matig;	435	Voldoende;	1.130	Goed;	1.739	Uitstekend.
0	Zeer slecht;												
52	Slecht;												
261	Matig;												
435	Voldoende;												
1.130	Goed;												
1.739	Uitstekend.												

9.2. Documentatie, Opleiding en Consultancy

UE 62.	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 63.	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 64.	In geval van uitstel of vertraging van de Implementatie van de Prestatie en/of in het geval de Aflevering van de Apparatuur 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.
--------	--

9.2.2. Voortbrenging van (onderdelen) van de ITSM-oplossing

Voortbrenging van Programmatuur en systeemonderdelen van de ITSM-oplossing gebeurt op basis van 'Security by Design'-principes. Beveiliging is vanuit het ontwerp geborgd, op een correcte manier geïmplementeerd en zowel proces als output wordt regelmatig geëvalueerd.
Als er open sourcecode wordt gebruikt dan is hier expliciet aandacht voor.

Dit is ook van toepassing op mobiele apps en de back-end daarvan. Bij Secure Software Development-processen kan gedacht worden aan ASVS en MASVS (zie website www.owasp.org of gelijkend).

GUE 126	De gangbare principes rondom 'Security by Design' en 'Security by Default' zijn uitgangspunt voor het ontwerp en de ontwikkeling van de Programmatuur van de ITSM-oplossing ondersteund door een secure software development life-cycle.
---------	--

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/>). Er moet minimaal een A-score behaald te worden. Zet 'Hide results' aan.

GUE 127.	Indien van toepassing op de ITSM-oplossing, dan voldoet de ITSM-oplossing aan bovenstaande alinea. Op deze Eis kan ingeval het niet van toepassing, met NVT worden geantwoord.
----------	--

Hoofdstuk 10. Beheer en Onderhoud & Support

10.1. Technisch Beheer & Consultancy

Opdrachtnemer is gehouden tot het leveren van Technisch Beheer en Consultancy ten behoeve van de ITSM-oplossing.

UE 65.	[OP] Opdrachtnemer voert het Technisch Beheer en Consultancy uit op locatie van Opdrachtgever, tenzij nadrukkelijk (schriftelijk) anders is overeengekomen.
UE 66.	[OP] Opdrachtnemer conformeert zich dat werknemers voor zowel Technisch Beheer als Consultancy van Opdrachtnemer voor de werkzaamheden alleen gebruik maken van een werkplekomgeving van de Opdrachtgever.
UE 67.	[OP] Opdrachtnemer conformeert zich dat werknemers voor zowel Technisch Beheer als Consultancy van Opdrachtnemer die voor werkzaamheden worden ingezet, minimaal 4 werkdagen per week beschikbaar zijn.
UE 68.	[OP] Opdrachtnemer levert medewerkers voor zowel Technisch Beheer als Consultancy die voldoen aan de rolbeschrijvingen zoals beschreven in Bijlage 7 Rolbeschrijvingen 1.1.
UE 69.	[OP] Opdrachtnemer zorgt ervoor dat bij uitval van een medewerker voor zowel Technisch Beheer als Consultancy, door bijvoorbeeld ziekte, er een vervanger beschikbaar is die over minimaal dezelfde kennis en kunde beschikt als de uitgevallen medewerker.
UE 70.	[OP] Om een Agile-team goed te laten werken is een stabiel vast team noodzakelijk. Het is daarom niet de bedoeling dat er wisselingen plaatsvinden in het team. Wisselingen van medewerkers voor zowel Technisch Beheer als Consultancy is alleen na onderling overleg toegestaan.
UE 71.	[OP] Opdrachtnemer conformeert zich dat een medewerker van de Opdrachtnemer die wordt ingezet, minimaal een (1) jaar meedraait / beschikbaar is in het Agile-team.

10.2. Onderhoud & Support

Opdrachtnemer is gedurende de looptijd van de Overeenkomst gehouden tot het leveren van Onderhoud & Support ten behoeve van ITSM-oplossing.

Service Level Agreement (SLA)

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

GUE 128.	Inschrijver levert bij inschrijving, op basis van de inhoud van Bijlage A 'Specificaties van de opdracht' gespecificeerde Service Levels, een concept SLA op. De SLA beschrijft in elk geval de wijze waarop door Opdrachtnemer invulling wordt gegeven aan derde lijns Onderhoud & Support. Het concept SLA wordt als Bijlage XVII concept SLA bij de Inschrijving ingediend.
----------	--

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, datalekken);

- Change-en releasemanagement (waaronder security patches en significante juridische en infrastructurele wijzigingen);
- Continuïteit (BCM);
- Securitymanagement;
 - Incident- en problemmanagement;
 - Audits, beveiligingstesten (A&P-testen, vulnerability scans) en continuïteitstesten (Back-up & Restore, Calamiteitentests);
 - Stekkermandaat;
 - Monitoring, alerting en logging.
- Rapportage

Rapportage

Opdrachtnemer rapporteert maandelijks in ieder geval over het volgende:

- KPI opgeloste beveiligingsincidenten/-problems.
- Status, voortgang en afhandeling van openstaande en opgeloste vragen, beveiligingsincidenten, -problems en -verbetervoorstellen. Hierbij wordt aangegeven: datum ontvangst, datum in behandeling, verwachte opleverdatum en datum afgevoerd.
- Cumulatieve rapportage (minimaal 14 maanden) over bovenstaande voor trend-analyse.

Opdrachtnemer rapporteert jaarlijks in ieder geval over het volgende:

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

Opdrachtnemer rapporteert m.b.t. de Cloud variant van de ITSM-oplossing jaarlijks de data wanneer onderstaande aspecten plaatsvinden:

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

UE 72.	Opdrachtnemer stelt in overleg met de Aanbestedende dienst na gunning én binnen 3 maanden na de ingangsdatum van de Overeenkomst, op basis van het ingediende concept SLA, de definitieve SLA op waarin alle, in de aanbestedingsstukken gevraagde onderwerpen zijn opgenomen.
UE 73.	De SLA wordt binnen 3 weken 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 tenminste Onderhoud & Support te verlenen op de voorlaatste (verse n-1) en nieuwste versie (versie n) van de ITSM-oplossing.
UE 75.	Opdrachtnemer verplicht zich om in overleg met de Opdrachtgever een Governance procedure te beschrijven in geval er escalaties optreden.
UE 76.	Opdrachtnemer stelt contactpersonen beschikbaar voor: • Een vast aanspreekpunt voor SLA-aspecten; • Een vast specifiek aanspreekpunt voor afhandelen van beveiligingsonderwerpen; • Een vast specifiek aanspreekpunt voor afhandelen van privacy gerelateerde onderwerpen. Dit mag één en dezelfde persoon zijn.

Dossier Afspraken & Procedures (DAP)

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;

- Standaard- en Escalatiecommunicatiestructuur met rollen en contactgegevens;
- Afspraken en Procedures (beveiligings- en privacyincidenten) betreffende:
 - Beschikbaarheid van de Servicedesk;
 - Prioriteriteitsbepaling, reactietijd en oplossingstijd;
 - Melding en afhandeling van incidenten, problems, common vulnerability disclosures en privacygerelateerde incidenten;
 - Release- en patchmanagement. Releasekalender;
 - Aanvraag, uitvoering en afhandeling van audits, beveiligingstesten (A&P-test en Vulnerabilityscan) en continuïteitstesten (Back-up & Restore, Calamiteitentest);
 - Beschikbaar stelling en afhandeling van rapportages van audits, beveiligingstesten en continuïteitstesten van de Opdrachtnemer;
 - Afhandeling van Stekkermanaat (uitvoeren, herstellen);
 - Afspraken rond monitoring, logging en alerting;
 - Wijzigingen van beveiligingsstandaards (Forum van Standaardisatie);
 - Beschikbaar stellen van SLA-rapportages (SNR);
 - Beschikbaarstelling en gebruik van productiegegevens (Stekkermandaat, 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.

UE 77. Opdrachtnemer stelt in overleg met de Aanbestedende dienst na gunning én binnen 3 maanden na de ingangsdatum van de Overeenkomst een DAP op waarin alle, in de aanbestedingsstukken gevraagde onderwerpen, zijn opgenomen.

UE 78. In het DAP is beschreven wat de procedure is hoe om gaan met wijzigingen bij het Forum Standaardisatie met betrekking tot (verplichte) Open Standaarden.

10.2.1. Service Levels

W 10	Geef aan of Inschrijver een in Nederland gevestigde vertegenwoordiging heeft.	
	De beoordelingscriteria voor deze Wens zijn:	
	Ja	200 punten;
	Nee	0 punten.

UE 79. Opdrachtnemer neemt op verzoek deel aan een strategisch-, tactisch- en/of operationeel overleg deel.

W 11	Geef aan of Inschrijver een gebruikersgroep m.b.t. de ITSM-oplossing faciliteert en/of ondersteunt.	
	De beoordelingscriteria voor deze Wens zijn:	
	Ja	800 punten;
	Nee	0 punten.

GUE 129. **Vervallen**

10.2.1.1. Beschikbaarheid

PI	Service Level
Beschikbaarheid 7x24x365	99,5 % per jaar ¹

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

UE 8o.	De ITSM-oplossing voldoet ten minste aan de Beschikbaarheid zoals opgenomen in Tabel 3 Service Levels Helpdesk en Incidentmanagement.
--------	---

GUE 13o	[OP] De ITSM-oplossing is zo ingericht dat bij uitval van 1 van de locaties van het Datacenter, P of Q, de ITSM-oplossing blijft werken.
---------	---

Het is belangrijk te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én hoe snel de Gegevens beschikbaar zijn danwel de ITSM-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 ITSM-oplossing wel of niet te gebruiken is), maar om de excepties als het mis gaat (Calamiteiten en Back-up & Restore). Verwacht wordt dat de ITSM-oplossing bij onbeschikbaarheid binnen bepaalde termijnen weer beschikbaar is zonder verlies van integriteit en vertrouwelijkheid.

10.2.1.2. 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 door middel van het automatisch uitbellen/signaleren van de Oplossing bij de Opdrachtnemer beschouwd als daadwerkelijke Incidenten.

Impact	
Hoog	Een Incident heeft of kan ernstige gevolgen hebben voor • Eén of meer bedrijfsprocessen die de burger en/of het bedrijf direct raken, en/of • Eén of meer fabriekstaken voor (massale) gegevensverwerking en/of • De Informatiebeveiliging en/of • Het imago van de Opdrachtgever en/of • Onacceptabele hoge kosten.
Laag	• Overige situaties
Urgentie	
Hoog	Een Incident • Beïnvloedt kwaliteit van functies/Beschikbaarheid/beveiliging en/of • Brengt integriteit van de Gegevens in het geding en/of • Treedt op tijdens piektijd/-periode van het bedrijfsproces en/of • Brengt uiterste verzenddatum van klantbescheiden in gevaar en/of • Verstoort de communicatie met de klanten van de Opdrachtgever en/of • Er geen Workaround mogelijk is en/of • De verwerking kan niet worden uitgesteld en/of • De schade is al een feit of zal dat zijn binnen 24 uur.
Laag	• Overige situaties
Prioriteit	
	• Impact Hoog / Urgentie Hoog geeft Prio 1; • Impact Hoog / Urgentie Laag geeft Prio 2; • Impact Laag / Urgentie Hoog geeft Prio 2; • Impact Laag / Urgentie Laag geeft Prio 3.

Tabel 2 Impact, Urgentie en Prioriteit

PI	Prioriteit	Service Level	Norm
Openstelling Helpdesk (Portal of email)	Incidenten	7 x 24 uur	99,9 % per jaar
Openstelling Helpdesk (Telefonisch)	Incidenten	07:00 – 21:00 uur	100% op Werkdagen
Openstelling Helpdesk (Portal of email)	Beveiligingsincidenten/ (potentiële) Datalekken	7 x 24 uur	100% voor Prio 1
Service requests		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 VOOR OPLOSSING			
Oplostijd	Prio 1	8 uur	100%
Oplostijd	Prio 2	1 Werkdag	100%
Oplostijd	Prio 3	5 Werkdagen	100%
STREEFTIJD VOOR HERSTEL			
Hersteltijd	Prio 1	2 Werkdagen	98%
Hersteltijd	Prio 2	5 Werkdagen	95%
Hersteltijd	Prio 3	10 werkdagen	90%
Recovery Time Objective (RTO)	n.v.t.	8 klokuren	n.v.t.
Recovery Point Objective (RPO)	n.v.t.	Maximaal 4 klokuren verlies aan Gegevens	n.v.t.

Tabel 3 Service Levels Helpdesk 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 Helpdesk 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 Helpdesk en Incidentmanagement.
UE 83.	Opdrachtnemer geeft ten aanzien van de afhandeling van beveiligingsincidenten en (potentiële) Datalekken 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 131	De voertaal op de Helpdesk is Nederlands en/of Engelstalig.
GUE 132	De ITSM-oplossing bevat een voor iedere gebruiker toegankelijke Knowledge database.
GUE 133.	De Knowledge database beschikt over een zoekfunctie.
GUE 134	Het aanmelden van Events, Incidenten en/of Problems is via meerdere kanalen, bijvoorbeeld via de Self service portal of mail, mogelijk.

10.2.1.3. Release – en Patch management

GUE 135	Inschrijver heeft Patchmanagement ingericht. De bedrijfsvoering is zodanig ingericht dat technische kwetsbaarheden adequaat worden ontdekt, geëvalueerd en geadresseerd. De procedures hiervoor worden in een DAP beschreven.
UE 84.	Opdrachtnemer informeert Opdrachtgever over nieuwe Releases en Patches ten behoeve van het optimaal gebruik van de ITSM-oplossing en de daarbij verwachte Impact voor Opdrachtgever. In het DAP worden afspraken gemaakt op welk tijdstip Opdrachtgever hierover geïnformeerd wordt.
UE 85.	[OP] Het doorvoeren van Releases en Patches ten behoeve van het optimaal gebruik van de ITSM-oplossing wordt in overleg met Opdrachtgever ingepland.
GUE 136	Tijdens het doorvoeren van Releases en Patches blijft de ITSM-oplossing beschikbaar.
UE 86.	Opdrachtnemer levert voorafgaand aan de Release ten behoeve van het optimaal gebruik van de ITSM-oplossing de releasenotes ten behoeve van Acceptatie(test) aan.
UE 87.	Opdrachtnemer stelt Releases door middel van een download beschikbaar. (Om de veiligheid van de transfer van Programmatuur te borgen dient voor het beschikbaar stellen van een Release gebruik te worden gemaakt van Belastingdienst File transfer.)
UE 88.	Gedurende de Overeenkomst is er voor Opdrachtgever een actuele Release kalender van de ITSM-oplossing beschikbaar.
UE 89.	Gedurende de Overeenkomst is er voor Opdrachtgever een actuele roadmap van de ITSM-oplossing beschikbaar, welke minimaal 1x per jaar wordt vernieuwd.
UE 90.	Opdrachtnemer zorgt ervoor dat de nieuwe ontwikkelingen binnen IT4IT en ITIL@4 worden doorgevoerd in Releases en Patches van de ITSM-oplossing. Deze informatie is terug te zien in de roadmap.
UE 91.	Opdrachtnemer informeert Opdrachtgever minimaal 1 jaar over de datum wanneer delen van de ITSM-oplossing EOD en/of EOL en/of EOS zijn.
UE 92.	Opdrachtnemer biedt Opdrachtgever de mogelijkheid om ideeën en wensen aan te dragen met betrekking tot de functionaliteit van de ITSM-oplossing.
GUE 137	De ITSM-Oplossing beschikt over een geautomatiseerd voortbrengingsmechanisme t.b.v. Functionele configuraties. Voorbeeld: In de Testomgeving wordt bijvoorbeeld een workflow ontwikkelt; deze kan dan geautomatiseerd worden voortgebracht naar de productie omgeving.
UE 93.	[OP] Releases van de ITSM-oplossing kunnen worden geïnstalleerd zonder handmatige migratieacties op servers of werkplekken.
W 12	[OP] Geef aan of een Release of Patch teruggedraaid kan worden. De beoordelingscriteria voor deze Wens zijn: Ja Nee 74 punten; 0 punten.

10.2.1.4. Verbeterplan

UE 94.	Indien de ITSM-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.
--

10.2.2. Remote support

Remote support biedt de mogelijkheid om, op ad hoc basis aan een medewerker van de Opdrachtnemer ondersteuning te vragen bij Incidenten, Problems of Changes. Met deze voorziening heeft Opdrachtgever de mogelijkheid Opdrachtnemer, op afstand mee te laten kijken binnen zijn/haar beheerapplicaties met aanvullend hierop het uit handen geven van toetsenbord en muis.

Opdrachtgever kan kiezen of Opdrachtnemer alleen bij een bepaalde applicatie mee kan kijken of dat deze de complete werkplek kan zien. Bij het uit handen geven van de regie krijgt Opdrachtnemer de mogelijkheid om de toetsenbord- en muisacties uit te voeren onder toezicht van de Opdrachtgever. Natuurlijk kan Opdrachtgever te allen tijde de regie terugnemen.

Opdrachtnemers die gebruik willen maken van de Remote support functionaliteit, gaan vooraf akkoord met de huisregels in relatie tot het gebruik van Remote support. Door gebruik te maken van Remote support gaat u akkoord met onderstaande voorwaarden:

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

GUE 138	Inschrijver conformeert zich aan bovenstaande voorwaarden indien gebruik gemaakt wordt van Remote support.
---------	--

10.2.3. Rapportage

UE 95.	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- en/of abonnementsgebruik.
--------	---

UE 96.	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.
--------	---

10.3. 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'.
--------	---

10.4. Factureren en bestellen

Als leverancier bent u verplicht elektronisch te factureren

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

Manieren van e-factureren

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

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

Bekijk de video op de website: [Home | Helpdesk e-factureren \(helpdesk-efactureren.nl\)](https://www.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 boekhoudstelsel of e-facturen versturen via een (commercieel)Peppol-portaal. Peppol is de nieuwe EU standaard voor elektronisch berichtenverkeer met de overheid. Meer informatie over Peppol vindt u op www.peppolautoriteit.nl/

Leveranciersportaal

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

UE 98.	De Opdrachtnemer voldoet, conform Bijlage 5 Bijsluit e-factureren juli 2022, aan de vereisten van e-facturatie via het leveranciersportaal of een geautomatiseerde koppeling met de DigiPoort (toekomstig E-procurementpoort) of het Peppol netwerk met daarin de referentie naar de inkooporder en de inkooporderregel. 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 inkoopordernummer als referentie op elke pakbon en factuur aan Opdrachtgever. Zonder dit Inkoopordernummer 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 Releases van het leveranciersportaal in gebruik genomen kunnen worden.
---------	---

10.5. Kaders voor (re)transitie

10.5.1. Inleiding

In geval van (tussentijdse) beëindiging of afloop van de Overeenkomst van de ITSM-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.

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 Beheer en/of Additionele diensten in de vorm van Consultancy, zoals ingevuld in Bijlage VIII 1.1 Prijzenformulier.

10.5.2. 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 paragraaf 10.5 en volgende 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.	[CL] 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.	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 vernietigt (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 111.	[CL] Naar de Belastingdienst herleidbare domeinnamen en URL's worden onbeschikbaar gemaakt op het internet en domeinnamen worden –zo mogelijk– overgedragen aan de Belastingdienst.
---------	---

UE 112.	[CL] Hergebruik van deze domeinnamen en URL's (n.a.v. UE 111) is niet toegestaan zonder nadrukkelijke toestemming van de Opdrachtgever.
---------	---

10.5.3. (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 113.	Bij overgang naar een nieuwe opdrachtnemer moet de Prestatie voor een periode van minimaal 6 maanden tegen gelijkblijvende condities (naar rato), voor Opdrachtgever beschikbaar blijven.
---------	---

UE 114.	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 115.	Opdrachtnemer houdt voldoende gekwalificeerd personeel beschikbaar voor de Retransitie.
---------	---

UE 116.	Opdrachtnemer verleent medewerking aan een Audit betreffende de inhoud en de kwaliteit van de informatie die Opdrachtnemer in het kader van Retransitie beheerd.
---------	--

UE 117.	Opdrachtnemer dient inzage te geven in de gebruikte middelen en processen tijdens de periode van Retransitie
---------	--

UE 118.	Opdrachtnemer dient onder meer de verbindingen te verbreken, eventueel aan Opdrachtgever ter beschikking gestelde Apparatuur terug te geven, eventuele licenties te verstrekken ten aanzien van de ITSM-oplossing die noodzakelijk is om de omgeving in stand te houden/te blijven beheren; en elektronische sleutels aan Opdrachtgever ter beschikking te stellen.
---------	---