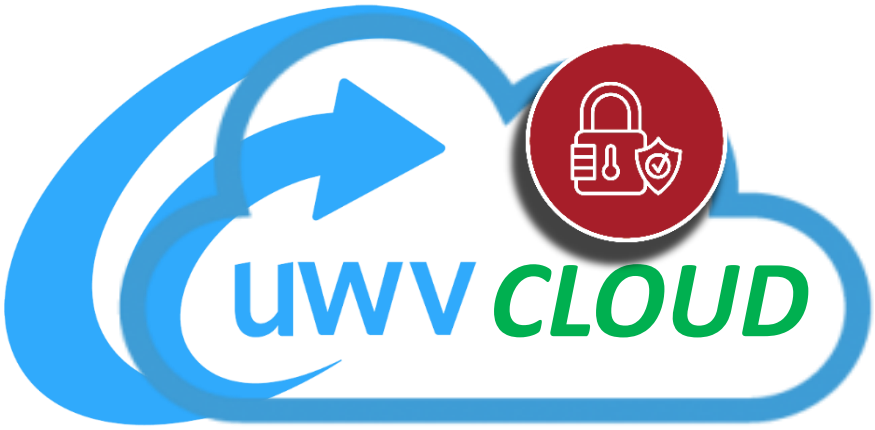
AB 24xxxx / xx x x



Programma van Eisen voor werving van een SaaS oplossing

Chief Information Officer
Versie: 1.2
Datum: 25-06-2025
Opsteller: René Zuidgeest

Managementsamenvatting

Dit document identificeert de eisen en criteria en beschrijft hoe deze kunnen worden meegenomen in de werving van een SaaS-product (Software-as-a-Service). Het doel is dat UWV SaaS-producten verwerft uit het brede marktaanbod die het beste bij UWV passen, niet alleen functioneel, maar ook non-functioneel.

De verwachting is dat het IT-landschap van UWV sterk zal 'ver-saas-en'. UWV heeft zowel te maken met een

- *technology push* waarin softwarefunctionaliteit voor een groot deel wordt aangeboden als SaaS (er is geen alternatief) als met een
- *technology pull* gedreven door ontzorging door de levenscyclus van de software (beheer, doorontwikkeling, etc.) bij de leverancier te leggen.

Derhalve zullen bij UWV veelvuldig SaaS-producten worden aanbesteed, verworven en vervolgens geïntegreerd.

Dit programma van eisen voor het werven van een SaaS-oplossing biedt een cafetariamodel van non-functionele criteria en hoe deze toe te passen in een werving. De criteria zijn ingedeeld naar een aantal domeinen:

- Technische criteria
    - Identiteit (IAM)
    - Integratie
    - Ontwikkeling
    - Beheer
    - Beveiliging
    - Opslag
    - Netwerk
- Business criteria
    - Financiën (FinOps)
    - Dienstverlening (SLA)
    - Ondersteuning

Inhoud

Wijzigingshistorie			
Datum	***Versie***	***Actie***	***Status***
12-09-2024	0.1	Eerste versie.	Draft
05-11-2024	0.2	Commentaar Inkoop verwerkt en set aan criteria uitgebreid.	Draft
04-03-2025	0.3	Eerste complete versie.	Draft
14-03-2025	0.4	Commentaar CCoE verwerkt.	Draft
25-04-2025	0.5	Commentaar Inkoop, JZ, LM verwerkt. Versie wordt naar AB gestuurd, ondanks dat er nog een paar commentaren open staan.	Ter vaststelling AB
09-05-2025	1.0	Commentaar AB verwerkt.	Akkoord AB
23-05-2025	1.1	Document verplaatst naar SaaS - Alle documenten	Akkoord AB
25-06-2025	1.2	Positionering tov forumstandaardisatie.nl toegelicht in 2.1. Commentaar WR verwerkt.	

1. Inleiding

Het UWV Cloudbeleid[1] is door de Raad van Bestuur vastgesteld in augustus 2023. Dit heeft UWV een duidelijk handvat gegeven om waardevolle clouddiensten op verantwoorde wijze te werven en in haar IT landschap te integreren.

In het brede palet aan (publieke) clouddiensten dat hedendaags wordt aangeboden is het overgrote deel van het type Software-as-a-Service (SaaS). Dit gegeven met daarnaast dat UWV het principe 'SaaS boven Paas boven IaaS' hanteert en vergelijkbare functionaliteit steeds minder als softwarepakket in een on-premise variant worden aangeboden, zullen bij UWV veelvuldig SaaS-producten worden aanbesteed, verworven en vervolgens geïntegreerd.[2]

Het is zaak dat UWV een SaaS-product verwerft uit het brede marktaanbod dat het beste bij UWV past, niet alleen functioneel, maar ook non-functioneel[3]. Dat laatste is weer onder te verdelen in IT-technische criteria en business criteria. Door het stellen van eisen aan en toepassing van de juiste criteria op het gebied van IT en business in de evaluatie van SaaS-producten kunnen risico's in een vroeg stadium worden gemitigeerd en pijn in het inrichtingstraject en bij gebruik worden vermeden.

Dit document identificeert deze eisen en criteria en beschrijft hoe deze kunnen worden meegenomen in de werving van een SaaS-product.

2. Positionering en besturing

2.1. Positionering

Dit document betreft een richtlijn. Het UWV Cloudbeleid is leidend en vormt het kader voor deze richtlijn. UWV kent ook architectuurprincipes en er wordt gewerkt naar een doelarchitectuur. SaaS-producten zijn in de regel onderdeel van een totaaloplossing en dienen te worden geïntegreerd in het UWV IT-landschap, conform deze architectuurprincipes en doelarchitectuur. Ook dit perspectief moet worden meegenomen in het opstellen van eisen aan en beoordeling van SaaS-producten.

Het IB&P perspectief en daarmee ook de BIO wordt afgedekt door de Beveiligings- en Verwerkers-overeenkomst[4] (BVO) dat een reeks bepalingen op dit gebied voorschrijft aan de SaaS leverancier. De criteria die betrekking hebben op IB&P (vooral Artikel 8 – Beveiliging) kunnen als additief worden beschouwd. Bij grote wereldspelers die eigen documenten hanteren, is het zaak om datgene wat zij hebben opgesteld te toetsen aan dit PvE SaaS en de BVO. Ontbrekende zaken kunnen dan in het betreffende PvE voor die uitvraag worden meegenomen.

Tot slot dient bij de aanschaf van een ICT-dienst of ICT-product boven de €50.000 voor een toepassingsgebied dat voorkomt op de lijst van www.forumstandaardisatie.nl (zie https://www.forumstandaardisatie.nl/open-standaarden/verplicht) gekozen te worden voor een bij het betreffende toepassingsgebied vermelde open standaard. Er kan worden afgeweken indien een dergelijke dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig is of niet functioneert, of om andere redenen van bijzonder gewicht. Dit dient dan gemotiveerd te worden en opgenomen te worden in het inkoopdossier. Deze eisen zijn dus additief aan de eisen in dit document en dienen te worden meegenomen in het betreffende PvE voor de uitvraag.

2.2. Besturing

De eigenaar van deze richtlijn is de CIO van UWV. Het beheer en doorontwikkeling van deze richtlijn ligt bij het EA-team binnen CIO Office o.l.v. de CTO (manager CIOO/EA), in nauwe samenwerking met Chief Information Security Office (CISO), Leveranciersmanagement (LM) en Inkoop.

---

[1] UWV Cloudbeleid 2.0

[2] How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria (gartner.com): "By 2025, 30% of organizations will rely solely on SaaS applications for their mission-critical workloads."

[3] How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria (gartner.com): "SaaS is becoming so pervasive that it has to be thought of as an integrated IT architecture as well as a business relationship."

[4] Beveiliging- en Verwerkersovereenkomst, Versie 5.1, 18-6-2024

Wijzigingsvoorstellen op het pakket aan artikelen kunnen worden ingediend bij het EA-team of CCoE[5].

2.3. Reikwijdte

De richtlijn zal worden toegepast bij aanbesteding en verwerving van een SaaS-product. De richtlijn concentreert zich op de non-functionele eisen. Zowel Inkoop als de BSO en Lead Architect van de Opdrachtgever zullen deze richtlijn ter hand nemen.

Deze richtlijn kan ook al worden toegepast op of als inspiratiebron dienen voor een marktverkenning of andersoortig onderzoek voorafgaand aan een aanbesteding. Deze onderzoeken helpen om de verzameling aan criteria verder toe te spitsen richting de aanbesteding naar behoefte en type product.

3. Richtlijn

De richtlijn is geformuleerd middels een aantal artikelen.

3.1. Artikel 1 – Toepassing

- Deze richtlijn is van toepassing op alle public cloudgebruik.
- Deze richtlijn wordt toegepast in het aanbestedingstraject van een SaaS-product door betrokkenen van de afdeling Inkoop en de Opdrachtgever (proceseigenaar/divisie/afdeling met de hierbij betrokken verantwoordelijken, (lead) architecten, SLM'ers en BSO'ers).
- De criteria worden gewogen als 'vereist', 'gewenst' of 'optioneel'.
    1. Wanneer afgeweken wordt van *vereiste* criteria, dient er uitleg te worden gegeven met een risicoanalyse en acceptatie met vastlegging hiervan en worden AB en CIO geïnformeerd.
    2. *Gewenste* criteria kunnen vooral een rol spelen in de afweging tussen SaaS-producten en
    3. *Optionele* criteria worden toegepast bij specifieke use cases of zijn meer op termijn van belang.
- Deze richtlijn hanteert een cafetariamodel, waarbij per aanbesteding door de opdrachtgever
    1. een pakket aan eisen wordt geselecteerd uit de brede verzameling en die eventueel worden verdiept (uitwerking van de toelichting op de eis),
    2. de vereiste criteria zijn opgenomen als vereist, tenzij hierop afgeweken wordt met vastlegging van een uitleg, een risicoanalyse en -acceptatie en het informeren van AB en CIO,
    3. de gewenste en optionele criteria kunnen worden gepromoveerd tot vereist of gewenst, en
    4. de toelichting kan nader worden uitgewerkt of aangescherpt.
- De toegepaste criteria in de aanbesteding en nadere invulling (beantwoording) hiervan door de SaaS-leverancier, eventueel in samenwerking of na onderhandeling met UWV, zullen worden opgenomen in de afspraken met de geselecteerde SaaS leverancier (i.e. BVO of SLA).

De criteria waartegen een SaaS-product wordt geëvalueerd zijn onderverdeeld in twee categorieën: technische criteria en business criteria en kennen respectievelijk zeven en drie subcategorieën die verder de opbouw van het document bepalen (vanaf 3.4 Artikel 4 – Identiteit (IAM)).

1. Technische criteria
    i. Identiteit (IAM)
    ii. Integratie
    iii. Ontwikkeling

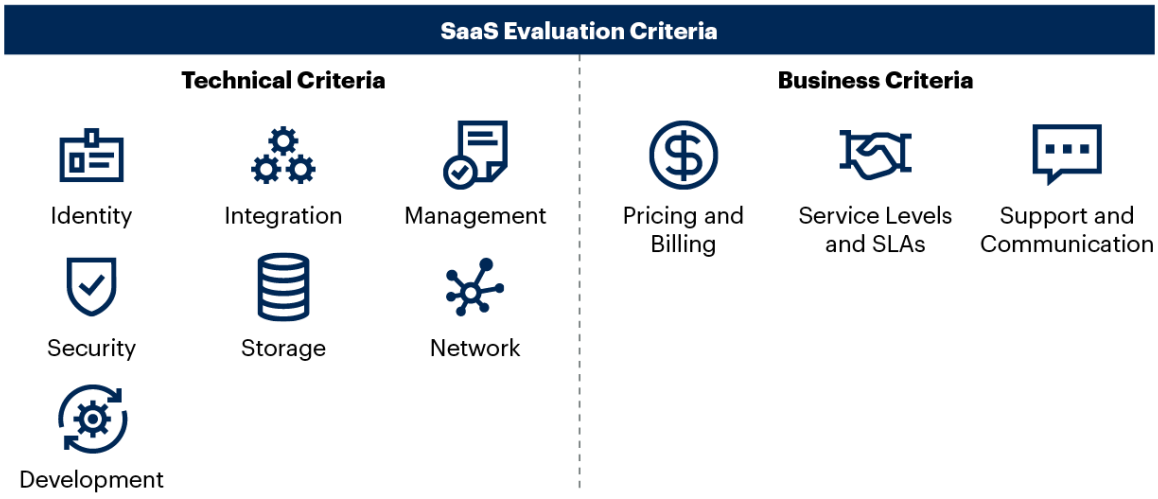
[5] Cloud CoE - Enterprise Architectuur UWV - Confluence

iv. Beheer
v. Beveiliging
vi. Opslag
vii. Netwerk

2. Business criteria
   i. Financiën (FinOps)
   ii. Dienstverlening (SLA)
   iii. Ondersteuning

- De toepassing van de criteria in een aanbestedingsproces kent risico's en valkuilen, waarvan de drie grootste:
  1. Niet beseffen dat IT-evaluatiecriteria slechts één soort criteria zijn.
     Elke evaluatie van een SaaS-oplossing en -leverancier moet evaluatiecriteria bevatten van managers van bedrijfseenheden, juridische zaken, inkoop en managers op C-niveau. Het is belangrijk dat een team wordt samengesteld en samenwerkt om een passende reeks criteria te ontwikkelen. Een gebrek aan inbreng vanuit een van deze gebieden kan een leemte achterlaten die resulteert in een slechte selectie.
  2. Overevaluatie.
     Het heeft geen zin om een eenvoudige SaaS-oplossing aan complexe evaluatiecriteria te laten voldoen. Pas de complexiteit van evaluatiecriteria aan op basis van het aantal gebruikers, de kosten, het type service, leveranciers en problemen die de SaaS-dienst voor UWV oplost. Stem de vereisten af op de omvang van het probleem dat door de oplossing wordt aangepakt. Hanteer eventueel een gewichten- of puntensysteem.
  3. Gebrek aan flexibiliteit.
     Sommige leveranciers kunnen een probleem oplossen op manieren die verschillen van de manieren die worden aangegeven door de criteria in dit document. Houd daar rekening mee bij het uitvoeren van een evaluatie. Begrijp de afwegingen wanneer niet aan de criteria wordt voldaan, en houd rekening met deze afwegingen bij het selecteren van een specifieke oplossing.

SaaS Evaluation Criteria Categories and Subcategories



Source: Gartner
741039_C

Gartner

3.2. Artikel 2 – Definities

Term	**Definitie**
a. CCoE	Cloud Center of Excellence
b. Opdrachtgever	Proceseigenaar/divisie/afdeling of directeur van, die met budget opdracht geeft tot aanbesteding en beslissingen neemt hierin.

3.3. Artikel 3 – Scope

De scope van deze richtlijn betreft alle public cloudgebruik door UWV.

De richtlijn richt zich op de toepassing van non-functionele eisen op SaaS-producten.

3.3.1. Artikel 3a – Taakverdeling

Een evaluatie van een SaaS-product of -oplossing dat een significant aantal gebruikers, kosten en/of veiligheidsrisico's met zich meedraagt vereist betrokkenheid van verschillende disciplines:

- IT (Cloud CoE)
- Informatiebeveiliging en privacy
- Business units (divisies)
- Juridische Zaken
- Inkoop
- Architectuur (leden Architectuur Board)
- Topmanagement (CIO/Directie)

Hoewel de opgestelde eisen vooral technisch van aard zijn, is de inbreng van andere disciplines noodzakelijk om ook businessaspecten af te dekken. Aan de hand van deze richtlijn en de betrokkenheid van de verschillende disciplines zal een ad hoc SaaS verwerving met onnodige risico's en kosten worden voorkomen.

Het volgende RACI model is van toepassing.

Activiteit	*CCoE*	*CIO*	*BU*	*CISO*	*CIOO/LM*	*Inkoop*	*JZ*	*AB*
Opstellen en bijhouden richtlijn	R	A	C	C	C	C	C	C
Toepassing van richtlijn bij aanbesteding SaaS	C	A	R	C	C	C	C	I

3.4. Artikel 4 – Identiteit (IAM)

Identiteits- en toegangsbeheer (IAM – Identity and Access Management) functies zijn essentieel voor SaaS-applicaties. Zonder IAM kan niemand zich authentiseren bij een SaaS-applicatie. Robuust IAM verbetert de ervaringen van eindgebruikers en beheerders door vooral single sign-on (SSO) en gecentraliseerd beheer te bieden. Een zwakke IAM implementatie resulteert in overmatig of ongewenste toegang, wat kan resulteren in datalekken en denial-of-service-aanvallen.

SaaS-applicaties moeten integreren met de identiteitsstructuur van de organisatie – de IAM-infrastructuur – die authenticatie, autorisatie en levenscyclusbeheer van identiteiten mogelijk maakt.

3.4.1. Artikel 4a – Webportaal voor gebruikersbeheer

4a.	**Webportaal voor gebruikersbeheer**	*Vereist*
Criterium	De SaaS-dienst heeft een webinterface waarmee ('privileged') beheerders- en gebruikersaccounts kunnen worden aangemaakt, beheerd en verwijderd.	
Toelichting	Deze interface wordt vooral gebruikt in de inrichtingsfase om gedelegeerde beheerdersaccounts aan te maken, IAM-services te configureren met daarbij het beperken van buitensporige beheerdersrechten en wellicht een eerste groep gebruikers te on-boarden. Een gebruikersinterface (web UI) om gebruikers te beheren is de minst geautomatiseerde service die een SaaS-dienst ten minste moet bieden.	

3.4.2. Artikel 4b – SSO en federatie

4b.	**SSO en federatie**	*Vereist*
Criterium	De SaaS-dienst (met een web UI) ondersteunt single-sign-on (SSO), federatie middels OpenID Connect en draagt bij aan een naadloze SSO-ervaring van de gebruiker.	
Toelichting	De SaaS-oplossing ondersteunt OpenID Connect op bedrijfsniveau (dus met een web UI) om UWV in staat te stellen bestaande identiteiten te hergebruiken en adaptieve en risicobewuste toegangscontrole te bieden via haar bestaande IAM-infrastructuur. Inloggen buiten SSO om voor UWV medewerkers is niet mogelijk. OpenID Connect is het geprefereerde, meest duurzame integratiemechanisme. De SaaS-provider biedt ook een merkbaar naadloze gebruikerservaring tussen systemen met een web UI die een koppeling hebben met UWV's IAM-infrastructuur dat weer gebaseerd is op MIcrosoft Entra ID.	

3.4.3. Artikel 4c – API voor gebruikersbeheer

4c.	**API voor gebruikersbeheer**	*Vereist*
Criterium	De SaaS-dienst biedt een API voor gebruikersbeheer met als doel om gebruikersbeheer volledig te kunnen automatiseren met UWV's provisioning systeem.	
Toelichting	Met een gebruikersbeheer-API kan UWV typische levenscyclusbewerkingen uitvoeren (d.w.z. gebruikersaccounts aanmaken, bijwerken en verwijderen). Bovendien kan deze API de lijm worden tussen ongelijksoortige systemen om naadloos gebruikersbeheer mogelijk te maken zonder voortdurende administratieve tussenkomst. Het SCIM protocol (System for Cross-domain Identity Management) is de aanbevolen standaard voor gebruikersinrichting. SCIM wordt ondersteund door alle toonaangevende leveranciers van toegangsbeheer en identiteitsbeheer en -administratie. Na een initiële configuratie kan UWV een deel van haar gebruikers geregistreerd in de user directory (MS EntraID) synchroniseren met de SaaS-dienst op basis van de geregistreerde organisatiestructuur of kenmerken. API's voor gebruikersbeheer worden vaak ook gebruikt om licenties voor de gebruikers te beheren. De API en achterliggende functies en processen zijn goed gedocumenteerd.	

3.4.4. Artikel 4d – OAuth2.0 en app management

4d.	**OAuth 2.0 en app management**	*Vereist*
Criterium	De SaaS-dienst ondersteunt OAuth2.0 als toegangscontrole op API's die gebruikt kunnen worden door apps.	
Toelichting	OAuth 2.0 is een protocol dat wordt gebruikt voor API-toegangscontrole, waarbij API's vaak worden gebruikt door apps van derden om toegang te krijgen tot informatie in de SaaS-dienst. OAuth 2.0 is uitgegroeid tot het standaardprotocol voor deze specifieke doeleinden en biedt doorgaans toegangscontrole tot de clients en services die worden beheerd onder de "API-ontwikkelaarsportal", zoals hieronder gedefinieerd in de sectie 3.5.4. Met OAuth 2.0 kunnen gebruikers en beheerders namens hen applicaties en services van derden toegang verlenen tot de SaaS-dienst. Het doet dit met behulp van verschillende mechanismen om toegangstokens (meestal JSON Web Tokens [JWT]) te verkrijgen voor applicaties – zoals mobiele applicaties, services, webapplicaties en apparaten – die worden gebruikt om toegang te krijgen tot de SaaS-dienst. Met OAuth 2.0 kan UWV gestandaardiseerde methoden opzetten om de toegang te beperken, toestemming af te handelen en de toegang van individuele apps te vernieuwen en in te trekken.	

3.4.5. Artikel 4e – Autorisatiebeheer

4e.	**Autorisatiebeheer**	*Vereist*
Criterium	De SaaS-dienst biedt zowel een API als een webportaal aan om autorisatiebeheer gebaseerd op RBAC (Role-Based Access Control) uit te kunnen voeren en UWV in staat stelt autorisatiebeheer verregaand te automatiseren.	
Toelichting	De SaaS-dienst heeft een formeel autorisatiebeheerproces voor het aanvragen, verwerken, intrekken of aanpassen, verwijderen en archiveren van autorisaties (Role-Based-Access-Control). Autorisatiebebeheer stelt de voorwaarden ('policies') waaronder een gebruiker of service een bewerking mag uitvoeren op een gegevensverzameling. De autorisatieverstrekking gaat met een formele autorisatie-opdracht van een bevoegde tot verlening daarvan. Dit is proces is goed gedocumenteerd en UWV kan dit inzien. De SaaS-dienst biedt interfaces om de voorwaarden (autorisaties) te beheren. Autorisatiebeheer verbindt rechten (bijvoorbeeld groepen) en privileges (bijvoorbeeld het bijwerken van klantgegevens) op basis van de RBAC-methodiek. Het opstellen en beheren van voorwaarden moet delegeerbaar zijn, zodat medewerkers van UWV dit kunnen onderhouden zonder afhankelijk te hoeven zijn van administratief IT-personeel. De SaaS-dienst stelt UWV in staat beheer te centraliseren en dit lokaal af te dwingen in de SaaS-dienst (ter ondersteuning van een gecentraliseerd/gedecentraliseerd beveiligingsmodel). Dit moet op een efficiënte wijze uitgevoerd kunnen worden gebaseerd op RBAC.	

3.4.6. Artikel 4f – Privacybeleid

4f.	**Privacybeleid**	*Vereist*
Criterium	De SaaS-dienst en leverancier, inclusief onderaannemers, voldoen aan het privacybeleid van UWV.	
Toelichting	Het privacybeleid van UWV is gebaseerd op de AVG. Dit betreft Europese wetgeving. Partijen buiten Europa dienen een beleid te volgen dat hiermee in sync is wat blijkt uit hun eigen privacystatement of DPA en tegemoetkomt aan het verwerkersdeel van de BVO.	

3.4.7. Artikel 4g – Verfijnd autorisatiebeheer

4g.	**Verfijnd autorisatiebeheer**	*Gewenst*
Criterium	De SaaS-dienst levert mogelijkheden voor verfijnd autorisatiebeheer.	
Toelichting	Autorisatie is zelden een grove (wel/niet) beslissing (dat een persoon de dienst wel of niet kan gebruiken). In werkelijkheid kunnen autorisatiebeslissingen gedetailleerder zijn om complexere, contextuele beslissingen mogelijk te maken (b.v. een medewerker heeft alleen toegang tot gegevens van klanten binnen een bepaalde geografische locatie). UWV's autorisatiebeleid en -regels kent verfijning en een SaaS-dienst biedt idealiter gedetailleerde autorisatieondersteuning om tegemoet te komen aan een breed scala aan bedrijfsbeleid en -regels. De SaaS-dienst beschikt dus over verfijnd autorisatiebeheer waarbij de toegekende rol (profiel, taak) overeenkomt met de verstrekte toegangsrechten tot logische middelen (functies en gegevens). De SaaS-dienst voorziet dat bij wijziging van een rol van een gebruiker (zoals andere functie, einde werkverband) op grond waarvan deze niet meer over rechten dient te beschikt, alle toegangsrechten die daarmee samenhangt automatisch worden ingetrokken, ofwel aangepast naar de gewijzigde rol.	

3.4.8. Artikel 4h – CLI voor gebruikers- en autorisatiebeheer

4h.	**CLI voor gebruikers- en autorisatiebeheer**	*Gewenst*
Criterium	De SaaS-dienst biedt een CLI aan voor het uitvoeren van gebruikers- en autorisatiebeheer.	
Toelichting	Beheerders gebruiken steeds vaker CLI's (Command Line Interface) om hun bronnen te beheren. Dit geldt ook voor beheer van gebruikers en applicaties en hun rechten. Het aanbieden van een CLI, direct naast het administratieve dashboard en de gebruikersbeheer-API, maakt beheer makkelijker.	

3.4.9. Artikel 4i – Signalen t.b.v. risicobeheer

4i.	**Delen van risicosignalen**	*Optioneel*
Criterium	De SaaS-dienst biedt (al dan niet als onderdeel van monitoring) mogelijkheden om afwijkende gebeurtenissen (ingegeven door proces, werking of andere oorzaken) te kunnen waarnemen en zet dit om in een signaal zodat UWV daarop kan reageren.	
Toelichting	UWV (m.n. CDC) en de SaaS-leverancier kunnen sessie- en risicosignalen delen binnen hun twee verschillende domeinen. Dit is mogelijk met behulp van op standaarden gebaseerde protocollen zoals het Continuous Access Evaluation Profile (CAEP). Het stelt UWV tevens in staat de toegang te blokkeren en dieper inzicht te geven in adaptieve en continue toegangsbeslissingen. Het signaal maakt (voor zover bekend) duidelijk: a) de gebeurtenis; (b) de benodigde informatie die nodig is om het voorval met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis. Het signaal bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden, zoals wachtwoorden en inbelnummers. Het signaleren en registreren van afwijkende gebeurtenissen voldoet aan de eisen van UWV op het gebied van monitoring en beheer inzake technisch beheer en informatiebeveiliging.	

3.4.10. Artikel 4j – Batch import van gebruikers

4j.	**Batch import interface**	*Optioneel*
Criterium	De SaaS-dienst biedt een batch import interface aan voor het uitvoeren van gebruikers- en autorisatiebeheer.	
Toelichting	Een batchinterface is een oude aanpak en het minst geprefereerde mechanisme voor het beheren van gebruikers, maar het is op zijn minst een iets meer geautomatiseerde mogelijkheid voor gebruikersbeheer dan alleen een administratieve gebruikersinterface en kan van nut zijn als (initiële) synchronisatie faalt. In dit geval maakt UWV een tekstbestand, vaak een bestand met door komma's gescheiden waarden (CSV), opgemaakt volgens de vereisten van de specifieke SaaS-provider. Dit bestand bevat gebruikers die moeten worden aangemaakt, gewijzigd of verwijderd. Een beheerder uploadt vervolgens het bestand. De SaaS-oplossing verwerkt uiteindelijk het bestand en voert indien nodig acties uit (d.w.z. gebruikersaccounts maken, bijwerken en verwijderen). Hiermee kunnen gebruikersaccounts in bulk worden beheerd.	

3.5. Artikel 5 – Integratie

Het introduceren van nieuwe SaaS-diensten, of het migreren van een on-premise applicatie of software naar een SaaS-oplossing, brengt vaak het herdefiniëren of opnieuw opbouwen van bestaande bedrijfsprocessen met zich mee. Bovendien dwingt de overstap naar SaaS vaak onverwachte integratie met andere SaaS- en on-premise-oplossingen af.

Het is niet langer acceptabel dat kritieke (strategisch belangrijke, bedrijfskritische) SaaS-diensten geen programmatische toegang bieden tot hun functionaliteit en gegevens zoals via API's en gebeurtenissen (‘events’). Een moderne SaaS-dienst is geen geïsoleerde tool, maar een platform waarop UWV voortbouwt, met een aanbod aan gedetailleerde API's en gebeurtenissen waarmee de dienst kan worden geïntegreerd in UWV’s applicaties, processen en workflows.

Toonaangevende SaaS-aanbieders erkennen dat integratie de sleutel is tot het succes van hun klanten. Ze pakken dit aan door de meest voorkomende integratiescenario's zo eenvoudig mogelijk te maken, maar zal in de praktijk nog steeds onvoldoende zijn om een volledig geïntegreerd UX- en bedrijfsproces te bieden.

De technologieën en methoden om SaaS-oplossingen te verbinden met andere SaaS- en on-premises oplossingen zijn nog steeds in ontwikkeling. Een geïntegreerde oplossing is vaak nodig om een optimaal bedrijfsproces te leveren. Een dergelijke oplossing is echter niet eenvoudig te implementeren. Daarom moet UWV de integratiemogelijkheden en interfaces van SaaS-oplossingen zorgvuldig beoordelen. De criteria in deze sectie zijn van hoog niveau. De criteria moeten mogelijk worden aangepast, afhankelijk van het te evalueren SaaS-aanbod en de bedrijfsapplicaties en data-omgevingen (zowel on-premise als cloud) waarmee het moet worden geïntegreerd (in een hybrid cloud omgeving).

3.5.1. Artikel 5a – API's voor gegevenstoegang

5a.	**API's voor gegevenstoegang**	*Vereist*
Criterium	De SaaS-dienst biedt API's voor gegevenstoegang aan met minimaal alle (non)functionele kenmerken die de gebruikersinterfaces biedt.	
Toelichting	Alle SaaS-diensten verwerken en slaan gegevens op. Een SaaS-dienst biedt de mogelijkheid om deze gegevens te ontsluiten, te creëren en te wijzigen. Er is minimaal een REST API aanwezig in JSON- (voorkeur) of XML-gegevensformaat. Sommige providers bieden mogelijk ook Open Data Protocol (OData) of SOAP API's aan. Bij gebruik van deze API's verloopt de communicatie synchroon, omdat ze geoptimaliseerd zijn voor real-time integraties. Ook is het mogelijk om met een business intelligence (BI) tool verbinding te maken met deze API's. Hoewel sommige SaaS-oplossingen analysefuncties hebben, zijn de rapporten en functionaliteit die ze bevatten vaak beperkt, en zijn hun analysemogelijkheden mogelijk beperkt tot de reikwijdte van de enkele SaaS-oplossing. BI-tools (zoals Microsoft Power BI, Tableau Cloud en QlikView) kunnen gegevens uit meerdere bronnen samenvoegen, realtime inzichten bieden en een veel rijkere set rapportformaten bieden. UWV kan data functioneel begrijpelijk uit de softwareoplossing halen, zowel voor bevragingen (API's) als voor bulk bijvoorbeeld t.b.v. analytics, maar ook t.b.v. referentietabellen die in het product worden aangemaakt en masterdata uit het product. Event-driven API's worden ondersteund die veranderingen in gegevens instant (of anders frequent bulk) aanbiedt ter verwerking in het verdere UWV IT landschap (t.b.v. data life cycle management, data integriteit). Gebruikslimieten aan API's (bijvoorbeeld aantal calls per licentie, kosten, per seconde) zijn helder gedocumenteerd. Een verzameling API's zal geen add-on-interface zijn van de SaaS-dienst die gedeeltelijke toegang tot het systeem biedt, maar eerder een fundamenteel onderdeel zijn van de SaaS-architectuur dat programmatische toegang biedt tot alle functionele kenmerken van de SaaS gelijk aan de web- en mobiele gebruikersinterfaces, waarbij faciliteiten als Vaults voor secrets management (o.a. authenticatie certificaten) standaard onderdeel zijn van de dienst.	

3.5.2. Artikel 5b – API's voor operationeel beheer

5b.	**API's voor operationeel beheer**	*Vereist*
Criterium	De SaaS-dienst biedt API's voor operationeel beheer aan met minimaal alle functionele kenmerken die de gebruikersinterfaces voor de beheerder (beheerdersportaal) biedt.	
Toelichting	Een operationele API, ook wel servicemanagement API genoemd, biedt toegang tot de dagelijkse administratieve functies van het platform, zoals het beheren van gebruikersaccounts en machtigingen, toegang tot platformgebruiksgegevens, het toepassen van licentiemanagement en het programmatisch beheren van de platformconfiguratie. Met deze API's kunnen algemene operationele processen worden geautomatiseerd en kritische configuratieactiviteiten 'as code' worden geïmplementeerd die zowel herhaalbaar als traceerbaar is. Deze wijze zal het risico op menselijke fouten tijdens de configuratie van de SaaS-applicatie verminderen. Een voorbeeld is het beschikbaar hebben van API's die gekoppeld kunnen worden aan FlexeraOne (in gebruik bij UWV) ten behoeve van licentiemanagement.	

3.5.3. Artikel 5c – API voor bulk import/export

5c.	**API voor bulk import/export**	*Vereist*
Criterium	De SaaS-dienst biedt API's voor bulk import/export aan.	
Toelichting	Naarmate het gebruik van een SaaS-platform groeit en de hoeveelheid gegevens die door het platform wordt beheerd toeneemt, is een manier nodig om gegevens efficiënt uit het platform te exporteren, bijvoorbeeld voor data-analyseplatforms of het regelmatig bewaren van een kopie van de gegevens voor back-up en noodherstel (Desaster/Recovery). Bulkimport is ook essentieel voor het efficiënt migreren van grote hoeveelheden data van bestaande systemen naar een SaaS-oplossing, bijvoorbeeld bij een cloudmigratie of exit. De bulkdata-API kan een combinatie zijn van webservice-interfaces, bestandsuitwisseling en/of opslagintegraties (bijvoorbeeld SSH file transfer protocol [SFTP], cloudopslag of enterprise file synchronization, en sharing [EFSS]-oplossingen).	

3.5.4. Artikel 5d – API ontwikkelportaal

5d.	**API ontwikkelportaal**	*Vereist*
Criterium	De SaaS-dienst biedt API ontwikkelportaal aan voor het ontwikkelen en testen van integraties.	
Toelichting	De SaaS-leverancier biedt een ontwikkelaarsportal aan met documentatie over alle API's, een rijke set aan softwareontwikkelingskits (SDK's) voor de toonaangevende programmeertalen (Java, .NET, Ruby, Perl en Python), code-wrapper-bibliotheken en voorbeeldcode. Het ontwikkelaarsportaal moet ook informatie publiceren over API-versie- en -levenscyclusbeheer, inclusief release-, afschaffings- ('deprecation') en buitengebruikstellingsschema's en moet proactieve meldingen hierover verstrekken aan stakeholders binnen UWV. De SaaS-dienst biedt een sandbox-omgeving aan om integraties te kunnen ontwikkelen en testen. Tot slot biedt de leverancier goed ondersteuning aan ontwikkelaars middels helpdesk en eventueel community.	

3.5.5. Artikel 5e – Datamodel gespecificeerd

5e.	**Datamodel gespecificeerd**	*Vereist*
Criterium	De SaaS-dienst biedt inzicht in het gebruikte datamodel (applicatie én API definities) en kan een (gepubliceerde) specificatie overleggen.	
Toelichting	Om juiste uitkomsten van UWV bedrijfsprocessen te kunnen garanderen is een specificatie nodig van de structuur en definitie van data elementen die verwerkt en via API beschikbaar gesteld worden door de SaaS dienst. De specificatie laat het (ingebakken) datamodel zien dat de interne processen en functies van de SaaS-dienst ondersteunt en bevat ten minste de volgende onderdelen per data element: naam, definitie, bij welke entiteit het element behoort, of het een sleutelgegeven betreft, data type, of het gegeven verplicht is, historisch gedrag (geeft aan hoe de historische waarde opgeslagen wordt: overschrijven, versioning, tijdlijnen) en relaties met andere data elementen inclusief kardinaliteit en optionaliteit. Zonder deze specificatie heeft UWV onvoldoende garanties dat data voldoet aan basale spelregels voor gebruik in bedrijfsprocessen (operationeel en analytisch). Dit datamodel betreft niet een beschrijving van de fysieke wijze waarop de SaaS dienst de data opslaat of verwerkt. Het betreft een inrichtingsafhankelijk logisch/functioneel model dat weergeeft welke constraints en andere regels van toepassing zijn wanneer UWV de dienst gebruikt om data in processen te verwerken. De wijze waarop de SaaS dienst de specificatie realiseert hoeft niet bekend te zijn bij UWV (black box).	

3.5.6. Artikel 5f – Horizontale data lineage

5f.	**Horizontale data lineage**	*Vereist*
Criterium	De SaaS-dienst biedt de mogelijkheid om via een API gegevens te delen ten behoeve van horizontale data lineage.	
Toelichting	De datastroom over verschillende systemen, platforms en applicaties wordt in kaart gebracht met behulp van horizontale data lineage, wat laat zien hoe data beweegt, integreert en transformeert tussen de bron en het doel. Het in kaart brengen van horizontale lineage omvat ook de tools en processen die betrokken zijn bij deze datastromen. Horizontale Data Lineage die in de SaaS-oplossing wordt aangemaakt kan minimaal gedeeld worden in onze kop-staart lineage tooling. Of het product staat open, hanteert standaard protocollen op dit gebied en is beschikbaar voor tools als Informatica, Collibra, die zelf actief lineage opbouwen.	

3.5.7. Artikel 5g – Verticale data lineage

5g.	**Verticale data lineage**	*Gewenst*
Criterium	De SaaS-dienst kan qua data definities, naamgeving, samenhang, etc. aansluiten op het canoniek gegevensmodel.	
Toelichting	Mapping van de verticaliteit van data verwijst naar de stroom binnen een specifiek systeem, platform of applicatie. Verticale data lineage (gegevensafstamming) is een gegevensafstamming die de relaties beschrijft tussen het conceptuele gegevensmodel, het logische gegevensmodel, het technische gegevensmodel en de onderliggende gegevens. Het geeft de relatie weer tussen de data en de bijbehorende modellen en definities op verschillende niveaus (conceptueel, logisch, fysiek). Bij een SaaS-oplossing komt het op neer hoe concepten (logisch) geïmplementeerd zijn in een API, de rest is black box. De SaaS-oplossing kan qua data definities, naamgeving, samenhang, etc. aansluiten op het UWV canoniek gegevensmodel, gecommuniceerd door het UWV, wat duidelijk blijkt uit de API definities. Zo niet, dan is het vooral aan UWV (Opdrachtgever / proceseigenaar) om de vergelijking te maken, significante afwijkingen en gaps te identificeren en te analyseren, want deze bevindingen zullen waarschijnlijk leiden tot een grotere integratieinspanning of maatwerk ('plumbing') dat moet worden ingecalculeerd of wellicht onhaalbaar blijkt.	

3.5.8. Artikel 5h – Hybride cloud

5h.	**Hybride cloud**	*Gewenst*
Criterium	De SaaS-dienst ondersteunt implementatie en integratie in een hybride cloud omgeving.	
Toelichting	UWV streeft een hybride cloud omgeving na. Doorgaans dient de SaaS-oplossing te integreren met andere cloudsystemen en met applicaties die lokaal worden geïmplementeerd of geïnstalleerd. Een context diagram zou dit moeten verduidelijken. Het is van cruciaal belang om alle potentiële contactpunten met een SaaS-oplossing te evalueren om te bepalen of integraties met on-premises of cloud infrastructuur of oplossingen nodig zijn. Zelden kan de dienst worden geleverd in een silo zonder enige contactpunten met het huidige UWV IT landschap.	

3.5.9. Artikel 5i – Partnerschap met integratieleveranciers

5i.	**Partnerschap met integratieleveranciers**	*Gewenst*
Criterium	De SaaS-dienst heeft partnerschappen met integratieleveranciers en ondersteunt implementatie en integratie in een veilige hybrid cloud omgeving.	
Toelichting	UWV heeft integratieproducten en -diensten en is voornemens deze ontoereikende set uit te breiden. Het heeft de voorkeur dat de SaaS leverancier partnerschappen heeft met de leverancier van deze integratieproducten en -diensten. Deze partnerschappen zorgen ervoor dat kant-en-klare connectoren of adapters en tools voor gegevenssynchronisatie beschikbaar zijn, via een palet dat wordt geleverd in het integratieproduct of -dienst. De opname van dit criterium hangt af van de SaaS-oplossing die wordt geëvalueerd. Zie ook Artikel 5l – Native applicatieconnectoren.	

3.5.10. Artikel 5j – Initiëren van notificaties

5j.	**Initiëren van notificaties**	*Gewenst*
Criterium	De SaaS-dienst ondersteunt met interfaces het initiëren van gebeurtenissen (events) en notificaties.	
Toelichting	SaaS-applicaties kunnen een centraal onderdeel zijn (of worden) van een bedrijfsproces en het registratiesysteem voor kritieke zakelijke gebeurtenissen, zoals het aanmaken van een nieuwe klant of medewerker. In deze scenario's moet de SaaS-dienst verwerking in/naar andere systemen en services kunnen initiëren. Dit kan bijvoorbeeld door ondersteuning van WebHooks voor kritieke gebeurtenissen en meldingen, zodat de SaaS-dienst een API van een systeem (kan ook weer een SaaS-dienst zijn, of een eigen applicatie) vrijwel in real-time kan aanroepen wanneer de gebeurtenis plaatsvindt. Of door het publiceren van gebeurtenisstreams waarop kan worden geabonneerd met behulp van integratieplatforms, streamverwerkingsplatforms of andere applicaties.	

3.5.11. Artikel 5k – Berichtenprotocollen

5k.	**Berichtenprotocollen**	*Gewenst*
Criterium	De SaaS-dienst ondersteunt marktconforme protocollen voor asynchrone berichtencommunicatie.	
Toelichting	Voor geavanceerde digitale bedrijfsoplossingen kan een traditionele API in request-response-stijl (zoals REST of SOAP via HTTP Secure [HTTPS]) beperkend zijn, omdat deze een synchroon interactiemodel biedt. Een API die op berichten gebaseerde protocollen ondersteunt, zoals AMQP of MQTT, biedt een asynchroon interactiemodel dat koppeling vermindert. Dit kan bidirectionele communicatie van opdrachten en gebeurtenissen tussen de SaaS-oplossing en andere cloudoplossingen of -systemen in uw omgeving ondersteunen.	

3.5.12. Artikel 5l – Native applicatieconnectoren voor platformintegratie

5l.	**Native applicatieconnectoren voor integratie**	*Gewenst*
Criterium	De SaaS-dienst heeft native applicatieconnectoren die integratieplatformleveranciers ondersteunt.	
Toelichting	Hoewel het bieden van een rijke set API's essentieel is voor het ondersteunen van uiteenlopende integratievereisten, kan het leren van een complexe API tijdrovend zijn en kan het ingewikkeld zijn om ermee te integreren. Als er native connectoren (in plaats van protocolconnectoren op laag niveau, zoals REST) beschikbaar zijn in het integratieplatform van UWV, wordt de integratie eenvoudiger en toegankelijker. Het heeft dus de voorkeur dat aanbieders van SaaS-oplossingen samenwerken met aanbieders van integratieplatform-as-a-service (iPaaS) en on-premises integratieplatforms om native SaaS-connectoren te leveren. Deze stroomlijnen de integratie met hun oplossingen en verbeteren de productiviteit en kwaliteit. Er bestaat geen alomtegenwoordige standaard voor deze connectoren, dus SaaS-leveranciers moeten kiezen met welke integratieplatformaanbieders ze willen werken. UWV dient bij het evalueren van een SaaS-oplossing de beschikbaarheid van connectoren te valideren in relatie tot haar integratieplatform en ervoor zorgen dat leveranciers zich blijven inzetten voor voortdurende ondersteuning.	

3.5.13. Artikel 5m – Native applicatieconnectoren voor desktopapplicaties

5m.	**Native applicatieconnectoren voor desktopapplicaties**	*Optioneel*
Criterium	De SaaS-dienst heeft native applicatieconnectoren voor populaire desktopapplicaties.	
Toelichting	Gebruikers, vooral mobiele werknemers, vinden het inefficiënt en niet altijd mogelijk om te navigeren en in te loggen op het webportaal van een SaaS-oplossing wanneer ze toegang moeten krijgen tot de gegevens ervan. Connectors voor veelgebruikte desktopapplicaties stellen werknemers in staat de SaaS-applicatie in hun workflows te integreren. SaaS-providers moeten connectoren aanbieden voor populaire desktop- en mobiele applicaties, zoals e-mail, contacten en agenda. Bij UWV is dat vooral MS365.	

3.5.14. Artikel 5n – Ingebed integratieplatform

5n.	**Ingebed integratieplatform**	*Optioneel*
Criterium	De SaaS-dienst ondersteunt een ingebed integratieplatform.	
Toelichting	Bedrijfsprocessen omvatten vaak meerdere services of systemen. Daarom kan een SaaS-oplossing integratiemogelijkheden bieden via een ingebed integratieplatform. Het gebruik van een ingebed integratieplatform biedt een snelle manier om ad-hoc- of point-to-point-integraties te creëren met andere SaaS- en on-premises oplossingen, maar je bent wel afhankelijk van de mogelijkheden van de ingebouwde integratiefuncties. Als een aanzienlijk aantal integraties wordt voorzien, geeft een speciale iPaaS (zie 3.5.12) meer controle over welke integraties en hoe deze worden gerealiseerd. Een SaaS-leverancier moet een basisset connectoren aanbieden in een ingebed (meegeleverd) integratieplatform, maar ook uitbreidingsframeworks zoals Swagger ondersteunen.	

3.5.15. Artikel 5o – Procesorkestratie en -workflow

5o.	**Procesorkestratie en -workflow**	*Optioneel*
Criterium	De SaaS-dienst ondersteunt procesorkestratie en workflow.	
Toelichting	Het doel van het integreren van SaaS-diensten met andere oplossingen is het automatiseren van bedrijfsprocessen. Grotere SaaS-oplossingen (zoals MS Dynamics 365) bieden functies voor procesorkestratie en taakbeheer waarmee het SaaS-platform een bedrijfsproces kan orkestreren. Deze functies bouwen voort op basisintegratiefuncties en omvatten ook het vasthouden en beheren van de status van een procesinstantie, zoals een zaak of taak, terwijl deze zich een weg baant door een keten van processtappen. Het aanbieden van procesorkestratie en -workflow functies, bij voorkeur in een low-code inrichtingsomgeving, helpt in het oplossen van (proces)integratievraagstukken en maakt deze eenvoudiger.	

3.5.16. Artikel 5p – Marktplaats voor uitbreidingen

5p.	**Marktplaats voor uitbreidingen**	*Optioneel*
Criterium	De SaaS-leverancier biedt een marktplaats voor uitbreidingen op de SaaS-oplossing.	
Toelichting	De SaaS-leverancier biedt een marktplaats waar extensies van de leverancier, van derden of van de afnemer (UWV) zelf beschikbaar kunnen worden gesteld voor (her)gebruik. Zo'n marktplaats biedt bijvoorbeeld vooraf-geconfigureerde integraties met applicaties die veel worden gebruikt in combinatie met de SaaS-oplossing. Dit kunnen connectoren zijn met toonaangevende SaaS-oplossingen voor algemeen gebruik (bijvoorbeeld opslag, e-mail of workflow) of connectoren met door partners geleverde oplossingen die vaak in combinatie met de SaaS-oplossing worden gebruikt. Deze vooraf-geconfigureerde integraties worden actief ondersteund door de SaaS-leverancier. Ze kunnen de tijd en moeite die nodig is om te integreren aanzienlijk verminderen. Wel zal door UWV beleid en richtlijnen geformuleerd moeten worden op gebied van architectuur en veiligheid om em hoe extensies te gebruiken. Kanttekening: Om rechtmatig gebruik te kunnen maken van een marktplaats dienen de beoogde functionaliteiten in scope van de aanbesteding dan wel in herzieningsclausule van aanbesteding te zijn opgenomen. Deze eis kan daarom niet op zichzelf staan.	

3.6. Artikel 6 – Ontwikkeling

Er zijn veel SaaS-applicaties die UWV kunnen helpen bij het implementeren van een of andere vorm van bedrijfsproces. Zij bieden een out-of-the-box oplossing, maar het kan zijn dat deze niet volledig aan de *functionele* wensen voldoet. Beperkte aanpassingen zijn misschien mogelijk via configuratie, maar zodra een aanzienlijk mate van maatwerk nodig is binnen de mogelijkheden van de SaaS-applicatie, is het eigenlijk softwareontwikkeling geworden. Veel SaaS-applicaties zijn verder gegaan dan alleen het leveren van beperkte configuratiemogelijkheden en zijn uitgegroeid tot een platform voor ontwikkeling. Door eigen extensies, modules, interfaces en integraties op een SaaS-platform te ontwikkelen, kan dit voor UWV nieuwe en op maat gemaakte gebruikerservaringen opleveren.

3.6.1. Artikel 6a – Maatwerk door programmeerbaarheid

6a.	**Maatwerk door programmeerbaarheid**	*Vereist*
Criterium	De SaaS-dienst biedt de mogelijkheid tot realiseren van maatwerk of uitbreiden van functionaliteit via programmeerbaarheid.	
Toelichting	Het uitbreiden van een SaaS-oplossing vergroot programmatisch de reikwijdte van de oplossing en stelt UWV in staat om niet alleen hiaten in de functionaliteit op te vullen, maar ook aanpassingen te creëren zoals nieuwe rapporten, nieuwe processen of zelfs integraties met andere (externe) diensten. Uitbreidbaarheid middels geparametriseerde configuraties, scripttalen (zoals JavaScript) of low-code biedt mogelijkheden voor maatwerk en in het geval van low/no-code kan deze gerealiseerd worden door burgerontwikkelaars. Doe dit wel met mate, het principe van standaardisatie en deze te omarmen staat voorop: pas de eigen processen hierop aan. LCM en CI/CD principes worden ondersteund.	

3.6.2. Artikel 6b – Programmeerbare interfaces

6b.	**Programmeerbare interfaces**	*Gewenst*
Criterium	De SaaS-dienst biedt programmeerbare interfaces (met SDK's, CLI's en wrappers).	
Toelichting	SaaS-leveranciers die programmeerbare interfaces (SDK's, inclusief CLI's en wrappers) voor hun dienst bieden, bieden bedrijven meer mogelijkheden om de waarde van de dienst te maximaliseren. Programmeerbare interfaces ontsluiten het potentieel voor klanten (UWV) en softwareleveranciers met toegevoegde waarde om extra functionaliteit te introduceren in het kernaanbod van de SaaS-dienst en te integreren met andere infrastructuur en applicaties. Leveranciers moeten SDK's leveren, inclusief CLI's en wrappers voor hun API's, in de meest voorkomende programmeertalen. Het aanbod moet mobiele platforms omvatten, zoals iOS en Android, om de integratie van een mobiele apps de SaaS API's te vergemakkelijken.	

3.6.3. Artikel 6c – Uitbreidbaarheid en integreerbaarheid van de UI

6c.	**Uitbreidbaarheid en integreerbaarheid van de UI**	*Gewenst*
Criterium	De SaaS-dienst biedt mogelijkheden om de user interface uit te breiden met of te integreren met/in user interfaces van andere applicaties.	
Toelichting	Een SaaS-oplossing biedt een manier om integraties op UI-niveau uit te voeren, hetzij door (1) zichzelf uit te kunnen breiden middels incorporeren of publiceren van delen van de gebruikersinterface van een andere oplossing, of (2) een raamwerk of functie te bieden waarmee een andere oplossing delen van de SaaS-UI in zijn gebruikersinterface kan opnemen. Met deze uitbreidingsmogelijkheden kan u een gebruikersinterface worden gecreëerd dat beter aansluit op de behoefte van de gebruiker (bijvoorbeeld één geïntegreerd webportaal).	

3.6.4. Artikel 6d – Uitbreidbare UX

6d.	**Uitbreidbare UX**	*Gewenst*
Criterium	De SaaS-dienst biedt mogelijkheden tot het uitbreiden van de 'user experience' (UX), waarin de SaaS-dienst slechts een onderdeel van is.	
Toelichting	Het uitbreiden van de UX impliceert het veranderen van de stappen en interacties die een gebruiker doorloopt. Dit kan het gebruik van modules inhouden om nieuwe interacties toe te voegen, zoals het toevoegen van handtekeningregistratie aan een mobiele applicatie.	

3.6.5. Artikel 6e – Low-code ontwikkelomgeving

6e.	**Low-code ontwikkelomgeving**	*Gewenst*
Criterium	De SaaS-dienst biedt een low-code omgeving om laagdrempelig nieuwe functies te kunnen ontwikkelen voor deze dienst.	
Toelichting	De ontwikkelaars die nieuwe functies voor een SaaS-applicatie willen ontwikkelen, reiken hedendaags verder dan alleen de 'traditionele' professionele ontwikkelaars en omvatten ook ad-hoc- en burgerontwikkelaars ('citizen developers'). Deze ontwikkelaars hebben een ontwikkelomgeving met weinig of geen code nodig om productief te zijn, en dezelfde productiviteitsverbeteringen stellen professionele ontwikkelaars in staat sneller functies te leveren dan wanneer ze traditionele programmeertalen zouden gebruiken. Een SaaS-oplossing biedt een grafische ontwikkelervaring, waarbij programmeercomponenten en constructies worden aangestuurd door een model of naar een canvas worden gesleept, neergezet en geconfigureerd.	

3.6.6. Artikel 6f – Professioneel ontwikkelaarsprogramma

6f.	**Professioneel ontwikkelaarsprogramma**	*Optioneel*
Criterium	De SaaS-leverancier biedt een professioneel ontwikkelaarsprogramma aan om vaardigheden van medewerkers op niveau te krijgen en te houden als ook het ecosysteem en community rond de SaaS-dienst.	
Toelichting	Een onrealistische verwachting van de afnemers (UWV) is vaak dat de SaaS-oplossing weinig of geen extra ontwikkeling zal vergen dan wellicht het selecteren van wat opties zonder extra werk. Maar naarmate SaaS-oplossingen volwassener worden (of al zijn) en er via API's meer integratiemogelijkheden beschikbaar komen, is het nuttig als de aanbieder van SaaS-oplossingen een programma aanbiedt dat ontwikkelaars certificeert. Een professioneel ontwikkelaarsprogramma valideert een uitgebreide reeks vaardigheden die nodig zijn om succesvolle applicaties voor het SaaS-platform te ontwikkelen. Het ondersteunen en versterken van een dergelijk ontwikkelingsprogramma zal een ecosysteem van vertrouwde derde partijen en individuen creëren, wat de adoptie van de clouddienst zal vergroten.	

3.7. Artikel 7 – Beheer

Eén van de aantrekkelijke eigenschappen van een SaaS-oplossing is de ontzorging op het gebied van IT-beheer. Deze ontzorging door verschuiving van verantwoordelijkheden naar de SaaS-leverancier is verregaand, maar IT (UWV of uitbesteed) moet nog steeds betrokken zijn bij het beheer van gebruikers, bijbehorende data en eventuele integraties met andere SaaS- of on-premise oplossingen.

Het beheer in een SaaS-omgeving beperkt zich doorgaans tot het beheren van rechten en soms de bijbehorende gegevens. Over het algemeen gebeurt dit via een webbeheerdashboard of -console of via een API, die integratie op de beheerlaag mogelijk maakt.

Voor UWV is het beheer van rechten en middelen van cruciaal belang voor de implementatie en het succes van een SaaS-oplossing. In tegenstelling tot applicaties op locatie staan SaaS-applicaties open voor internet. Het beheren van toegangsrechten is dan één van de belangrijkste verdedigingslinies voor alle SaaS-afnemers en dus ook voor UWV. Over het algemeen geldt dat hoe gedetailleerder de beheermogelijkheden voor toegangscontrole binnen de SaaS-oplossing zijn, hoe beter dit is voor UWV. UWV heeft echter doorgaans geen inzicht in of mogelijkheden voor het beheer van de onderliggende infrastructuur of applicatie. Hoewel dit deel uitmaakt van de

aantrekkingskracht van SaaS, kan het ook deel gaan uitmaken van de frustratie, omdat UWV heel weinig controle heeft.

3.7.1. Artikel 7a – Webportaal voor beheer van gebruikers

7a.	**Webportaal voor beheer van gebruikers**	*Vereist*
Criterium	De SaaS-dienst biedt een webgebaseerde beheerconsole waarmee ondernemingen gebruikers en bijbehorende gegevens kunnen beheren.	
Toelichting	De webgebaseerde beheerconsole biedt een verscheidenheid aan functies aan, zoals het inrichten en uitschrijven van gebruikers, het wijzigen van gebruikersrechten, het beperken of inschakelen van services of functies, en het leveren van operationele gegevens hieromtrent. Deze vereiste omvat Artikel 4a – Webportaal voor gebruikersbeheer. Het is een algemene vereiste dat de webconsole wordt ondersteund voor gebruik in drie van de belangrijkste webbrowsers.	

3.7.2. Artikel 7b – Real-time monitoring

7b.	**Real-time monitoring**	*Vereist*
Criterium	De SaaS-leverancier of -dienst biedt de mogelijkheid om de algemene gezondheid van de dienst te monitoren op storingen en limieten en waarschuwingen hierover te versturen.	
Toelichting	De SaaS-leverancier biedt de mogelijkheid om de algemene gezondheid van hun dienst te monitoren op storingen en limieten, en de SaaS-oplossing kan een waarschuwing sturen als er een storing optreedt of een limiet wordt overschreden. Bij SaaS-oplossingen wordt dit vaak gedaan via een managementdashboard of statuspagina die informatie biedt over de gezondheid of status van de SaaS-oplossing die aan UWV wordt geleverd. De SaaS-leverancier biedt UWV op zijn minst de mogelijkheid om waarschuwingen te ontvangen binnen 30 seconden nadat een prestatiebewakingsdrempel wordt bereikt of overschreden, of wanneer zich een kritieke gebeurtenis voordoet die van invloed is op de aangeboden SaaS-oplossing (bijvoorbeeld uitval, verlies van functionaliteit of prestatieproblemen). De leverancier kan niet van UWV verwachten dat ze al hun tijd besteden aan het kijken naar een realtime monitoringsysteem, en als zodanig zijn meldingen belangrijk voor het dagelijkse beheer van de SaaS-oplossing en voor ketenmonitoring. De SaaS-leverancier ondersteunt waarschuwingen via e-mail of webservices en die integreerbaar zijn in/met de monitoringsystemen van UWV (of centraal monitoringsysteem).	

3.7.3. Artikel 7c – Tools voor het meten van gebruik en operatie

7c.	**Tools voor het meten van gebruik en operatie**	*Vereist*
Criterium	De SaaS-dienst biedt tools aan voor het meten en monitoring van gebruik en operatie.	
Toelichting	Tools die operationeel gebruik en gebruik van gegevens volgen helpen UWV de waarde van de dienst te begrijpen, SLA-statistieken te monitoren en audits uit te voeren om wettelijke redenen. De SaaS-leverancier biedt tools voor de belangrijkste statistieken van de SaaS-oplossing, evenals voor algemeenheden zoals toegangs- en gebruiksstatistieken. Deze gebruiks- en datatrackingtools van de SaaS-oplossing moeten worden geëvalueerd in de context van welke informatie UWV nodig heeft om de service op ten minste deze gebieden te meten: waarde van de service, SLA-statistieken en wettelijke of compliance-eisen.	

3.7.4. Artikel 7d – Schaalbaarheid

7d.	**Schaalbaarheid**	*Vereist*
Criterium	De SaaS-dienst heeft het vermogen om snel op te schalen; UWV kan gebruikers en gegevens aan een dienst toevoegen of het gebruik van de dienst laten toenemen, zonder dat er tijd nodig is om infrastructuur toe te voegen.	
Toelichting	De mogelijkheid om een dienst op- of af te schalen is een van de belangrijkste aantrekkingskrachten van SaaS-oplossingen. SaaS-leveranciers moeten hun dienstverlening snel kunnen op- of afschalen in termen van gebruikers, opslag en netwerk. Bij meer gebruik is opschalen van infrastructuur en elasticiteit van de software vereist. De moeilijkheid bij deze eis is vooral 'snel'. Verschillende SaaS-oplossingen zullen verschillende definities hierin hanteren, van instant om atypische en functionele pieken in het gebruik te ondersteunen tot dagen, omdat extra hardware moet worden ingezet. Het is echter niet acceptabel dat een SaaS-leverancier de behoefte van UWV niet kan nakomen door tijd te vragen om meer servers of infrastructuur toe te voegen. Aan dit criterium wordt voldaan als UWV gebruikers en gegevens aan een dienst kan toevoegen of het gebruik van de dienst laat toenemen, zonder dat er tijd nodig is om infrastructuur toe te voegen.	

3.7.5. Artikel 7e – Wijzigingslogboek

7e.	**Wijzigingslogboek**	*Vereist*
Criterium	UWV vereist dat er logboeken bestaan voor alle SaaS-wijzigingsgebeurtenissen, zoals implementaties, verwijderingen en aanpassingen en dat deze in te zien zijn.	
Toelichting	UWV vereist dat er logboeken (wijzigingsgeschiedenis) bestaan voor alle SaaS-wijzigingsgebeurtenissen, zoals implementaties, verwijderingen en aanpassingen. Dit wijzigingsbeheerlogboek kan van cruciaal belang zijn voor het controleren of uitvoeren van een hoofdoorzaakanalyse van een gebeurtenis, incident of factureringsgeschil. De SaaS-leverancier moet logbestanden voor wijzigingsbeheer aanbieden die zes of meer maanden aan wijzigingsbeheergeschiedenis bevatten voor: • Gebeurtenissen maken/inrichten/bijwerken • Gebeurtenissen verwijderen/beëindigen • Toegangstoewijzing/wijziging Deze logbestanden kunnen worden gedownload of geëxporteerd naar CSV- en XML-bestandsformaten voor offline retentie/archivering en analyse.	

3.7.6. Artikel 7f – Prestatiemonitoring volgens eigen metrieken

7f.	**Prestatiemonitoring volgens eigen metrieken**	*Gewenst*
Criterium	De SaaS-leverancier biedt de mogelijkheid om aangepaste statistieken te definiëren die niet zijn opgenomen in de standaard prestatiemonitoringsrapporten.	
Toelichting	Om voor dit criterium in aanmerking te komen, moet de leverancier klantgedefinieerde-metrics aanbieden in ten minste de toegangs- en opslagdiensten, omdat deze diensten in een SaaS-oplossing vaak gekoppeld zijn aan SLA's en facturering. De leverancier moet de statistieken ook toegankelijk maken via zowel een API als een beheerconsole. Het biedt UWV de mogelijkheid om kosten door te belasten naar gebruik aan de organisatieonderdelen in geval van gezamenlijk gebruik.	

3.7.7. Artikel 7g – Beheerfunctie is robuust ingericht

7g.	**Beheerfunctie is robuust ingericht**	*Gewenst*
Criterium	De beheerinterfaces van de SaaS-oplossing (zoals API's, endpoints en CLI’s) en beheerconsole moeten op een hoog-beschikbare en hoog-toegankelijke manier worden ontworpen en geïmplementeerd.	
Toelichting	Geen enkel probleem in een onderliggend (cloud-)datacenter of infrastructuur mag een storing in de beheerbaarheid van de SaaS-oplossing veroorzaken. Als een deel van de SaaS-dienst niet beschikbaar is, moet UWV kunnen inloggen op de beheerconsole om de status van de omgeving te beoordelen of om gebruikers en bijbehorende gegevens voor de wel-beschikbare delen van de SaaS-dienst te beheren. De leverancier moet beheerinterfaces en -consoles op een hoog-beschikbare manier ontwerpen om bewijs te leveren dat zij ook hoog-beschikbare businessfuncties in de SaaS-dienst kunnen ontwerpen.	

3.7.8. Artikel 7h – Real-time notificaties op maat

7h.	**Real-time notificaties op maat**	*Gewenst*
Criterium	Prestatiedrempels (-limieten) kunnen worden gedefinieerd waarvoor UWV gewaarschuwd wil worden, via e-mail of webservices.	
Toelichting	-	

3.7.9. Artikel 7i – Acties op notificaties

7i.	**Acties op notificaties**	*Optioneel*
Criterium	Specifieke acties kunnen worden gedefiniëerd die een SaaS-dienst (automatisch) opvolgt op basis van prestatiedrempels of gebeurtenissen (notificaties).	
Toelichting	UWV wil vooraf specifieke acties kunnen definiëren die een SaaS-dienst (automatisch) zal opvolgen op basis van prestatiedrempels of gebeurtenissen (notificaties). Deze scenario's worden doorgaans elastischer wanneer componenten van de service dynamisch moeten groeien of krimpen op basis van belasting of prestaties. Een voorbeeld is het verhogen van een opslaglimiet wanneer een vooraf gedefinieerde drempel wordt bereikt, om het gebruik van de service te niet in gevaar te brengen. Voor de duur die nodig is om extra opslagkosten te voorkomen. Om aan dit criterium te voldoen, moet een SaaS-leverancier UWV in staat stellen een specifieke cloudactie uit te voeren (dat wil zeggen een beheerinterface aanroepen) wanneer een standaard of door de klant gedefinieerde prestatiedrempel wordt overschreden of een andersoortige notificatie van een gebeurtenis.	

3.8. Artikel 8 – Beveiliging

Het gebrek aan beveiligingsmogelijkheden en dan met name de controle hierop, van een SaaS-dienst is doorgaans de moeilijkste toetredingsdrempel voor de adoptie. De SaaS-aanbieder is verantwoordelijk voor het grootste deel van de infrastructuur en de beveiliging daarvan. Daarom is het voor UWV van cruciaal belang dat de competenties, best practices en verklaringen (proof of compliancy) van de SaaS-aanbieder transparant zijn tijdens het beveiligingsevaluatieproces (risicoanalyse).

Het beoordelen van een SaaS-aanbieder op informatiebeveiligingsaspecten vereist inzicht in de competenties van de aanbieder op drie belangrijke gebieden:

1. Gedocumenteerd beveiligingsbeleid en audits, certificering, bewijsstukken en/of evaluaties, een ingerichte beveiligingsorganisatie, inclusief processen, die de beveiligingsaanpak van de aanbieder valideren met betrekking tot beveiligingsnormen en/of compliance-raamwerken.
2. Controles die door de afnemer (UWV) binnen de SaaS-applicatie geconfigureerd kunnen worden die de mogelijkheid bieden voor applicatie- en gegevens-/transactiebeveiliging.
3. Controles bij externe partners van de SaaS-aanbieder, zoals IaaS-platforms of hostingdiensten waarop de SaaS-dienst is gebouwd en andere externe diensten waarvan de SaaS-dienst afhankelijk is.

Door transparantie en verificatie wordt vertrouwen opgebouwd. UWV zal een partnerschap aangaan met een SaaS-aanbieder dat gebaseerd moet zijn op zichtbaarheid van het beveiligingsecosysteem dat de SaaS-dienst omringt. Inzicht in welke infrastructuur en tools de SaaS-provider gebruikt om

de dienst te bouwen en in de markt te zetten, helpt bij de beveiligingsevaluatie van de end-to-end-stack van de leverancier.

Niet alle SaaS-aanbieders zijn even transparant over hun beveiliging. UWV moet inzicht krijgen in de risico's die ze loopt door gegevens onder te brengen bij de SaaS-dienst, deze begrijpen en mitigeren. Daarbij moet UWV zich wel houden aan de servicevoorwaarden van de SaaS-leverancier en deze accepteren, zodat er geen disputen ontstaan bij incidenten ten nadele van UWV. Afspraken hierover dienen in een bedrijfsovereenkomst (BVO[6]) te worden vastgelegd, op basis van één van de volgende uitgangspunten:

- De SaaS-dienst wordt gebruikt als de algemene voorwaarden acceptabel zijn, of
- UWV tekent het risico af en gebruikt de SaaS-dienst, zelfs als de algemene voorwaarden niet acceptabel zijn, of
- Risico's worden gemitigeerd door gebruik te maken van een 'cloud access security broker' (CASB)[7] dat functioneel beperkte toegang tot een SaaS-dienst verleent als de algemene voorwaarden niet acceptabel zijn, of door toevoeging van andere beveiligingsoplossingen.

Met betrekking tot de derde partijen (onderaannemers) van de SaaS-aanbieder moet UWV ervoor zorgen dat zij voldoende inzicht heeft in de identiteiten van die partijen waarvan de SaaS-dienst afhankelijk is. Het is belangrijk om te weten of de SaaS-aanbieder gebruik maakt van een IaaS- of PaaS-aanbieder van het hoogste niveau met sterke beveiligingspraktijken, in plaats van bijvoorbeeld een kleinere of minder bekende aanbieder met zwakke beveiligingspraktijken. Daarnaast moet UWV er rekening mee houden dat eventuele certificeringen van deze derde partijen niet automatisch betekenen dat de SaaS ook gecertificeerd is.

De criteria in deze sectie moeten worden beschouwd als aanvulling op de BVO als benoemd in sectie 2.1 Positionering.

[6] Zie 2.1 voor een link naar de UWV BVO met afspraken en eisen die minimaal standaard moeten worden opgenomen in de BVO.

[7] CASB's hebben ook ingebouwde risicodatabases voor cloudapplicaties, waar ze SaaS-applicaties hebben gescand, verzameld en geëvalueerd om te bepalen hoe riskant ze zijn voor organisaties. De gesteld eisen zijn mogelijk al door de CASB's geëvalueerd en stellen IT- en beveiligingsorganisaties in staat hun eigen onderzoek op maat te snijden bij de keuze van een SaaS-applicatie.

3.8.1. Artikel 8a – Gepubliceerd beleid inzake openbaarmaking en herstel van inbreuken

8a.	**Gepubliceerd beleid inzake openbaarmaking en herstel van inbreuken**	*Vereist*
Criterium	De SaaS-leverancier heeft gepubliceerd beleid inzake de openbaarmaking van inbreuken waarin wordt uiteengezet wie zij op de hoogte zullen stellen, hoe en wanneer zij hen op de hoogte zullen stellen en welke processen worden gevolgd om de gegevens, klanten en gebruikers van UWV te beschermen.	
Toelichting	UWV moeten op de hoogte zijn van inbreuken om erop te kunnen reageren, of dit nu betekent dat de bedrijfsstrategie moet worden gewijzigd omdat het vertrouwen verloren is gegaan, of dat zij moeten voldoen aan hun eigen verplichtingen inzake openbaarmaking van inbreuken. Deze verplichtingen zijn van toepassing op de eigenaar van de gegevens, ook al is de SaaS-leverancier mogelijk schuldig, en aan kennisgevings- of openbaarmakingsvereisten is vaak een deadline verbonden. Er kan cruciale tijd verloren gaan bij het wachten op een melding van de leverancier. Ook moet de onderneming zoveel mogelijk weten over de omvang van de inbreuk om te bepalen wat haar meldplichten of reactiemogelijkheden zijn. Om aan dit criterium te voldoen, heeft de SaaS-leverancier een beleid inzake de openbaarmaking van inbreuken te publiceren waarin wordt uiteengezet wie zij op de hoogte zullen stellen, hoe en wanneer zij hen op de hoogte zullen stellen en welke processen de SaaS-leverancier zal volgen om de gegevens, klanten en gebruikers van UWV te beschermen. Als onderdeel van de evaluatie van de SaaS-leverancier moet UWV het beleid inzake de openbaarmaking van inbreuken beoordelen om te bepalen of het voldoet aan de vereisten voor kennisgeving, hulp en herstel.	

3.8.2. Artikel 8b – Fysieke beveiliging

8b.	**Fysieke beveiliging**	*Vereist*
Criterium	De SaaS-leverancier verstrekt UWV details over de fysieke beveiliging die de datacentra en faciliteiten beschermt waarin de gegevens en informatie van UWV wordt opgeslagen.	
Toelichting	De details omvatten biometrie over fysieke toegangspunten, CCTV, beveiligingspersoneel, monitoring van natuurrampen en meerdere voedingspunten op het elektriciteitsnet.	

3.8.3. Artikel 8c – Onderzoeksondersteuning bij inbreuk of compromittering van gegevens of gebruikers

8c.	**Onderzoeksondersteuning bij inbreuk of compromittering van gegevens of gebruikers**	*Vereist*
Criterium	De SaaS-leverancier biedt UWV als onderdeel van het inbreukbeleid en -proces ondersteuning aan in onderzoeken bij inbreuk of compromittering van gegevens of gebruikers.	
Toelichting	Omdat de SaaS-leverancier de dienst beheert en toegang tot de infrastructuur over het algemeen niet bestaat, is UWV afhankelijk van de SaaS-leverancier om onderzoeksinspanningen te ondersteunen voor elk geïdentificeerde inbreuk of compromittering van gegevens of gebruikers in de dienst. Deze ondersteuning is gedetailleerd beschreven in het beveiligingsplan dat aan UWV wordt verstrekt tijdens de evaluatie van de SaaS-leverancier.	

3.8.4. Artikel 8d – Reputatie

8d.	**Reputatie**	*Vereist*
Criterium	De SaaS-leverancier verstrekt UWV informatie, waaronder de identificatie van eventuele inbreuken in het afgelopen jaar, de gevolgen van die inbreuken en het herstel van de situatie door de SaaS-leverancier, of pogingen tot inbreuk die succesvol zijn afgewend.	
Toelichting	Normaal onderzoek van leveranciers, inclusief SaaS-leveranciers, omvat doorgaans het vaststellen van de reputatie van de leverancier en het contacteren van geschikte referenties. Bij SaaS-leveranciers is het echter belangrijk om in dat normale controleproces een specifieke reputatiebeoordeling en vragen voor referentieklanten met betrekking tot beveiliging op te nemen. Om aan dit criterium te voldoen verstrekt de SaaS-leverancier informatie aan UWV, waaronder de identificatie van eventuele inbreuken in het afgelopen jaar, de gevolgen van die inbreuken en het herstel van de situatie door de SaaS-leverancier. Deze informatie helpt UWV bij het evalueren van de beveiligingsreputatie van de SaaS-leverancier. Daarnaast levert de SaaS-leverancier bij voorkeur (grote) referentieklanten voor de dienst, waarbij specifiek kan worden gevraagd naar hun ervaringen met de beveiligingsmaatregelen van de SaaS-leverancier. Inbreuken worden soms niet door een leverancier bekendgemaakt. Probeer daarom via afzonderlijke kanalen andere referenties te vinden. Geef de voorkeur aan leveranciers die gebruikersgemeenschappen hebben waarmee bestaande en potentiële klanten kunnen communiceren en netwerken met andere gebruikers op conferenties en in discussiedatabases. Beveiligingsbeoordelingsdiensten bieden ook betrouwbare en onafhankelijke informatie. BitSight en SecurityScorecard zijn voorbeelden van beveiligingsbeoordelingsdiensten. Daarnaast hebben de meeste CASB-aanbieders ook ingebouwde databases die beoordelingsgegevens (waaronder beveiliging, maar ook andere risicoaspecten) bevatten van populaire SaaS-leveranciers.	

3.8.5. Artikel 8e – Beoordelingen door derden

8e.	**Beoordelingen door derden**	*Vereist*
Criterium	De SaaS-leverancier heeft in de afgelopen twaalf maanden minimaal één beveiligingsaudit van zijn dienst door een erkend onafhankelijk accountantskantoor of beveiligingsorganisatie laten uitvoeren.	
Toelichting	Dit is een basisvereiste. Specifieke audits of raamwerken voor een audit moeten worden geselecteerd uit de voorkeurs- of optionele criteria, afhankelijk van de behoeften van UWV (zie ook BVO). Het is onpraktisch voor een SaaS-leverancier om audits door individuele klanten toe te staan, maar het is wel praktisch om hen evaluatieresultaten van derden te verstrekken. SaaS-leveranciers delen deze audits graag, maar de reikwijdte van de audit is enorm belangrijk. Zo geven sommige SaaS-leveranciers aan dat ze een SOC 2 hebben, maar geldt SOC 2 alleen voor de onderliggende IaaS. Het is van essentieel belang dat de beveiligingscontroles worden geëvalueerd en geïnspecteerd door een objectieve derde partij. Beweren dat er controles aanwezig zijn, is één ding; het hebben van een beoordeling door een derde partij die bewijst van hun bestaan, de succesvolle werking ervan en deze goed onderhouden worden is iets anders. De afgelopen jaren hebben alle soorten leveranciers van clouddiensten (IaaS, PaaS en SaaS) laten zien dat ze begrijpen hoe belangrijk assessments door derden zijn door deel te nemen aan meerdere – vaak overlappende en complementaire – assessmentprogramma's. Aan beoordelingen door derden die worden uitgevoerd door een auditor of examinator met gebruikmaking van een gevestigde standaard voor evaluatie en ondersteund door hun verzekering tegen wanpraktijken of aansprakelijkheid voor fouten wordt meer aandacht aan besteed dan aan beoordelingen zonder expliciete kwalificaties van de beoordelaar of professionele normen. Vaak bevatten deze rapporten 'gebruikerscontroleoverwegingen': controles waarvan de beoordeling veronderstelt dat deze door de gelicenseerde organisatie als UWV worden uitgevoerd. Deze controles beperken de controleverantwoordelijkheden van de dienstverlener of verduidelijken de verantwoordelijkheden van de onderschrijvende organisaties als UWV. Ze moeten vóór adoptie worden geëvalueerd, en ze kunnen op elk moment veranderen. HIPAA BAA's bevatten vaak lijsten met controles die door de afnemer moeten worden geïmplementeerd voor een conforme werking. Ten slotte kan het bedrijfsprobleem dat moet worden aangepakt of het beoogde gebruik van de SaaS-oplossing aanleiding geven tot een vereiste voor bepaalde beoordelingen of certificeringen. Vereiste beoordelingen moeten de International Organization for Standardization (ISO) 27000 en Service and Organization Controls (SOC) 2 omvatten.	

3.8.6. Artikel 8f – ISO 27000

8f.	**ISO 27000**	*Vereist*
Criterium	De SaaS-leverancier levert het bewijs van een externe audit, certificering en verklaring van toepasbaarheid in de afgelopen twaalf maanden voor ten minste ISO 27001.	
Toelichting	ISO 27000 is een reeks normen voor informatiebeveiligingsbeheersystemen die zijn gepubliceerd door de ISO. Twee veel voorkomende certificeringen zijn ISO 27001[8] en ISO 27018[9]. Om aan deze vereiste te voldoen, levert de SaaS-leverancier het bewijs van een externe audit, certificering en verklaring van toepasbaarheid in de afgelopen twaalf maanden voor ten minste ISO 27001. ISO 27001 is heel gebruikelijk voor de grotere cloudleveranciers, maar het is een generieke standaard zonder cloud-specifieke inhoud. Een klein maar groeiend aantal heeft formele beoordelingen uitgevoerd van de twee cloudspecifieke praktijkkaders: ISO 27017 (praktijkcode voor informatiebeveiligingscontroles gebaseerd op ISO/IEC 27002 voor clouddiensten) en ISO 27018 (praktijkcode voor de bescherming van persoonlijk identificeerbare informatie [PII] in public cloud die fungeren als PII-verwerkers).	

3.8.7. Artikel 8g – SOC 2 beoordeling

8g.	**SOC 2 beoordeling**	*Vereist*
Criterium	De SaaS-leverancier levert het bewijs van een jaarlijkse audit door een onafhankelijke externe auditor middels het verstrekken van een Service Organization Control (SOC) 2-rapport niet ouder dan een jaar.	
Toelichting	Vervang deze vereiste niet door een SOC 1-rapport. SOC 1-rapporten evalueren financiële controles en doen geen uitspraken over informatiebeveiliging. Andere veel voorkomende beoordelingen die relevant zijn voor SaaS worden vermeld verderop als gewenst of optioneel.	

[8] The ISO 27000 Directory
[9] ISO/IEC 27018:2014

3.8.8. Artikel 8h – Geprivilegieerde en administratieve toegangscontroles

8h.	**Geprivilegieerde en administratieve toegangscontroles**	*Vereist*
Criterium	De SaaS-leverancier heeft geprivilegieerde en administratieve toegangscontroles voor personeel op basis van de behoefte (least-privileged) waarbij toegang wordt gemonitord, om ongeautoriseerde toegang tot gegevens te voorkomen en te detecteren en geprivilegieerde en beheerdersreferenties niet kunnen worden misbruikt.	
Toelichting	Toegang van personeel of derden van de SaaS-leverancier tot productiesystemen en klantgegevens vindt plaats op basis van de behoefte en wordt gemonitord om ervoor te zorgen dat de werknemers, contractanten en externe leveranciers van de SaaS-provider geen onbelemmerde toegang hebben tot gegevens van UWV. Bovendien zijn er controles om ervoor te zorgen dat deze geprivilegieerde en beheerdersreferenties niet kunnen worden misbruikt als ze bekend worden bij een aanvaller. Om aan dit criterium te voldoen, heeft de dienst alle volgende controles actief: • Geen permanente toegang. Toegang tot productiesystemen wordt alleen verleend om geïdentificeerde en goedgekeurde taken uit te voeren, en wordt vervolgens onmiddellijk weer ingetrokken. • Multifactor-authenticatie. Voor alle toegang tot productiesystemen en infrastructuur waarop de SaaS-dienst zich bevindt, is multifactor-authenticatie vereist zijn om de impact te verminderen van inloggegevens die door een aanvaller worden gestolen of onderschept. • Monitoring. De acties die individuen ondernemen terwijl ze geprivilegieerde of beheerderstoegang hebben, worden gelogd en geregistreerd, zodat ze duidelijk en volledig kunnen worden begrepen wanneer ze worden beoordeeld. Dit bevat duidelijke informatie over welke gegevens of bestanden naar of uit de productieomgeving worden overgebracht.	

3.8.9. Artikel 8i – Toegang tot auditlogboeken

8i.	**Toegang tot auditlogboeken**	*Vereist*
Criterium	De SaaS-leverancier verstrekt de auditlogboeken rond administratieve toegang en activiteiten die betrekking hebben op de tenant van UWV.	
Toelichting	De SaaS-leverancier geeft toegang tot auditlogboeken voor administratieve toegang en actie voor bedrijfsgegevens en gebruikersinformatie. Een belangrijke methode voor beveiligingsverificatie voor UWV is het verkrijgen en beoordelen van de SaaS-leverancier voor administratieve toegang en actielogboeken voor de tenant van UWV. De SaaS-leverancier verstrekt deze logboeken regelmatig ter beoordeling aan UWV. De SaaS-leverancier biedt UWV op zijn minst de mogelijkheid om zelf een kopie van de toegangs- en actielogboeken op te vragen, en levert deze logbestanden binnen één werkdag aan. Optioneel kunnen leveranciers de doorlopende mogelijkheid bieden om deze logboeken op te nemen in een SIEM-oplossing (Security Information and Event Management). Een geavanceerdere functie ten slotte is de mogelijkheid om UWV beheerderstoegang te verlenen voor het inzien van de logboeken.	

3.8.10. Artikel 8j – Screening van personeel

8j.	**Screening van personeel**	*Vereist*
Criterium	De SaaS-leverancier volgt verifieerbaar best-practices bij het screenen en aannemen van werknemers die toegang hebben tot en verantwoordelijk zijn voor de bedrijfsgegevens en gebruikersinformatie binnen de SaaS-dienst.	
Toelichting	De SaaS-leverancier heeft screening- en aanwervingsprocedures voor werknemers die toegang hebben tot bedrijfsgegevens en gebruikersinformatie. UWV kan verifiëren middels opgevraagde documentatie dat de SaaS-leverancier best-practices volgen bij het screenen en aannemen van werknemers die toegang hebben tot en verantwoordelijk zijn voor de bedrijfsgegevens en gebruikersinformatie binnen de SaaS-oplossing. De SaaS-leverancier heeft hun screening- en wervingspraktijken gedocumenteerd. Daarnaast kan de SaaS-leverancier aantonen dat het dit eist van alle derde partijen die toegang krijgen tot de gegevens van klanten, en beschikt het over een bijbehorend governanceprogramma.	

3.8.11. Artikel 8k – Preventie, auditing en melding van ongepaste beheeractiviteiten

8k.	**Preventie, auditing en melding van ongepaste beheeractiviteiten**	*Vereist*
Criterium	De SaaS-leverancier levert bewijs van aanwezige detectie en preventie van ongepaste beheeractiviteiten binnen de dienst, inclusief een meldingsprocedure in geval van een incident.	
Toelichting	Wachten tot ongepaste beheeractiviteiten plaatsvinden is te laat. De SaaS-leverancier levert UWV het bewijs van aanwezige detectie en preventie van ongepaste beheeractiviteiten binnen de dienst. Het beschikt ook over een meldingsprocedure waarin het tijdsbestek, de details, de impact en de oplossingsinspanningen van de SaaS-leverancier worden beschreven in het geval van een incident dat gevolgen heeft (of potentieel zou kunnen hebben) voor UWV.	

3.8.12. Artikel 8l – API voor beveiligingsfuncties

8l.	**API voor beveiligingsfuncties**	*Vereist*
Criterium	De SaaS-leverancier biedt API-toegang tot alle beveiligingsfuncties om integratie te bieden met CASB, SIEM, gebruikers- en entiteitsgedragsanalyse (UEBA) en andere beveiligingsoplossingen als ook voor het ondersteunen van SOAR (Security Orchestration and Automated Respons).	
Toelichting	Beschikbare functies zijn onder meer de opname van activiteitenlogboeken, gegevensbescherming, toegangscontrole, UEBA, beveiligingsconfiguratie en handhaving als ook functies voor het ondersteunen van SOAR. SOAR. SOAR-technologie biedt een end-to-endsysteem dat automatisch kwetsbaarheden opspoort en daarop reageert zonder menselijke tussenkomst on SOC-teams te ontlasten. Daar de SaaS-dienst integraal onderdeel uitmaakt van het UWV landschap is *end-to-end* monitoring en automated incident respons zeer nodig en zal SOAR ondersteund worden door de SaaS-dienst in haar API's.	

3.8.13. Artikel 8m – Veilige en gecodeerde API's/open interfaces

8m.	**Veilige en gecodeerde API's/open interfaces**	*Vereist*
Criterium	De SaaS-leverancier verstrekt informatie over hoe API's en open interfaces worden beveiligd en gecodeerd en aantonen dat deze SSD (Secure Software Development) of OWASP compliant zijn.	
Toelichting	SaaS-oplossingen kunnen een grote verscheidenheid aan toegangsmethoden bieden tot gegevens, applicaties, gebruikers en diensten via API's en open interfaces. Het beveiligen van interfaces en het waar mogelijk gebruiken van encryptie zijn beide belangrijk voor het beschermen van bedrijfsgegevens in een SaaS-oplossing. De SaaS-leverancier verstrekt informatie over hoe API's en open interfaces worden beveiligd en gecodeerd, eventueel specifiek voor integratie met UWV, en toont aan dat deze SSD of OWASP compliant zijn	

3.8.14. Artikel 8n – Multitenant-controles voor scheiding

8n.	**Multitenant-controles voor scheiding**	*Vereist*
Criterium	De SaaS-leverancier verstrekt informatie over multitenant-controls hoe gebruikers en gegevens van klanten in een multi-tenant omgeving gescheiden worden gehouden.	
Toelichting	Als een multitenant-dienst wordt aangeboden, verstrekt de SaaS-leverancier informatie waarin het uitlegt hoe de logische vergrendelingen die de data en toegang van de tenant gescheiden worden gehouden, terwijl dezelfde bronnen worden gebruikt, zoals hardware, opslag en authenticatie. Dat kan bijvoorbeeld in een gepubliceerd beveiligingswitboek. De informatie omvat hoe identiteitscontroles worden gebruikt om de scheiding te bewerkstelligen.	

3.8.15. Artikel 8o – Encryptie data-in-transit

8o.	**Encryptie data-in-transit**	*Vereist*
Criterium	De SaaS-leverancier zorgt ervoor dat gegevens tijdens de overdracht zijn geëncrypt, minimaal TLS 1.3 of IPsec.	
Toelichting	Elke overdracht van gegevens of elektronische communicatie tussen de SaaS-provider en bedrijfseindpunten worden tijdens de overdracht gecodeerd met gestandaardiseerde protocollen zoals Transport Layer Security (TLS) of IPsec. De protocollen zijn van een recente versie zijn zonder bekende kwetsbaarheden, waarbij gebruik wordt gemaakt van implementaties zonder bekende exploits. Zij zijn NCSC compliant (Nationaal Cyber Security Center).	

3.8.16. Artikel 8p – Adaptieve toegangscontrole

8p.	**Adaptieve toegangscontrole**	*Vereist*
Criterium	De SaaS-dienst biedt ondersteuning voor adaptieve en conditionele toegangscontrole met een juiste granulariteit.	
Toelichting	Het beschermen van de service en gegevens tegen ongeautoriseerde toegang is een belangrijke vereiste voor ondernemingen die SaaS-oplossingen willen gebruiken. De SaaS-leverancier geeft UWV een gedetailleerde uitleg van de methodologieën die in de service worden gebruikt om ongeautoriseerde toegang te voorkomen op basis van gebruikers-, apparaat-, gedrags- en kwaadaardige informatie of andere type condities (conditional access). De granulariteit van deze controles is belangrijk om te begrijpen, omdat beperkte granulariteit (bijvoorbeeld alle gebruikers van UWV die in de service zijn ingericht, alle inhoud kunnen zien) UWV ervan kan weerhouden de SaaS-oplossing te gebruiken vanwege wettelijke vereisten.	

3.8.17. Artikel 8q – Configureerbare content-beveiliging

8q.	**Configureerbare content-beveiliging**	*Vereist*
Criterium	De SaaS-leverancier moet configureerbare content hygiene-mogelijkheden bieden als onderdeel van de dienst zodat controles kunnen worden afgestemd op de behoefte	
Toelichting	Content-beveiligings/-hygiene-oplossingen (bijv. antivirus/antispam) beschermen UWV tegen malware en verschillende vormen van aanvallen die via externe communicatie en gegevensuitwisseling binnenkomen (bijvoorbeeld phishing, adware en wormen). Aanvallen kunnen het gebruik van de SaaS-oplossing door UWV verstoren en bedrijfsgegevens en -infrastructuur infiltreren, afhankelijk van de gebruikte service en de verbindingen met UWV. Content hygiene-controles kunnen worden afgestemd om meer of minder streng te zijn, wat van invloed is op de service die wordt geleverd. Het is belangrijk om UWV enige controle over die afstemming te geven; UWV moet de content hygiene-controles kunnen aanpassen aan haar zakelijke behoeften. Strikte spamcontroles op e-mail kunnen bijvoorbeeld problematisch zijn voor UWV die regelmatig e-mail gebruikt om met consumenten te communiceren. Strikte controles kunnen resulteren in het blokkeren van legitieme berichten van de grote verscheidenheid aan e-mailoplossingen voor consumenten. De SaaS-leverancier moet configureerbare content hygiene-mogelijkheden bieden aan UWV als onderdeel van de service waarmee UWV de controles kan afstemmen.	

3.8.18. Artikel 8r – Gedocumenteerde DDoS-preventiemogelijkheden

8r.	**Gedocumenteerde DDoS-preventiemogelijkheden**	*Vereist*
Criterium	De SaaS-leverancier levert documentatie met procedures en tools om de impact van DDoS-aanvallen op de SaaS-dienst(en) en API's te weerstaan of te verminderen.	
Toelichting	De SaaS-leverancier heeft procedures en tools om de impact van DDoS-aanvallen op SaaS-diensten en API's te weerstaan of te verminderen. De SaaS-leverancier verstrekt documentatie aan UWV met daarin de gebruikte technologieën en mogelijkheden, evenals processen voor het omgaan met incidenten. Deze dienen state-of-the-art te zijn om de grootste aanvallen te kunnen pareren.	

3.8.19. Artikel 8s – Privacy en anonimiseren van persoonsgegevens

8s.	**Privacy en anonimiseren van persoonsgegevens**	*Vereist*
Criterium	De SaaS-leverancier en de SaaS-dienst ondersteunen het anonimiseren en beschermen van gebruikers en/of persoonsgegevens met het inzetten van passende methoden en technieken.	
Toelichting	Privacy en anonimiseren van gebruikers- en/of persoonsgegevens ter ondersteuning van nalevingsnormen zijn geborgd in het ontwerp en functies van de SaaS-dienst. De SaaS-leverancier voldoet aan Algemene Verordening Gegevensbescherming (AVG), anonimiseren en beschermen van gebruikersgegevens zijn vereiste functies van de SaaS-leverancier en -dienst. Technieken kunnen pseudonimisering, hashing of volledige anonimisering van gebruikersgegevens omvatten. Anonimisering van gebruikersgegevens wordt gerespecteerd door zowel de gebruikersinterface als API's van de SaaS-oplossing.	

3.8.20. Artikel 8t – Beveiligingstesten zijn geborgd in releases

8t.	**Beveiligingstesten zijn geborgd in releases**	*Vereist*
Criterium	De SaaS-leverancier heeft beveiligingstesten opgenomen in het releasemanagementproces.	
Toelichting	De SaaS-leverancier heeft een gedocumenteerd, veilig softwareontwikkelingsproces, met daarin geborgd uitvoering van geautomatiseerde codescans en pentests op alle door de leverancier ontwikkelde code. Rapportages hierover zijn inzichtelijk voor UWV. Het is aan UWV om al dan niet gerichte pentests uit te voeren op basis van de aangeleverde documentatie. Zie ook Artikel 8z – Regelmatige penetratietests.	

3.8.21. Artikel 8u – Encryptiesleutels in eigen beheer

8u.	**Encryptiesleutels in eigen beheer**	*Vereist*
Criterium	De SaaS-leverancier maakt het UWV mogelijk om encryptiesleutels op basis van standaarden in eigen beheer te nemen en om tokenisatie toe te kunnen passen.	
Toelichting	De SaaS-leverancier maakt met een open of op standaarden gebaseerde API het beheren van door de client (UWV) gecontroleerde encryptiesleutels (HYOK of BYOK) mogelijk. Wanneer de encryptie van gegevens wordt geleverd/gedaan door de SaaS-oplossing, is het beheer van de sleutels door UWV als afnemer vaak noodzakelijk voor een effectieve implementatie. Ook op basis van wet- en regelgeving verwachten toezichthouders bewijs dat UWV de sleutels beheert en de controle over het gebruik van de sleutels kan documenteren. Bovendien is het gebruik van een open of op standaarden gebaseerde API, zoals het key management interoperability protocol (KMIP), wenselijk boven propriëtaire API's. Bring your own key (BYOK) is een andere belangrijke functie die vereist is door zwaar gereguleerde organisaties als UWV in geval van (zeer) gevoelige data. BYOK is de functionele mogelijkheid binnen de oplossing om sleutels te genereren via software key vaults of on-premises hardware security modules (HSM's). Hold your own key (HYOK) is waar UWV een sleutel genereert en gegevens versleutelt voor volledige scheiding van de SaaS-leverancier. Tokenisatie betreft het aan UWV zijde tokeniseren en de-tokeniseren van (sleutel)velden zonder aanpassing van de databasestructuur waardoor data geen waarde hebben voor andere entiteiten.	

3.8.22. Artikel 8v – Integratie met CASB-leveranciers

8v.	**Integratie met CASB-leveranciers**	*Vereist*
Criterium	De SaaS-leverancier ondersteunt samenwerking en integratie met toonaangevende CASB-leveranciers (Cloud Access Security Brokerage) tbv UEBA (User/Entity Behavior Analytics) en DLP (Data Loss Prevention).	
Toelichting	De SaaS-leverancier werkt samen met toonaangevende CASB-leveranciers om UEBA en DLP volledig te ondersteunen. De SaaS-leverancier heeft API's voor CASB-leveranciers om de applicatie aan te roepen voor gebruikers- en entiteitsgedragsbewaking en gegevensverliespreventiemogelijkheden. De samenwerking kan gebeurtenissen blootleggen en biedt beschermingsmogelijkheden. Enkele voorbeelden zijn de mogelijkheid om bestanden die niet voldoen aan het CASB DLP-beleid in quarantaine te plaatsen en te verwijderen en gebruikers uit te sluiten als onverwacht gedrag wordt gedetecteerd.	

3.8.23. Artikel 8w – Toestaan van 3rd-party onderzoek

8w.	**Toestaan van 3rd-party onderzoek**	*Gewenst*
Criterium	De SaaS-leverancier ondersteunt, staat toe, onderzoek door derden in geval van inbreuk of compromittering van gegevens of gebruikers.	
Toelichting	Een alternatief voor het rechtstreeks leveren van onderzoeksondersteuning aan UWV is dat de SaaS-leverancier gedetailleerd beschrijft welke onderzoeksondersteuning het levert en akkoord gaat met het verlenen van volledige onderzoekstoegang door een wederzijds overeengekomen derde partij. Deze derde partij moet de nodige controles en juridische overeenkomsten hebben met zowel de SaaS-leverancier als UWV om ieders belangen te beschermen. Dit vergroot mogelijk de hoeveelheid informatie die kan worden verstrekt ter ondersteuning van het onderzoek, omdat de derde partij in staat zal zijn om de belangen van andere klanten te beschermen, zoals wanneer loggegevens informatie van meerdere klanten bevatten.	

3.8.24. Artikel 8x – Configureerbare DLP opties

8x.	**Configureerbare DLP opties**	*Gewenst*
Criterium	De SaaS-leverancier ondersteunt het configureren van DLP door de klant aan de hand van een aantal opties (policies).	
Toelichting	De SaaS-leverancier kan IT DLP-oplossingen implementeren die gegevens monitoren om inbreuken of verlies van gevoelige bedrijfsgegevens te voorkomen. De SaaS-leverancier kan DLP ook implementeren binnen hun services en afnemers als UWV de mogelijkheden bieden om zelf de DLP-instellingen te configureren om inbreuken en verlies van gevoelige gegevens te voorkomen. Een SaaS-e-mailservice kan bijvoorbeeld extra DLP-mogelijkheden bieden aan een onderneming om te voorkomen dat overheidsidentificatie- of creditcardnummers via e-mail worden verzonden vanuit de SaaS-oplossing. Om aan dit criterium te voldoen, biedt de SaaS-leverancier de mogelijkheid om de DLP te configureren die binnen de service wordt geboden, bijvoorbeeld door de mogelijkheid te bieden om DLP-beleidsjablonen (policies) te selecteren voor belangrijke naleving van wet- en regelgeving, zoals de AVG of BIO. Bovendien moet de service proactief de informatie markeren of voorkomen dat deze wordt opgeslagen; het is niet voldoende om UWV achteraf op de hoogte te stellen dat verdachte informatie is opgeslagen.	

3.8.25. Artikel 8y – Kwetsbaarheidsscans op applicatieniveau

8y.	**Kwetsbaarheidsscans op applicatieniveau**	*Gewenst*
Criterium	De SaaS-leverancier biedt een proces om kwetsbaarheidsscans op de service aan te vragen en de mogelijkheid om deze uit te voeren.	
Toelichting	Kwetsbaarheidsscans (vulnerability scans) helpen valideren dat de SaaS-oplossing veilig is, met name na wijzigingen of upgrades van de service. De SaaS-leverancier biedt UWV het proces om kwetsbaarheidsscans op de service aan te vragen en de mogelijkheid om deze uit te voeren. Als alternatief regelt de SaaS-leverancier onafhankelijke derde partijen om periodieke kwetsbaarheidsscans uit te voeren en de resultaten aan UWV te rapporteren, als de mogelijkheid niet rechtstreeks wordt geboden. De scans moeten actuele CVE kwetsbaarheden (Common Vulnerabilities and Exposures) vanaf een bepaalde score automatisch herkennen, rapporteren en hierop acties uitzetten.	

3.8.26. Artikel 8z – Regelmatige penetratietests

8z.	**Regelmatige penetratietests**	*Gewenst*
Criterium	De SaaS-leverancier biedt een proces om penetratietests op de service aan te vragen en de mogelijkheid om deze uit te voeren, inclusief een initiële pentest voor of bij ingebruikname.	
Toelichting	Net als kwetsbaarheidsscans helpen penetratietests bij het valideren dat de SaaS-oplossing veilig is. De SaaS-leverancier biedt UWV een proces om penetratietests aan te vragen en uit te (laten) voeren tegen de service, of regelt onafhankelijke derde partijen om periodieke penetratietests uit te voeren en de resultaten te rapporteren. Vaak zijn SaaS-providers terughoudend om details van penetratietests of kwetsbaarheidsrapporten openbaar te maken vanwege het risico dat ze een aanval op hen kunnen uitvoeren. Gezuiverd bewijs moet echter gemakkelijk te leveren zijn. Voorbeelden zijn: • Een factuur voor penetratietestservices of een brief van de SaaS-leverancier waarin de uitgevoerde services worden beschreven. • Documentatie van interne of externe auditors van tijdige en volledige naleving van kwetsbaarheidsdetectie- en herstelbeleid en -procedures.	

3.8.27. Artikel 8aa – Gedocumenteerde inbraakpreventie en -detectie

8aa.	**Gedocumenteerde inbraakpreventie en -detectie**	*Gewenst*
Criterium	De SaaS-leverancier verstrekt documentatie met daarin de gebruikte technologieën en mogelijkheden betreffende inbraakpreventie en -detectie, evenals processen voor het omgaan met incidenten.	
Toelichting	De SaaS-oplossing bevat oplossingen t.b.v. inbraakpreventie en -detectie. De SaaS-leverancier verstrekt documentatie aan UWV met daarin de gebruikte technologieën en mogelijkheden, evenals processen voor het omgaan met incidenten.	

3.8.28. Artikel 8ab – Zelfbeoordeling op basis van CSA

8ab.	**Zelfbeoordeling op basis van CSA**	*Gewenst*
Criterium	De SaaS-leverancier onderneemt een zelfbeoordeling op basis van Cloud Security Alliance (CSA) Security, Trust, Assurance en Risk (STAR) criteria en vertrekt rapportages met de resultaten.	
Toelichting	De SaaS-leverancier voert een zelfevaluatie uit op basis van de CSA Security, Trust, Assurance and Risk (STAR)-criteria. Als een SaaS-leverancier deze zelfevaluatie heeft uitgevoerd, kan deze UWV gedetailleerd inzicht geven in zijn beveiligingscontroles via de Consensus Assessments Initiative Questionnaire (CAIQ).	

3.8.29. Artikel 8ac – Security health check

8ac.	**Security health check**	*Gewenst*
Criterium	De SaaS-leverancier biedt een security health check en scoring tools.	
Toelichting	De SaaS-leverancier heeft security health check- en scoringtools opgenomen als onderdeel van de dienst om IT-organisaties, en dus ook UWV, te helpen de security posture van de totale SaaS-oplossing te begrijpen. Dit stelt de SaaS-leverancier ook in staat om voorschrijvende richtlijnen en best practices te leveren over hoe UWV haar specifieke tenant kan beschermen.	

3.8.30. Artikel 8ad – Dataclassificatie of -tagging

8ad.	**Dataclassificatie of -tagging**	*Gewenst*
Criterium	De SaaS-leverancier biedt methoden en technieken voor dataclassificatie of -tagging.	
Toelichting	Naarmate er meer gegevens naar cloud SaaS-applicaties worden verplaatst, wordt het belang van gegevensclassificatie of tagging steeds belangrijker om te helpen met algemene gegevensbeschermingsstrategieën. Hierdoor kan UWV begrijpen welke en waar gevoelige gegevens worden opgeslagen en beleid opstellen om te voorkomen dat bepaalde gegevenstypen worden blootgesteld. Het vergemakkelijkt ook datagovernance en e-discovery-scenario's (b.v. Woo-verzoeken).	

3.8.31. Artikel 8ae – Locatie-gebaseerde toegangscontrole

8ae.	**Locatie-gebaseerde toegangscontrole**	*Optioneel*
Criterium	De SaaS-leverancier biedt locatie-gebaseerde of -gevoelige toegang, inclusief de mogelijkheid om op persoonsniveau te whitelisten.	
Toelichting	Gebruikersmobiliteit blijft groeien naarmate meer en meer tablets, smartphones en persoonlijke laptops de primaire apparaten van gebruikers worden. De mogelijkheid om geavanceerdere adaptieve toegangsbeleid te implementeren kan nodig zijn. Een voorbeeld is de mogelijkheid om gebruikers te blokkeren of te beperken in hun toegang tot de SaaS-applicatie op basis van hun locatie.	

3.9. Artikel 9 – Dataopslag

UWV moet de wijze van dataopslag bij de SaaS-dienst onderzoeken. Een SaaS-dienst kan een aanzienlijke operationele last van het UWV wegnemen, maar SaaS-oplossingen hoeven niet goedkoop op dit gebied te zijn en sommige vereisen extra werk voor volledige gegevensbescherming. Een evaluatie van dataopslag is daarom op zijn plaats.

UWV moet rekening houden met de regelgevende gevolgen van het opslaan van gebruikersgegevens en content bij SaaS-diensten. UWV moet ervoor zorgen dat het plaatsen van gegevens, persoonlijke informatie in het bijzonder, in de cloud niet resulteert in verlies (van de waarde) van de gegevens of in strijd is met de toepasselijke wettelijke vereisten.

3.9.1. *Artikel 9a – Hoge beschikbaarheid en herstelbaarheid*

9a.	**Hoge beschikbaarheid en herstelbaarheid**	*Vereist*
Criterium	De SaaS-leverancier voorziet UWV van gedocumenteerde competenties en procedures voor hoge beschikbaarheid (HA – High Availability), een gepubliceerd trackrecord voor de beschikbaarheid van de dienst gedurende ten minste het afgelopen jaar en een gedetailleerde beschrijving van hoe de dienst zal worden hersteld in het geval van een storing of een ramp (DR – Disaster Recovery).	
Toelichting	In de SLA moet de SaaS-leverancier de hersteltijddoelstelling (RTO – Recovery Time Objective) en de herstelpuntdoelstelling (RPO – Recovery Point Objective) opgeven van de gemeenschappelijke applicatie-infrastructuur die wordt gebruikt om de SaaS-dienst te leveren. De aanvaardbare RTO en RPO moeten specifiek door UWV worden gedefinieerd voor de SaaS-oplossing die wordt geëvalueerd. Daarnaast moet de SaaS-leverancier testresultaten beschikbaar stellen die hun DR- en HA-procedures demonstreren.	

3.9.2. *Artikel 9b – Verwijderen en opruimen van gegevens*

9b.	**Verwijderen en opruimen van gegevens**	*Vereist*
Criterium	De SaaS-leverancier garandeert UWV dat, zodra UWV besluit gegevens te verwijderen, niemand van het personeel er nog toegang toe heeft en dat deze ook uiteindelijk fysiek worden verwijderd.	
Toelichting	De SaaS-leverancier geeft UWV een gedetailleerde beschrijving van de manier waarop gegevens uit de dienst worden verwijderd (op basis van dataretentieregels) en het tijdsbestek voor de complete opruiming (permanente fysieke vernietiging op basis van bewaartermijn), zodra UWV besluit de gegevens te verwijderen. Dit omvat alle kopieën van de gegevens die worden gemaakt via replicatie voor HA en DR. De SaaS-aanbieder moet zijn klanten een opruimingsgarantie bieden. Dat wil zeggen, een garantie dat, na de gespecificeerde periode, de gegevens die UWV heeft gekozen om te verwijderen of uit de dienst te verwijderen, volledig verdwenen zijn, zonder dat er ergens kopieën aanwezig zijn binnen de infrastructuur van de SaaS-leverancier.	

3.9.3. *Artikel 9c – Voldoen aan wet- en regelgeving voor gegevensopslag*

9c.	**Voldoen aan wet- en regelgeving voor gegevensopslag**	*Vereist*
Criterium	De SaaS-leverancier voldoet aantoonbaar aan de relevante normen voor gegevensopslag.	
Toelichting	De SaaS-leverancier documenteert de processen en procedures om te voldoen aan relevante nalevingsnormen voor gegevensopslag, zoals AVG. Deze documentatie is inzichtelijk. Als de SaaS-leverancier persoonlijke gegevens opslaat, moet uit de documentatie blijken hoe de leverancier aan de AVG voldoet en (aan de hand van richtlijnen) hoe UWV kan voldoen aan de AVG. In dit geval blijkt ook hoe wordt voldaan aan de richtlijn "(bijzondere) persoongegevens in de public cloud"[10] en in het bijzonder "*data at rest is versleuteld volgens <richtlijn cryptografie en versleuteling>".*	

[10] Richtlijn (Bijzondere) persoonsgegevens in de public cloud

3.9.4. Artikel 9d – Historiseren van transacties

9d.	**Historiseren van transacties**	*Vereist*
Criterium	De SaaS-dienst is waar nodig in staat om transacties te verwerken in een geldigheidstijdlijn en transactietijdlijn.	
Toelichting	De implementatie van deze tijdlijnen garandeert dat waarden van een data element historisch te traceren zijn, inclusief eventuele correcties van die data waarden. Dit voorkomt bijvoorbeeld dat een historische data waarde met een terugwerkende kracht mutatie wordt overschreven zonder dat de oude waarde nog beschikbaar is voor reconstructie. Of en hoe lang de historie vastgehouden moet houden verschilt per type transactie en is afhankelijk van het bedrijfsproces en wetgeving. De geldigheidsdimensie verwijst naar het moment waarop een gebeurtenis daadwerkelijk plaatsvindt of het moment waarop een toestand intreedt. We spreken hier van "datum aanvang geldigheid" en "datum einde geldigheid". Deze dimensie is alleen van toepassing voor tijdsafhankelijke gegevenselementen. De transactiedimensie verwijst naar het moment waarop een gebeurtenis aan een informatie systeem bekend werd gemaakt. Hier spreken we van een "transactiemoment". Dit is altijd aan de orde en is van toepassing voor zowel tijdsafhankelijke als voor tijdsonafhankelijke gegevenselementen.	

3.9.5. Artikel 9e – Documentatie over opslaglimieten

9e.	**Documentatie over opslaglimieten**	*Vereist*
Criterium	De SaaS-leverancier verstrekt informatie over opslaglimieten die binnen de SaaS-oplossing worden opgelegd.	
Toelichting	De opslaglimieten zijn o.a. gedefinieerd per dienst, groep en gebruiker. De limieten zijn gedefinieerd, inzichtelijk en redelijk voor de SaaS-oplossing, groep of klasse van gebruikers en/of een specifieke gebruiker. Deze informatie moet op een klantenportaal of website zijn gepubliceerd.	

3.9.6. Artikel 9f – Opslaglimieten overschrijden

9f.	**Opslaglimieten overschrijden**	*Vereist*
Criterium	De SaaS-leverancier biedt de mogelijkheid om de limieten voor gegevensopslag te overschrijden zonder de dienstverlening te beïnvloeden (zoals een verslechtering van de dienst).	
Toelichting	Het overschrijden van de overeengekomen opslaglimieten kan extra kosten met zich meebrengen en kan bespreekbaar zijn. De SaaS-leverancier moet UWV onmiddellijk op de hoogte stellen wanneer een opslaglimiet wordt overschreden en opties bieden om de gegevens in opslag te verminderen (bijvoorbeeld door middel van gegevensoverdracht). Als alternatief kan de leverancier UWV de mogelijkheid bieden om extra opslagruimte te verkrijgen/aan te schaffen binnen een onderhandeld tijdsbestek dat is vastgelegd in de servicevoorwaarden. De SaaS-leverancier moet UWV standaard ook waarschuwen, via meldingsprocessen die zijn gedefinieerd in de servicevoorwaarden, wanneer de opslaglimieten bijna worden overschreden. De drempel voor het verzenden van een melding moet door UWV kunnen worden gedefinieerd, of op zijn minst duidelijk zijn gedefinieerd door de SaaS-leverancier.	

3.9.7. Artikel 9g – Documentatie over locatie

9g.	**Documentatie over locatie**	*Vereist*
Criterium	De SaaS-leverancier voorziet UWV van geografische details rond de dienst en gegevensopslag, zoals de relatieve locaties (d.w.z. stad en land) van datacenters.	
Toelichting	Deze informatie is belangrijk voor de risicobepaling op basis van geografie, overheidscontrole, jurisdictie en rampenparaatheid. De politieke lijnen op een kaart maken een verschil in het begrijpen van welke overheidscontroles kunnen worden toegepast op de SaaS-leverancier en de gegevens die op specifieke fysieke locaties zijn opgeslagen. Van belang is ook welke jurisdictie van toepassing is. Weten waar een datacenter zich bevindt, helpt UWV ook risicobeoordelingen te maken op basis van de kans op natuurrampen. De regels rond onroerend goed zijn ook van belang voor het bepalen van de risico's. Conform cloudbeleid dient de dienst en gegevensopslag binnen de EER plaats te vinden.	

3.9.8. Artikel 9h – Dicteren van de locatie

9h.	**Dicteren van de locatie**	*Vereist*
Criterium	De SaaS-leverancier biedt de mogelijkheid om locaties van dataopslag te dicteren, af te dwingen.	
Toelichting	De SaaS-leverancier staat UWV toe om te dicteren in welke datacenters en/of regio's hun data wordt opgeslagen. De SaaS-leverancier biedt ook een garantie dat data niet willekeurig naar andere datacenters, regio's of locaties zal worden verplaatst. Dit omvat primaire (bron), gerepliceerde en geback-upte data.	

3.9.9. Artikel 9i – Documentatie over de infrastructuurdiensten

9i.	**Documentatie over de infrastructuurdiensten**	*Vereist*
Criterium	De SaaS-leverancier voorziet UWV van informatie over de infrastructuurdiensten die het afneemt voor de SaaS-dienst.	
Toelichting	Als de SaaS-leverancier geen eigen infrastructuur en platform bezit/exploiteert/verstrekt, maar gebruikmaakt van een IaaS/PaaS-leverancier of gecoloceerde/beheerde diensten, moet de SaaS-leverancier deze leverancier(s) bekendmaken. Hierdoor kan UWV de gehele waardeketen van dienstverlenende bedrijven inspecteren/auditen.	

3.9.10. Artikel 9j – Bulksgewijs fysiek importeren van gegevens

9j.	**Bulksgewijs fysiek importeren van gegevens**	*Gewenst*
Criterium	De SaaS-leverancier biedt een manier om grote hoeveelheden gegevens via fysieke bulkimport naar de dienst te migreren.	
Toelichting	Bulkgegevensimport is vaak nodig voor gegevensmigratie alvorens de dienst in gebruik kan worden genomen. Dit kan zowel digitaal als fysiek gefaciliteerd worden. Als digitaal niet gewenst is, is fysiek een alternatief.	

3.9.11. Artikel 9k – Documentatie over de architectuur

9k.	**Documentatie over de architectuur**	*Gewenst*
Criterium	De SaaS-leverancier stelt minimaal architectuurdiagrammen op hoog niveau beschikbaar, met informatie over protocollen, verbindingen, datastromen, HA/DR, beveiligingsdiensten, serverrollen en opslagomgevingen.	
Toelichting	Meer gedetailleerde informatie mag alleen beschikbaar worden gesteld onder een geheimhoudingsovereenkomst (NDA), en van de SaaS-dienst mag niet worden verwacht dat het eigendomsinformatie verstrekt die zijn dienst uniek maakt.	

3.9.12. Artikel 9l – Documentatie over prestatielimieten

9l.	**Documentatie over prestatielimieten**	*Gewenst*
Criterium	De SaaS-leverancier stelt documentatie beschikbaar over prestatie- en/of gebruikslimieten (per dienst, groep en/of gebruiker) voor het gebruik van gegevens binnen, het importeren van gegevens naar en het exporteren van gegevens uit de dienst.	
Toelichting	Deze documentatie moet, als deze limieten bestaan, de opgelegde harde limieten omvatten die UWV niet kan overschrijden, evenals zachte limieten die de dienst (stapsgewijs) beperken of limiteren om de algehele kwaliteit van de dienstverlening voor het bredere klantenbestand te behouden.	

3.9.13. Artikel 9m – Documentatie over opslag- en prestatieoptimalisatie

9m.	**Documentatie over opslag- en prestatieoptimalisatie**	*Gewenst*
Criterium	De SaaS-leverancier geeft gedocumenteerde richtlijnen om gebruik van de dienst te kunnen optimaliseren, kwaliteit te kunnen verbeteren en totale opslagverbruik te kunnen verminderen.	
Toelichting	De SaaS-leverancier heeft ook op zijn minst richtlijnen gepubliceerd met best-practices in het gebruik van de dienst.	

3.10. Artikel 10 – Netwerk

Voor het gebruik van een SaaS-dienst is netwerkverbinding (connectiviteit) nodig. Er zijn standaardoplossingen mogelijk (denk aan Azure ExpressRoute), maar worden niet altijd aangeboden en blijft het bij publiek internet. Bovendien kunnen er problemen ontstaan rond opschaling en prestaties.

Uiteindelijk is UWV (ICTS) eindverantwoordelijk voor connectiviteit en de SLA's richting (interne en externe) klanten en dient op dit gebied de netwerktechnologieën te evalueren die een SaaS-dienst gebruikt om de optimale prestaties van de SaaS-oplossing te garanderen.

3.10.1. Artikel 10a – Documentatie over netwerkinrichting

10a.	**Documentatie over netwerkinrichting**	*Vereist*
Criterium	De SaaS-leverancier documenteert de vereiste netwerkconfiguraties en -overwegingen voor de gebruikers van UWV die toegang krijgen tot de SaaS-oplossing.	
Toelichting	De documentatie bevat instructies voor de toegang tot de SaaS-oplossing via internet en via een privéverbinding. Het bevat ook gedetailleerde instructies voor het gebruik van een firewall. Dit omvat configuratie-instellingen zoals gespecificeerde poorten, IP-adresbereiken en verbindingen van wildcard-domeinnamen. De SaaS-leverancier kan bijvoorbeeld aangeven dat IP-adressen voor de dienst naar believen kunnen worden gewijzigd en dat de dienst daarom wildcard-naamruimten vereist. De minimaal vereiste bandbreedte, evenals de maximale latentie die wordt toegestaan om aanvaardbare prestaties te bereiken is goed gedocumenteerd. De documentatie omvat ook de netwerk- en internetconnectiviteitsarchitectuur voor de SaaS-oplossing per datacenter. Dit is van cruciaal belang voor UWV om te kunnen bepalen of de betrouwbaarheid, fail-over en bandbreedte voldoende zijn om aan de eisen te voldoen. Het biedt een maatstaf voor de levensvatbaarheid van de dienst in termen van de werkelijke werklast, en helpt UWV om samen te werken met de SaaS-leverancier wanneer niet aan de prestatieverwachtingen wordt voldaan. De leverancier verstrekt ook informatie over bandbreedte en latentie over datacenterlocaties en andersoortige relevante locaties.	

3.10.2. Artikel 10b – Documentatie over capaciteitsmanagement

10b.	**Documentatie over capaciteitsmanagement**	*Vereist*
Criterium	De SaaS-leverancier documenteert hoe het capaciteitsmanagement voor de dienst benadert.	
Toelichting		

3.10.3. Artikel 10c – Transparante geografische distributie

10c.	**Transparante geografische distributie**	*Vereist*
Criterium	De SaaS-leverancier host de dienst in geografisch verspreide datacenters, volledig transparant voor de afnemer (UWV).	
Toelichting	De SaaS-leverancier host oplossingen in geografisch verspreide datacenters die gegevens synchroniseren. Bovendien heeft de SaaS-oplossing routeringslogica die een gebruiker naar het dichtstbijzijnde datacenter leidt op basis van zijn of haar fysieke locatie. De SaaS-leverancier gebruikt deze connectiviteit ook voor HA- en DR-replicatie. Deze locaties zijn in overeenstemming met Artikel 9g – Documentatie over locatie en Artikel 9h – Dicteren van de locatie	

3.10.4. Artikel 10d – Samenwerking met cloud security brokers

10d.	**Samenwerking met cloud security brokers**	*Vereist*
Criterium	De SaaS-leverancier heeft aantoonbaar partnerships met een aantal toonaangevende cloud security leveranciers.	
Toelichting	Naarmate de SaaS-adoptie wordt opgeschaald, wordt geprobeerd beveiligings- of beleidstaken te centraliseren. Hierin kan een cloud security gateway of een cloud access security broker (CASB) een belangrijke rol in spelen als een manier om deze activiteiten te centraliseren. De SaaS-leverancier zorgt dat ze een partnerschap hebben met een aantal toonaangevende cloud security gateway- of CASB-providers om in deze behoefte te kunnen voorzien.	

3.10.5. Artikel 10e – Samenwerking met netwerk-leveranciers

10e.	**Samenwerking met netwerk-leveranciers**	*Gewenst*
Criterium	De SaaS-leverancier heeft een samenwerking met netwerk leveranciers die het mogelijk maken om direct, zonder tussenkomst van internet, te verbinden met de aangeboden dienst(en) om ervoor te zorgen dat UWV over uitstekende prestaties en betrouwbaarheid beschikt.	
Toelichting	Het internet is "by design" het meest onbetrouwbare netwerk ter wereld, moderne applicaties zijn ontwikkeld om hier zonder problemen mee om te gaan. Echter is het in specifieke gevallen wenselijk om zonder tussenkomst van internet direct te worden ontsloten op de aangeboden dienstverlening door tussenkomst van een netwerk leverancier. **Rationale:** • Deze directe ontsluiting zou van toepassing zijn op zowel gebruikers toegang, maar ook voor service integratie waardoor een hogere mate van beveiliging kan worden toegepast op gegevens uitwisseling tussen de SaaS-dienst en UWV informatie systemen door middel van API's (Application Programming Interface). • In geval van specifieke eisen ten aanzien van snelheid en/of latency is directe ontsluiting een vereiste. • De dienst dient zowel via het publieke internet als de directe ontsluiting mogelijk te zijn maar desgewenst beperkt kunnen worden. Nadelen: • Dure hardware; De besparing op de verbindingen wordt direct gecompenseerd door de dure hardware die nodig. Eigenlijk wordt het IT budget grotendeels verplaatst van de netwerkleverancier naar de hardwareleverancier. • Afhankelijkheid van leverancier; Bij SD-WAN wordt je single-point-of-failure de hardware (en software). Het netwerk wordt in de cloud van de leverancier geregeld. Is er daar een storing, kan je niks. Vergelijk het met een storing bij iDeal. Dan heb je alles goed geregeld, maar kan je niet betalen doordat er daar een storing is. Dit komt nog bovenop de storingen die toch af en toe in het netwerk voorkomen.	

3.10.6. Artikel 10f – Publicatie van netwerkprestaties

10f.	**Publicatie van netwerkprestaties**	*Gewenst*
Criterium	De SaaS-leverancier voert periodiek netwerkprestatie- en -latentietests uit van de dienst en deelt de resultaten met UWV.	
Toelichting	De SaaS-leverancier voert periodiek netwerkprestatie- en -latentietests uit van de dienst. De resultaten worden gedeeld met UWV of gepubliceerd via een whitepaper, bulletin of artikel. Het rapport bevat het testscenario, de gebruikte methodiek en de resultaten van de test. De tests moeten gemakkelijk herhaalbaar zijn voor afnemers als UWV en worden uitgevoerd voor elke fysieke locatie van de clouddienst en elke geografische locatie die wordt ondersteund voor toegang tot de dienst. Het rapport bevat ook algemene resultaten van ping- en traceroute-statistieken, zoals latentie. De tests en resultaten hebben tot doel om een baseline van prestatieverwachtingen vast te leggen, ook als onderdeel van een keten. Baselines helpen bij het voorspellen en oplossen van problemen tijdens het gebruik van de dienst.	

3.10.7. Artikel 10g – Ondersteuning directe netwerkverbindingen

10g.	**Ondersteuning directe netwerkverbindingen**	*Gewenst*
Criterium	De SaaS-leverancier ondersteunt (directe) netwerkverbindingen anders dan internet.	
Toelichting	Een directe verbinding tussen een on-premises datacenter (DXC) en een SaaS-leverancier om het internet te omzeilen kan gewenst zijn vanwege veiligheid of betrouwbaarheid. UWV verwacht niet dat de SaaS-leverancier een ‘as-a-service’-aanbod heeft voor dergelijke verbindingen, maar zou deze wanneer gewenst moeten ondersteunen en met UWV meedenken over hoe de verbinding tot stand kan worden gebracht om aan de zakelijke vereisten te voldoen. Voorbeelden van verbindingen zijn dark fiber, dedicated circuits en huurlijnen. De verbindingen moeten multiprotocol label-switching (MPLS) ondersteunen voor gegevensoverdracht.	

3.10.8. Artikel 10h – Real-time monitoring netwerkprestatie

10h.	**Real-time montoring netwerkprestatie**	*Gewenst*
Criterium	De SaaS-leverancier heeft een real-time prestatiemonitoringservice waar UWV toegang tot heeft om de netwerkprestaties van de dienst te kunnen beoordelen.	
Toelichting	UWV heeft toegang nodig tot real-time prestatiemonitoringdiensten van de SaaS-leverancier, zodat het snel en eenvoudig kan begrijpen of de dienst goed of slecht bereikbaar is en welk effect het heeft op de keten. Een monitoringsysteem is de gemakkelijkste manier om deze taak te volbrengen (ook als onderdeel van bredere ketenmonitoring). Deze real-time prestatiemonitoringservice moet toegankelijk zijn via een service-interface of de beheerconsole en moet voorkomen dat UWV haar eigen prestatiemonitoring en/of integratiepunten moet bouwen. De volgende netwerkprestatiegegevens moeten deel uitmaken van de standaardservice en moeten worden gerapporteerd in intervallen van vijf minuten of minder: • Latentie tussen internetpunten en dienst vanuit elk van de geografische gebieden die worden ondersteund door de SaaS-oplossing. • Doorvoer (throughput) tussen internetpunten en dienst vanuit elk van de geografische gebieden die worden ondersteund door de SaaS-oplossing. • Een geschiedenis van minimaal 60 dagen van latentie en doorvoer tussen internetpunten en dienst vanuit elk van de geografische gebieden die worden ondersteund door de SaaS-oplossing, minimaal op uurbasis geregistreerd.	

3.10.9. Artikel 10i – Optimalisatie netwerkprestatie

10i.	**Optimalisatie netwerkprestatie**	*Gewenst*
Criterium	De SaaS-leverancier ondersteunt methoden en technieken voor optimalisatie van netwerkprestatie.	
Toelichting	De SaaS-leverancier past methode en technieken toe om netwerkprestaties te kunnen optimaliseren, zoals: • Samenwerking aangaan met leveranciers van WAN-optimalisatiediensten in geval van hoge latentie. De SaaS-leverancier zou partnerschappen moeten hebben met aanbieders van WAN-optimalisatie (zoals Aryaka of Riverbed) om UWV de mogelijkheid te bieden WAN-optimalisatie toe te passen met SaaS-oplossingen. • Verbeterde samenwerking op het gebied van internetdiensten. De SaaS-leverancier moet samenwerken met overlay-prestatiegebaseerde routeringsmechanismen via internet, zoals Teridion. Deze moeten de verouderde BGP-internetroutering omzeilen. • Verbeterde gedistribueerde internetaanwezigheid. De SaaS-leveranciers moeten hun internetaanwezigheid uitbreiden, met behulp van technieken zoals het publiceren van een op internet gebaseerd IP-anycast-adres en het mogelijk maken van cold-potato-routering, zodat eindgebruikers een verbeterd, geoptimaliseerd netwerk dichtbij hun locatie kunnen betreden en verlaten.	

3.11. Artikel 11 – Financiën

UWV dient inzicht te hebben over prijsstelling en facturering van SaaS-oplossingen. Dit is niet alleen het domein van Inkoop en Leveranciersmanagment, maar ook van IT (of Enterprise Architectuur) dat een relatie moeten leggen tussen te gebruiken (technische) componenten en verwachte kosten. Vaak zijn deze partijen vertegenwoordigd in een FinOps-team.

3.11.1. Artikel 11a – Variabele contracttermijnen

11a.	**Variabele contracttermijnen**	*Vereist*
Criterium	De SaaS-leverancier biedt een variabele lengte van contractvoorwaarden en aankoopopties aan, zoals jaarlijks of meerjarig.	
Toelichting	Het hebben van verschillende keuzes voor de lengte van de contractvoorwaarden biedt UWV flexibiliteit bij het gebruik van de SaaS-oplossing.	

3.11.2. Artikel 11b – Duidelijke beschrijving van de dienst

11b.	**Duidelijke beschrijving van de dienst**	*Vereist*
Criterium	De SaaS-leverancier definieert duidelijk wat is inbegrepen en uitgesloten van de dienst.	
Toelichting	De SaaS-leverancier geeft een duidelijke definitie van welke functies en functionaliteit de dienst biedt, evenals eventuele afhankelijkheden die de dienst kan hebben van componenten die naar verwachting door UWV zullen worden geleverd. Een SaaS-oplossing kan bijvoorbeeld een desktopclient ondersteunen die wordt geleverd door en onder de verantwoordelijkheid valt van UWV.	

3.11.3. Artikel 11c – Verscheidenheid aan prijs- en verpakkingsopties

11d.	**Verscheidenheid aan prijs- en verpakkingsopties**	*Vereist*
Criterium	De SaaS-leverancier biedt een verscheidenheid aan prijs- en verpakkingsopties voor hun dienst aan om UWV de flexibiliteit te geven om met die dienst aan de slag te gaan op basis van geïdentificeerde behoeften en segmentatie.	
Toelichting	Een belangrijke aantrekkingskracht van een SaaS-oplossing is de flexibiliteit die ze organisaties als UWV bieden om gebruikers te segmenteren op basis van verschillende factoren, zoals taakverantwoordelijkheid, status, divisie, locatie of functie. De hoeveelheid en verscheidenheid aan prijzen en verpakkingen zal per SaaS-oplossing variëren, maar een SaaS-leverancier biedt op zijn minst verschillende opties aan, gebaseerd op het niveau van functionaliteit dat moet worden geleverd en de ondersteuning die aan UWV moet worden geleverd. Voorbeelden hiervan zijn aanbiedingen voor hoofdgebruikers, kiosk-/light-gebruikers, standaardgebruikers, multi-tenant-service, speciale service, service voor een specifieke gemeenschap (bijvoorbeeld de federale overheid of hoger onderwijs), hogere garantie voor uptime of snellere ondersteuning.	

3.11.4. Artikel 11d – Tijdige melding van wijzigingen in features

11d.	**Tijdige melding van wijzigingen in features**	*Vereist*
Criterium	De SaaS-leverancier maakt tijdig melding van wijzigingen in features en daarmee verbonden kosten.	
Toelichting	De SaaS-leverancier levert een roadmap van zes maanden aan – eventueel onder een NDA – die de timing en mogelijkheden van nieuwe features aangeeft en maandelijks wordt bijgewerkt. Dit geldt ook voor grote wijzgingen in of uitfaseren van features. Verwachte prijswijzigingen of aanvullende opties worden ook gecommuniceerd. UWV wordt minimaal drie maanden van te voren op de hoogte gesteld wanneer een gewijzigde (nieuwe of uitfaserende) functie moet worden geadopteerd, en krijgt een respijt van zes maanden voordat extra kosten moet worden betaald voor de nieuwe of gewijzigde functie.	

3.11.5. Artikel 11e – Bescherming tegen toenemende en aanvullende kosten

11e.	**Bescherming tegen toenemende en aanvullende kosten**	*Vereist*
Criterium	De SaaS-leverancier heeft in haar contractvoorwaarden clausules opgenomen dat UWV beschermd tegen oplopende (reguliere) verlengingskosten en meerkosten voor aanvullende behoeften.	
Toelichting	De SaaS-leverancier neemt een clausule in het contract op dat UWV in staat stelt de verlengingsprijs te beperken ('renewal price protection'). Idealiter is de verhogingslimiet voor verlenging een eenmalige verhoging op de verlengingsdatum en niet een jaarlijkse verhoging, die is vastgesteld op maximaal 3 tot 5%, of de consumentenprijsindex (CPI), afhankelijk van welke waarde lager is. Over het algemeen bieden grotere SaaS-leveranciers vaste prijzen voor de initiële looptijd van het contract, terwijl kleinere aanbieders een jaarlijkse verhoging in een meerjarige overeenkomst kunnen opnemen. Bij contracten met jaarlijkse verhogingen is een limiet die lager is dan 3% of CPI geschikter. Een SaaS-leverancier neemt ook een clausule op die de prijs vastlegt die wordt betaald voor extra behoeften (zoals opslagruimte of aantal gebruikers). Gartner's Top 10 SaaS-voorwaarden om te onderhandelen die financiële en continuïteitsrisico's te voorkomen: 1. Onderhandel over een verlengingsprijslimiet om ervoor te zorgen dat de kosten van het SaaS-contract binnen het budget blijven. 2. Identificeer en onderhandel proactief over eventuele 'verborgen' kosten die van toepassing kunnen zijn op de SaaS-deal. 3. Onderhandel over flexibiliteit in het prijsmodel en de contractvoorwaarden, zodat deze aansluiten bij de behoefte ('demand', gevraagde capaciteit). 4. Neem gedetailleerde servicebeschrijvingen voor alle producten op in het SaaS-contract, zodat alle beperkingen duidelijk worden gedocumenteerd. 5. Onderzoek en neem andere belangrijke referentiedocumenten (vaak een URL-verwijzing) expliciet (kopie) op in het SaaS-contract om 'sluipende' afname in ondersteuning, functionaliteit en beveiligingsnormen te beperken of te voorkomen. 6. Lees de voorwaarden met betrekking tot beveiliging en gegevensprivacy grondig door om ervoor te zorgen dat aan de vereisten wordt voldaan. 7. Zorg ervoor dat de SaaS-leverancier de verantwoordelijkheid neemt voor zijn onderaannemers. 8. Neem belangrijke serviceniveaus en passende oplossingen als het een kritieke SaaS-applicatie of feature betreft. 9. Ga er niet van uit dat gegevens zonder onderhandelingen gemakkelijk of gratis te extraheren zijn wanneer je ze nodig heeft (in de operatie of bij een exit). 10. Onderhandel over hulp bij de migratie en toekomstige uitbreidingen van de dienst.	

3.11.6. Artikel 11f – Inzicht in de kosten op basis van gebruik

11f.	**Inzicht in de kosten op basis van gebruik**	*Vereist*
Criterium	De SaaS-leverancier geeft UWV inzicht via een selfservice-interface in de kosten (op basis van gebruik of licentie).	
Toelichting	Of de SaaS-oplossing nu in rekening wordt gebracht op basis van gebruik of abonnement (bijvoorbeeld per gebruiker per jaar), UWV kan via een selfservice-interface inzicht verkrijgen in gebruikers, welke componenten van de dienst ze gebruiken en hoeveel ze het gebruiken. Dit helpt UWV de ROI voor de dienst te identificeren en wijzigingen of aanpassingen aan de aankoop van de dienst te rechtvaardigen (zoals het vragen om volumekortingen of het toevoegen of verwijderen van componenten/features van de dienst). Als UWV uit gebruiksrapporten kan opmaken welke gebruikers de dienst gebruiken en welke niet, kan zij de licentieverlening voor de dienst dienovereenkomstig aanpassen. Daarnaast verstrekt de SaaS-leverancier ook details over verborgen kosten, zoals ondersteuning op een hoger niveau, opslag, sandboxes, taalpakketten, bandbreedte, back-up, API-verzoeken en kosten voor encryptie, waardoor de kosten aanzienlijk kunnen stijgen of hoger uitvallen.	

3.11.7. Artikel 11g – Verschillende vormen van betaling

11g.	**Verschillende vormen van betaling**	*Gewenst*
Criterium	De SaaS-leverancier biedt verscheidene vormen van betaling aan.	
Toelichting	De SaaS-leverancier ondersteunt de mogelijkheid om meerdere betalingsvormen aan te bieden, zoals betaling per creditcard of het sturen van een factuur naar crediteuren. De SaaS-leverancier biedt creditcardfacturering en een andere vorm van zakelijke facturering, zoals een inkooporder of factuur, kunnen aanbieden. De SaaS-leverancier kan bepaalde beperkingen stellen aan facturering, zoals een maximale doorlooptijd om de factuur te betalen. De SaaS-leverancier biedt echter minimaal 30 dagen aan voor de juiste afhandeling van de betaling van bedrijfsfacturen. UWV is een complexe organisatie en dient voldoende tijd te hebben om transacties via haar systemen te verwerken.	

3.11.8. Artikel 11h – Kortingen bij langlopende contracten of grootschalige inzet

11h.	**Kortingen bij langlopende contracten of grootschalige inzet**	*Gewenst*
Criterium	De SaaS-leverancier biedt kortingen aan bij langlopende contracten (van langer dan een jaar) en grootschalige inzet van meer dan 5.000 gebruikerslicenties of een andere meeteenheid.	
Toelichting	Kortingen op grootschalige implementaties nemen toe naarmate de omvang van de implementatie toeneemt. Dit komt door de schaalvoordelen die de SaaS-leverancier kan herkennen. De leverancier geeft een deel van deze besparingen door aan UWV. De kortingen zijn geadverteerd en consistent. Deze kortingen zal UWV helpen de kosten versus de voordelen af te wegen bij het segmenteren van de gebruikers (in gebruikersgroepen) voor de dienst. Een voldoende korting kan UWV er bijvoorbeeld van overtuigen om nog een segment toe te voegen en het aantal gebruikers van een dienst te vergroten, met dien verstande dat er mogelijk aanpassingen nodig zijn om tegemoet te komen aan de gebruikersvereisten van het toegevoegde segment.	

3.11.9. Artikel 11i – Op-consumptie-gebaseerde prijsoptie

11i.	**Op-consumptie-gebaseerde prijsoptie**	*Gewenst*
Criterium	De SaaS-leverancier biedt een op-consumptie-gebaseerd prijsmodel aan voor gebruik dat niet voorspelbaar of betrouwbaar is.	
Toelichting	Dit is niet een prijsmodel dat alle SaaS-leveranciers op dit moment aanbieden. Organisaties vragen echter steeds vaker naar deze optie wanneer het geschatte gebruik van de SaaS-oplossing lastig te bepalen is.	

3.11.10. Artikel 11j – Gedetailleerde factureringS- en rapportagemogelijkheden

11j.	**Gedetailleerde factureringS- en rapportagemogelijkheden**	*Gewenst*
Criterium	De SaaS-leverancier biedt zelfbedienings- of geautomatiseerde, gedetailleerde factureringS- en rapportagemogelijkheden aan.	
Toelichting	UWV heeft hulp nodig die verder gaat dan geconsolideerde facturen. UWV wil het gebruik van een SaaS-oplossing in kaart brengen op basis van aangepaste asset- of meta-datatags die door UWV zijn gedefinieerd. Een voorbeeld hiervan is het toewijzen van een meta-datatag voor een afdelingscode of kostenplaats aan elke gebruiker in de service. Op het moment van facturering dient UWV de exacte licentie en gebruik (indien van toepassing, bijvoorbeeld wanneer de kosten worden berekend op basis van gebruik) per code kunnen zien. Dit helpt UWV om gebruik door te belasten (middels een terugboekingssysteem) naar interne bedrijfseenheden (b.v. devops teams). Bedrijven segmenteren gebruikers in hun omgevingen vaak op basis van een verscheidenheid aan kenmerken (bijvoorbeeld locatie, functieverantwoordelijkheid of organisatiestructuur). Dankzij gedetailleerde facturering en rapportage krijgt de onderneming een beter inzicht in de manier waarop verschillende segmenten de SaaS-oplossing gebruiken en de bijbehorende kosten. UWV zit hier niet anders in.	

3.11.11. Artikel 11k – Proactief aanbevelen van kostenbesparingen

11k.	**Proactief aanbevelen van kostenbesparingen**	*Gewenst*
Criterium	De SaaS-leverancier beveelt op een proactieve wijze licentiewijzigingen en verbeterde eenheidsprijzen aan op basis van het gebruik van de dienst ten behoeven van kostenoptimalisatie.	
Toelichting	De SaaS-leverancier biedt aanbevelingen voor het afstemmen van de kosten voor de dienst op basis van het daadwerkelijke gebruik van de dienst door UWV. De dienst zou bijvoorbeeld moeten kunnen rapporteren: "gebruiker A heeft een volledige licentie, maar gebruikt alleen functies die onder de basislicentie vallen. Daarom zou je ze in de toekomst moeten overzetten naar een basislicentie." Dit is een standaardmogelijkheid, zodat het UWV de mogelijkheid geeft te betalen voor wat het gebruikt en niet meer. Hoewel een standaard abonnementstarief per gebruiker per jaar misschien gemakkelijk aan te schaffen en te begrijpen is, is de optie om dat model af te stemmen op basis van gebruik aantrekkelijk.	

3.11.12. Artikel 11l – Betalingspauzes en flexibele betalingsfrequentieopties

11l.	**Betalingspauzes en flexibele betalingsfrequentieopties**	*Gewenst*
Criterium	De SaaS-leverancier neemt een clausule in het contract op dat niet hoeft te worden betaald voor functies die gedurende een periode niet worden gebruikt.	
Toelichting	Afnemers van een SaaS-dienst worden vaak gefactureerd voor bestaande of geplande modules of functies, ook al worden deze gedurende een bepaalde periode binnen de abonnementstermijn niet gebruikt. De SaaS-leverancier zou een 'Payment Holiday'-clausule in het contract moeten opnemen, waardoor UWV niet in rekening kan worden gebracht voor specifieke functies die gedurende een afgesproken periode niet worden gebruikt. Daarnaast neemt de SaaS-leverancier ook voorwaarden op in het SaaS-contract die UWV flexibele betalingscyclusopties biedt, zoals maandelijkse of driemaandelijkse betalingsfrequenties, evenals uitgestelde betalingsopties in tijden van crisis.	

3.11.13. Artikel 11m – ROI-calculators

11m.	**ROI-calculators**	*Optioneel*
Criterium	De SaaS-leverancier biedt ROI-calculators of tools die helpen de kosten van de SaaS-oplossing te beoordelen in vergelijking met het bouwen of implementeren van een dienst via een on-premises model.	
Toelichting	Eén van de belangrijkste aantrekkingskrachten van SaaS-oplossingen – maar soms ook een aanzienlijke teleurstelling – is het potentieel voor kostenbesparingen. De mogelijkheid om geld te besparen is een belangrijke drijfveer voor de adoptie van SaaS-oplossingen. UWV heeft hulp nodig om die kans te begrijpen. De SaaS-leverancier helpt UWV door ROI-calculators of tools aan te bieden die helpen de kosten van de SaaS-oplossing te beoordelen in vergelijking met het bouwen of implementeren van een dienst via een on-premises model. Zoals bij elk hulpmiddel van deze aard moet de rekenmachine van de SaaS-leverancier duidelijk zijn over wat hij berekent en de gebruiker opties bieden om de berekeningen aan te passen voor specifieke omstandigheden. Het verschil tussen dit criterium en het kostencalculatorcriterium is dat een ROI-tool de besparingen berekent door gebruik te maken van de gegevens uit de kostencalculator en aanvullende gegevens over de infrastructuur-, beheer- en applicatiebesparingen binnen de klantomgeving.	

3.11.14. Artikel 11n – Accounts geconsolideerd in één factuur

11n.	**Accounts geconsolideerd in één factuur**	*Optioneel*
Criterium	De SaaS-leverancier biedt de mogelijkheid om meerdere accounts te consolideren in één factuur/factuur.	
Toelichting	De SaaS-leverancier stelt UWV in staat om facturen die zijn aangevraagd bij accounts te consolideren in één enkele factuur. Vanwege de beperkingen op het gebied van accountbeheer die bij sommige leveranciers gelden, moeten klanten mogelijk meerdere, afzonderlijke gebruikersaccounts bij die leveranciers aanmaken. Als dit gebeurt, staat de SaaS-leverancier UWV toe één enkele factuur te ontvangen voor het gehele verbruik voor alle SaaS-accounts.	

3.12. Artikel 12 – Dienstverlening

Hoofddoel van een SLA of servicecontract met een SaaS-leverancier zou het definiëren van transparantie moeten zijn, zodat UWV (IV) de dienst kan beheren. Voor SaaS-oplossingen moeten SLA's zeer helder zijn op het gebied van beschikbaarheid, herstel, prestaties, RTO en RPO.

Hoe snel moet een SaaS-leverancier UWV op de hoogte stellen van een storing? Welk escalatiepad is beschikbaar? Hoe moet de SaaS-leverancier UWV op de hoogte stellen? Wat stelt UWV aan eisen op het gebied van beschikbaarheid, herstel, prestaties, RTO en RPO? Deze kunnen per SaaS-dienst variëren.

De criteria in dit gedeelte omvatten niet alle criteria die UWV moet nastreven voor serviceniveaus en SLA's. De juridische, inkoop- en business teams zullen aanvullende criteria hebben, zoals contractvoorwaarden, geschillenprocessen, financiële beoordelingen, escrow-opties en boetes. De volgende criteria zijn gericht op IT-implementatie en bemiddeling van een SaaS-oplossing.

3.12.1. Artikel 12a – Definitie van downtime

12a.	**Definitie van downtime**	*Vereist*
Criterium	De SaaS-leverancier hanteert een definitie van downtime die begint wanneer de dienst niet beschikbaar of verslechterd is en communiceert deze met UWV.	
Toelichting	UWV geeft de voorkeur aan dat de downtimeberekeningen onmiddellijk beginnen wanneer de downtime begint. Clausules die specificeren dat storingen langer dan vijf, tien of vijftien minuten moeten duren om in aanmerking te komen voor SLA's, communiceren de verkeerde boodschap naar UWV en afnemers in het algemeen. Voor sommige kritieke of transactionele applicaties kan zelfs de kortste uitval grote gevolgen hebben voor UWV. Daarom hanteert zowel UWV als de SaaS-leverancier de definitie van downtime wanneer de dienst niet meer beschikbaar of verslechterd is. UWV moet er rekening mee houden dat geplande onderhoudsuitval met de juiste kennisgeving te verwachten is in SaaS-oplossingen, en dat deze doorgaans niet wordt meegenomen in de berekening van boetes zoals ongeplande downtime door de SaaS-leverancier. Als dit voor UWV onaanvaardbaar is voor de SaaS-oplossing die wordt geëvalueerd, zou het criterium van 'geen uitzonderingen op downtime' in de SLA moeten worden vereist.	

3.12.2. Artikel 12b – Gepland onderhoud wordt vooraf gecommuniceerd

12b.	**Gepland onderhoud wordt vooral gecommuniceerd**	*Vereist*
Criterium	De SaaS-leverancier levert voor elke maand een actueel onderhoudsschema aan.	
Toelichting	Beperkt gepland, maandelijks onderhoud wordt vooraf gecommuniceerd. De SaaS-leverancier levert voor elke maand een actueel onderhoudsschema aan. Het maandelijkse schema communiceert een consistent onderhoudsplan, zoals 'Elke zaterdag van 02.00 uur tot 04.00 uur EST'. De SaaS-leverancier stelt UWV uiterlijk 72 uur vóór de planningswijziging op de hoogte van eventuele wijzigingen in gepland onderhoud.	

3.12.3. Artikel 12c – Meldingen betreffende noodonderhoud

12c.	**Meldingen betreffende noodonderhoud**	*Vereist*
Criterium	De SaaS-leverancier stelt UWV vooraf op de hoogte van noodonderhoudswerkzaamheden die nodig zijn om onvoorziene dienstonderbrekingen (beveiliging, netwerk enz.) aan te pakken.	
Toelichting	De SaaS-leverancier stelt UWV over het algemeen 24 tot 48 uur vóór de onderhoudsprocedure op de hoogte. Bovendien zijn de meldingsprocessen voor noodonderhoud duidelijk vermeld in SLA's.	

3.12.4. Artikel 12d – Garantie van 99,7% uptime

12d.	**Garantie van 99,7% uptime**	*Vereist*
Criterium	De SaaS-leverancier garandeert een uptime van de SaaS-oplossing van minimaal 99,7%, gemeten op maandbasis (30 dagen rollend).	
Toelichting	Dit is een minimale eis, inclusief servicewindows. Gegeven de ***B***IV kan deze hoger liggen conform beleid hierop. Mocht de eis tijdens de operatie niet gehaald worden, kan gekozen voor een penalty of uiteindelijk een exit.	

3.12.5. Artikel 12e – Bescherming tegen dataverlies en -integriteitsproblemen

12e.	**Bescherming tegen dataverlies en -integriteitsproblemen**	*Vereist*
Criterium	De SaaS-leverancier heeft een gedefinieerde SLA waarin hun verantwoordelijkheid wordt beschreven om niet bij te dragen aan dataverlies of data-integriteitsproblemen met door UWV opgeslagen data.	
Toelichting	De SaaS-leverancier definieert de voorwaarden van deze SLA verder, inclusief boetes en/of verhaalmogelijkheden. UWV kan per ongeluk eigen gegevens verwijderen, maar SaaS-leveranciers mogen nooit deze gegevens kwijtraken en moeten in de SLA opnemen dit te ondersteunen.	

3.12.6. Artikel 12f – RTO en RPO gedefinieerd

12f.	**RTO en RPO gedefinieerd**	*Vereist*
Criterium	De SaaS-leverancier heeft RTO en RPO gedefinieerd voor de dienst.	
Toelichting	De SaaS-provider heeft de definitie voor RTO (Recovery Time Objective: maximale toegestane downtime na een onverwachte gebeurtenis, oftewel hoelang het maximaal mag duren, om de belangrijkste systemen weer op de been te krijgen na een storing of andere calamiteit) en RPO (Recovery Point Objective: maximaal toegestane tijd dat data is verloren, oftewel hoeveel data maximaal kan worden gemist zonder dat dit heftige gevolgen heeft; dit cijfer geeft dus aan hoe vaak er back-ups gemaakt moeten worden) voor de dienst opgenomen in de SLA, inclusief in het geval van disaster recovery. Hoewel deze afhankelijk van de dienst aanzienlijk kunnen variëren, moeten ze over het algemeen in minuten en uren worden uitgedrukt. Elke RTO of RPO langer dan 24 uur is verdacht voor de meeste SaaS-oplossingen.	

3.12.7. Artikel 12g – Servicekredieten/restituties voor storingen

12g.	**Servicekredieten/restituties voor storingen**	*Vereist*
Criterium	De SaaS-leverancier biedt servicekredieten of restituties aan die gelijk zijn aan of groter zijn dan de kosten die zijn gemaakt voor niet-beschikbare services tijdens de periode van een storing.	
Toelichting	Als de dienst bijvoorbeeld vijf uur niet beschikbaar is, moet de klant minimaal een tegoed voor de abonnementskosten voor die vijf uur ontvangen. Gedeeltelijke servicekredieten, zoals 5% van de maandelijkse factuur, zijn variabel en weerspiegelen niet noodzakelijkerwijs de kosten van de storing. Omdat een tegoed of terugbetaling gelijk is aan de kosten die tijdens een storing zijn ontstaan, mag de SaaS-leverancier bovendien geen maximale limieten opleggen aan financiële boetes. Klanten mogen niet betalen voor diensten die niet worden geleverd. Als een SaaS-leverancier 48 uur lang een storing zou hebben gehad, maar de financiële boetes zou beperken tot 24 uur verloren service, zou UWV betalen voor diensten die hij niet heeft ontvangen. Een andere acceptabele optie zou zijn dat de SaaS-leverancier de facturering opschort tijdens een storing.	

3.12.8. Artikel 12h – Meldingsvenster voor een SLA-claim

12h.	**Meldingsvenster voor een SLA-claim**	*Vereist*
Criterium	De SaaS-leverancier gunt twee factureringscycli de tijd om een claim in te dienen na een gemiste SLA.	
Toelichting	Het meldingsvenster voor UWV om een SLA-misclaim in te dienen is gelijk aan of groter dan twee factureringscycli. UWV heeft een ingewikkelde organisatiestructuur, waaronder debiteuren/crediteuren, inkoop, bedrijfsvoering en architectuur. UWV heeft minimaal twee factureringscycli nodig om SLA-misclaims in te dienen bij een SaaS-leverancier.	

3.12.9. Artikel 12i – Eigendomsrechten op gegevens, inputs en outputs

12i.	**Eigendomsrechten op gegevens, inputs en outputs**	*Vereist*
Criterium	De SaaS-leverancier erkent dat alle eigendomsrechten op gegevens, inputs en outputs bij UWV blijven en handelt daarnaar.	
Toelichting	SaaS-leveranciers leveren vaak diensten aan organisaties die deze services kunnen gebruiken om intellectueel eigendom te genereren dat grote hoeveelheden geld waard is. Hoewel de SaaS-leverancier de rechten op de dienst en de fysieke infrastructuur bezit, moeten de voorwaarden van de dienst en de overeenkomsten specificeren dat de eigendomsrechten op alle gegevens, inputs en outputs van het gebruik van de service door UWV behouden blijven.	

3.12.10. Artikel 12j – Prestatie-, probleemoplossing-, verzoek- en auditstatistieken

12j.	**Prestatie-, probleemoplossing-, verzoek- en auditstatistieken**	*Vereist*
Criterium	De SaaS-leverancier neemt in de SLA statistieken op betreffende prestaties, probleemoplossing, verzoeken en audits.	
Toelichting	Naast beschikbaarheids-, RTO- en RPO-statistieken bevat de SLA ook statistieken voor prestaties, probleemoplossing, verzoeken en audits. Deze statistieken variëren afhankelijk van de SaaS-oplossing, maar de leverancier heeft op zijn minst een SLA met gedocumenteerde statistieken. Prestatiestatistieken kunnen een grote verscheidenheid aan statistieken omvatten, maar over het algemeen moeten ze gekoppeld zijn aan statistieken die een positieve gebruikerservaring meten, zoals de responstijd voor de service. Ondersteuning voor de service is van cruciaal belang (zoals beschreven in 3.13). Daarom maakt een SLA voor het oplossen van problemen en het behandelen van verzoeken van UWV deel uit van de overeenkomst. Ten slotte bevat de overeenkomst ook meetgegevens voor het uitvoeren van regelmatige audits zoals vereist door de UWV en/of aangeboden door de SaaS-leverancier.	

3.12.11. Artikel 12k – Escalatie als niet aan de SLA wordt voldaan

12k.	**Escalatie als niet aan de SLA wordt voldaan**	*Vereist*
Criterium	De SaaS-leverancier beschikt over een gedocumenteerde procedure om te escaleren, de hoofdoorzaak te bepalen en het probleem aan te pakken dat de oorzaak was van het niet voldoen aan de SLA.	
Toelichting	Wanneer niet aan de SLA wordt voldaan, is het niet voldoende dat de SaaS-leverancier servicekredieten of restituties aanbiedt. De SaaS-leverancier beschikt ook over een gedocumenteerde procedure om te escaleren, de hoofdoorzaak te bepalen en het probleem aan te pakken dat de oorzaak was van het niet voldoen aan de SLA. UWV heeft inzicht nodig in de procedure en de resultaten om er zeker van te zijn dat het probleem op de juiste manier is aangepakt en dat het onwaarschijnlijk is dat dit zich opnieuw zal voordoen.	

3.12.12. Artikel 12l – Vooraf melden van SLA-wijzigingen

12l.	**Vooraf melden van SLA-wijzigingen**	*Vereist*
Criterium	De SaaS-leverancier stelt minstens 90 dagen van tevoren UWV op de hoogte van SLA-wijzigingen.	
Toelichting	Na verloop van tijd zullen er wijzigingen worden aangebracht in de SLA's voor een SaaS-oplossing; dit is een feit van innovatie en evolutie. Voor een SLA-wijziging in taal, uitsluitingen, voorwaarden of metingen moet de SaaS-leverancier dit minimaal 90 dagen van tevoren melden voordat deze de wijziging doorvoert. UWV heeft voldoende tijd nodig om een verandering te evalueren en de eventuele impact op de dienstverlening en financiële verplichtingen met de SaaS-leverancier te beoordelen. De SaaS-leverancier definieert de SLA-wijzigingskennisgeving in de servicevoorwaarden als gedrag waaraan de SaaS-leverancier zich zal houden bij elke SLA-wijziging.	

3.12.13. Artikel 12m – Voorwaarden voor niet-vermindering

12m.	**Voorwaarden voor niet-vermindering**	*Vereist*
Criterium	De SaaS-leverancier neemt in de SLA niet-verminderingsclausules op om downgrades van de dienst of specifieke features door toekomstige updates tijdens de licentieperiode te voorkomen.	
Toelichting	De SaaS-leverancier deelt gedetailleerde beschrijvingen van alle actieve scenario's van de dienst. Niet-verminderingsclausules worden opgenomen in de SLA om downgrades van features door toekomstige updates tijdens de licentieperiode te voorkomen. Bovendien worden kleine upgrades in toekomstige versies of patches van de dienst over het algemeen gratis geleverd en zijn de bijbehorende voorwaarden opgenomen in de SLA.	

3.12.14. Artikel 12n – Openbaar toegankelijke en downloadbare servicevoorwaarden

12n.	**Openbaar toegankelijke en downloadbare servicevoorwaarden**	*Vereist*
Criterium	De SaaS-leverancier biedt de mogelijkheid om de servicevoorwaarden te downloaden via een link of bijlage.	
Toelichting	Licentieovereenkomsten voor eindgebruikers (EULA's) of servicevoorwaarden (TOS – Terms of Service) zijn bindende juridischx`xe overeenkomsten waar UWV doorheen klikt om een nieuwe clouddienst te starten. Niet alle leveranciers bieden hun service aan met een doorklikovereenkomst, maar voor degenen die dat wel doen, eist UWV dat de TOS-overeenkomst openbaar toegankelijk en downloadbaar is voor verdere beoordeling.	

3.12.15. Artikel 12o – Beëindiging bij aanhoudende SLA-schendingen

12o.	**Beëindiging bij aanhoudende SLA-schendingen**	*Vereist*
Criterium	De SaaS-leverancier biedt een optie waarmee licenties kunnen worden beëindigd bij aanhoudende storingen.	
Toelichting	Afgezien van een kritieke misser van het beschikbaarheidsdoel (zoals een beschikbaarheidspercentage van 95% in één maand), worden gebeurtenissen zoals drie SLA-schendingen in een periode van twaalf maanden of SLA-schendingen in drie opeenvolgende maanden doorgaans geclassificeerd als aanhoudende fouten. Idealiter zou het recht om de overeenkomst te beëindigen wegens aanhoudend slechte prestaties niet in de tijd beperkt moeten zijn. Zodra de gedefinieerde beëindigingsgebeurtenis heeft plaatsgevonden, moet de mogelijkheid tot beëindiging blijven bestaan voor de rest van de licentietermijn.	

3.12.16. Artikel 12p – Algemene voorwaarden gekoppeld aan de SLA

12p.	**Algemene voorwaarden gekoppeld aan de SLA**	*Vereist*
Criterium	De SaaS-leverancier heeft de algemene voorwaarden in het contract gekoppeld aan de SLA.	
Toelichting	UWV zorgt ervoor dat de SaaS-leverancier de algemene voorwaarden van het contract heeft gekoppeld aan de SLA-clausules die zijn gespecificeerd (met name de vereiste criteria vermeld in dit document). Dit helpt UWV juridische en operationele verhaalmogelijkheden te bieden (bijvoorbeeld het beëindigen van de dienst en het beëindigen van het contract zonder boete) als niet aan de SLA niet wordt voldaan. De SaaS-Leverancier accepteert bij voorkeur de gehanteerde ICT en/of SaaS-voorwaarden van UWV. In het geval UWV hiervan afwijkt, zorgt de verantwoordelijke van UWV (op advies van JZ) dat de aanpassingen /alternatieven voldoen aan het volgende: 1) SaaS diensten/producten/oplossingen worden uitsluitend op basis van een formele overeenkomst conform UWV beleid verkregen en vastgelegd. 2) De contractuele afspraken houden rekening met de relevante en specifiek geldende wet- en regelgeving en bestaande contractuele verplichtingen van het UWV. 3) In overleg met de verantwoordelijke voor contractmanagement / servicelevel management worden de te leveren SaaS diensten, oplossingen en middelen (in dienstenniveaus) nader beschreven en vastgelegd (bijvoorbeeld in een SLA) die verbonden is aan de overeenkomst. De niveaus zijn in lijn met het beleid van UWV en onder andere gericht op beschikbaarheid, openstelling, vertrouwelijkheid (zonering) en herstel (disaster recovery), en zodanig vastgelegd dat deze voldoende bepaalbaar, beheersbaar en juridisch verbindend zijn. 4) Voor het onderzoeken en bepalen of een aanpassing/alternatief passend is, gelden de voorwaarden en standaarden van het UWV als vertrekpunt en wordt een afwijking ten nadele van UWV tijdig vooraf getoetst bij de verantwoordelijke (stakeholders) binnen UWV.	

3.12.17. Artikel 12q – Mogelijkheid om te onderhandelen over aanpassing

12q.	**Mogelijkheid om te onderhandelen over aanpassing**	*Vereist*
Criterium	De SaaS-leverancier biedt de mogelijkheid om te onderhandelen over aangepaste servicevoorwaarden/cloudhostingovereenkomst.	
Toelichting	Vaak wordt een SaaS-cloudoplossing in den beginne gebruikt op basis van een openbaar toegankelijke TOS-overeenkomst. Uiteindelijk zal UWV een robuustere overeenkomst willen ondertekenen voor de service naarmate deze groeit of een belangrijk onderdeel wordt van de workflows van UWV. Naarmate meer data naar de SaaS-oplossing wordt verplaatst of opgebouwd, komen er bovendien, naast toenemende kosten, zorgen over de wettelijke en nalevingsvereisten naar boven. UWV zal willen onderhandelen of de overeenkomsten willen wijzigen om dergelijke problemen aan te pakken. De SaaS-leverancier biedt UWV de mogelijkheid om over een overeenkomst op maat te onderhandelen. Om voor dit criterium in aanmerking te komen, biedt de SaaS-leverancier een aanvraagproces aan waarmee UWV een op maat onderhandelde overeenkomst kan initiëren.	

3.12.18. Artikel 12r – Automatische melding van missen SLA

12r.	**Automatische melding van missen SLA**	*Vereist*
Criterium	De SaaS-leverancier maakt een automatische melding wanneer de SLA wordt gemist.	
Toelichting	De SaaS-leverancier stelt UWV onmiddellijk op de hoogte als de SLA wordt gemist of buiten de afwijking valt. Het is moeilijk of men verzuimt de SLA voor clouddiensten nauwlettend in de gaten te houden. Daarom moet de SaaS-leverancier transparant zijn en blijk geven van integriteit door de verantwoordelijkheid te nemen voor het bijhouden van de naleving van de SLA, UWV onmiddellijk op de hoogte te stellen wanneer er iets misgaat en een onmiddellijke vergoeding te bieden. Kennisgeving vindt plaats via telefoon en/of e-mail aan door UWV opgegeven contactpersonen, en de bevestiging van de kennisgeving wordt vastgelegd. De kennisgeving is specifiek en gedetailleerd. Een melding met de tekst "Sommige klanten in Europa ondervinden mogelijk af en toe vertragingen in sommige delen van de dienst" is bijvoorbeeld niet specifiek en daarom onaanvaardbaar.	

3.12.19. Artikel 12s – Exitstrategie

12s.	**Exitstrategie**	*Vereist*
Criterium	De SaaS-leverancier werkt mee aan het formuleren van een haalbare, concrete exitstrategie als onderdeel van de overeenkomst. De SaaS-leverancier accepteert de exit-regeling zoals vastgelegd in de overeenkomst met UWV, of een exit-document met daarin de verplichtingen van partijen bij eindigen van de SaaS-dienst.	
Toelichting	UWV is verplicht om een exitstrategie te formuleren bij aanschaf van een SaaS-dienst. De SaaS-leverancier geeft aan hoe zo'n exitstrategie eruit kan zien, inclusief de verantwoordelijkheden; ook die van UWV, want een exit betreft vaak een gezamenlijke verantwoordelijkheid en inspanning. Ook UWV heeft vanuit haar perspectief hierin wensen en eisen. Uiteindelijk worden de afspraken rond een exitstrategie opgenomen in de overeenkomst. De exit-regeling omvat in elk geval: · Wanneer de exit-regeling intreedt: na looptijd, opzegging of een andere reden. De regeling zorgt dat de voor exit relevante delen van overeenkomst (en eventuele BVO) van kracht blijft totdat de exit-regeling helemaal is uitgevoerd. · Dat SaaS-leverancier volle medewerking verleent in de voorbereiding, uitvoering en eindigen/migreren van de SaaS-dienst naar UWV of derde. · De opzegtermijn geeft voldoende tijd om te kunnen migreren. · SaaS-leverancier mag de data, persoonsgegevens en configuratiegegevens pas verwijderen na schriftelijke acceptatie daarvan door UVW, e.e.a. conform exit-regeling. · Op verzoek van UWV werkt SaaS-leverancier mee aan controle van een onafhankelijke partij in kader van voorbereiding op exit, bijvoorbeeld om advies te leveren over een aankomende migratie, om de uitvoering van SaaS leverancier te beoordelen, om vast te stellen dat de exit is uitgevoerd conform de exit-regeling of om te verifiëren in hoeverre data, persoonsgegevens en configuratiegegevens succesvol zijn gemigreerd. · SaaS-leverancier werkt mee met actualiseren van de exit-regeling bij wijziging van de omstandigheden zoals functionele en technische voorzieningen van de SaaS-dienst of verandering in het gebruik. · Bij een situatie waarop de exit-regeling wordt ingezet neemt SaaS-leverancier de rechten en belangen van UWV en betrokken personen in acht, volgt instructies op en levert informatie op eerste verzoek van UWV aan. Zie ook Exitvoorwaarden van VNG Projecten - GCE met een checklist en voorbeeld bepalingen om in een exit-regeling op te nemen[11].	

[11] VNG - Aandachtspuntenbij het Exitplan SaaS,
VNG - PvE Voorbeeld Exit voorwaarden ten behoeve van inkoopproces SaaS

3.12.20. Artikel 12t – Geen downtime-uitzonderingen in de SLA

12t.	**Geen downtime-uitzonderingen in de SLA**	*Gewenst*
Criterium	De SaaS-leverancier beschouwt alle downtime-gebeurtenissen die niet door UWV zijn geïnitieerd, als storingen, ongeacht hoe de downtime plaatsvindt.	
Toelichting	Dit betekent dat alle geplande, aangekondigde, geplande, ongeplande of kwaadwillige gebeurtenissen allemaal meetellen als downtime in de gedocumenteerde SLA. UWV geeft er de voorkeur aan dat de SaaS-leverancier het algehele volgen van de SLA heeft vereenvoudigd, in plaats van deze in verschillende soorten gebeurtenissen te classificeren. Dit kan betekenen dat leveranciers met 100% SLA-garanties hun gepubliceerde SLA feitelijk verlagen om rekening te houden met een minimale geplande of geplande downtime gedurende maanden, kwartalen of jaren. UWV zal haar huiswerk moeten doen met betrekking tot daadwerkelijke storingen en niet verwachten dat SLA-verklaringen een indicatie zijn van de geschiedenis of verwachtingen van het serviceniveau.	

3.12.21. Artikel 12u – Garantie van 99,99% uptime of hoger

12u.	**Garantie van 99,99% uptime of hoger**	*Gewenst*
Criterium	De SaaS-leverancier garandeert een uptime van 99,99% of hoger.	
Toelichting	Een SaaS-leverancier die een uptime-garantie van 99,99% of beter kan bieden (maandelijks gemeten), biedt potentieel een aanzienlijk betere service dan anderen. Hoewel een uptime-garantie van drie negens een vereist criterium is, demonstreren SaaS-leverancier die naar vier negens of beter kunnen gaan een meer volwassen dienstverlening.	

Uptime	Year	Month	Week
99.9%	8.76 hours	43.2 minutes	10.1 minutes
99.99%	52.56 minutes	4.32 minutes	1.01 minutes
99.999%	5.26 minutes	25.9 seconds	6.05 seconds

3.12.22. Artikel 12v – Regelmatige evaluatie van SLA, problemen en verzoeken

12v.	**Regelmatige evaluatie van SLA, problemen en verzoeken**	*Gewenst*
Criterium	De SaaS-leverancier werkt samen met UWV om minimaal jaarlijks een evaluatie te houden van de SLA, problemen en verzoeken.	
Toelichting	Om UWV te helpen het gebruik van een SaaS-oplossing te maximaliseren, werkt de SaaS-leverancier samen met UWV (ICT en Business) om minimaal jaarlijks een evaluatie te houden van de SLA, problemen en verzoeken. Dit helpt om de relatie te verstevigen, schept passende verwachtingen voor de service en stimuleert mogelijk innovatie bij de SaaS-leverancier wanneer nieuwe mogelijkheden worden geïdentificeerd om de service te verbeteren of te veranderen. Dit beoordelingsproces is waarschijnlijk een opt-in-service die is opgenomen in een zakelijke of premium ondersteuningsovereenkomst.	

3.12.23. Artikel 12w – Openbaar toegankelijke versies van service levels

12w.	**Openbaar toegankelijke versies van service levels**	*Gewenst*
Criterium	De SaaS-leverancier heeft een openbaar toegankelijke service level (SL)definitie voor alle clouddiensten met versiebeheer en revisiegeschiedenis voor standaardservices.	
Toelichting	UWV kan niet alle cloud-SL's onthouden, dus hebben SaaS-leveranciers de SL voor standaardservices op elk moment toegankelijk voor beoordeling via selfservice, en wordt inzicht gegeven in versiebeheer en revisiegeschiedenis van de SLs. UWV heeft de mogelijkheid nodig om de revisiegeschiedenis van alle SL-wijzigingen te bekijken voor een goede audit en continue beoordeling. De revisiegeschiedenis is belangrijk voor de voortdurende evaluatie en trending van SaaS-leveranciers. Ook verbetert het de communicatie en transparantie tussen de SaaS-leverancier en de klant.	

3.12.24. Artikel 12x – Programmatisch leesbaar formaat

12x.	**Programmatisch leesbaar formaat**	*Optioneel*
Criterium	De SaaS-leverancier biedt de SLA in een programmatisch leesbaar formaat aan.	
Toelichting	Organisaties zullen SaaS-leveranciers steeds meer dwingen om SLA's aan bedrijven aan te bieden in programmatisch leesbare formaten, zoals XML. Organisaties maken meer en meer gebruik van meerdere inclusief clouddiensten wat het handmatig bijhouden van elke individuele SLA tot een uitdaging maakt. UWV zal het volgen van SLA's willen automatiseren, dus wordt van de SaaS leverancier geëist dat de SLA wordt aangeboden in een programmatisch leesbaar formaat of via een service-interface die kan worden geïntegreerd in een SLA-volgsysteem of dashboard.	

3.12.25. Artikel 12y – Aansprakelijkheid voor de gevolgen

12y.	**Aansprakelijkheid voor de gevolgen**	*Optioneel*
Criterium	De SaaS-leverancier is aansprakelijk voor de gevolgen van het niet voldoen aan de SLA.	
Toelichting	De schade die kan worden aangericht wanneer een bedrijfskritische SaaS-oplossing faalt, gaat verder dan de waarde van de kosten die in rekening worden gebracht gedurende de tijd dat de service niet beschikbaar is. Sommige gevolgen voor de activiteiten van UWV hebben financiële gevolgen of gevolgen in de dienstverlening van UWV. Het beperken van de aansprakelijkheid tot de waarde van het contract of een deel van het contract is mogelijk niet adequaat voor UWV. SaaS-leveranciers aanvaarden over het algemeen geen aansprakelijkheid voor dergelijke gevolgen. UWV kan echter proberen dergelijke aansprakelijkheidsbetalingen met de SaaS-leverancier te onderhandelen voordat zij zich engageert voor bedrijfskritische diensten om het partnerschap met de SaaS-leverancier te verstevigen en verwachtingen te wekken over de bedrijfskritische aard van de dienst aan UWV. Aan dit criterium wordt voldaan als de SaaS-leverancier tijdens de evaluatie de mogelijkheid biedt om met UWV te onderhandelen over de aansprakelijkheid voor uitval van de dienstverlening. De afspraken over aansprakelijkheid zijn in lijn met de UWV inkoopvoorwaarden.	

3.13. Artikel 13 – Ondersteuning

Met de komst van SaaS-oplossingen verschuift de ondersteuning van intern (IT) naar extern, naar een dienst geleverd door de SaaS-leverancier, eventueel bemiddeld door een interne (IT) afdeling. Daarom worden effectieve ondersteuningsprocessen en communicatie met de IT-afdeling van UWV belangrijk voor het succes van de SaaS-oplossing binnen UWV.

3.13.1. Artikel 13a – Openbaar dashboard met statusinformatie

13a.	**Openbaar dashboard met statusinformatie**	*Vereist*
Criterium	De SaaS-leverancier biedt een openbaar dashboard of momentopname van de servicestatus en de standaard SL-status aan.	
Toelichting	De SaaS-leverancier beidt een dashboard of momentopname van de servicestatus en de standaard SL-status aan, zodat elke potentiële klant en elke klant, en dus UWV, deze op elk moment kan bekijken. Dit dashboard is openbaar zichtbaar, er is geen login vereist. Bovendien is het binnen vijf minuten na een servicestoring bijgewerkt.	

3.13.2. Artikel 13b – Tweede-lijns ondersteuning

13b.	**Tweede-lijns ondersteuning**	*Vereist*
Criterium	De SaaS-leverancier biedt 2e-lijns ondersteuning, dat wil zeggen de mogelijkheid voor de IT-helpdesk van UWV om contact op te nemen met de ondersteuningsdiensten van de SaaS-leverancier.	
Toelichting	Het verzoek kan via e-mail of telefoon worden gedaan. Bovendien biedt de leverancier ook een live-chatkanaal aan waarmee UWV instant messaging kan gebruiken om met ondersteuning te communiceren over hun technische en niet-technische serviceverzoeken. Bij voorkeur 24/7 en afspraken kunnen worden gemaakt wat betreft een gegarandeerde bevestiging en reactie op het verzoek binnen een bepaalde tijd, afhankelijk van de BIV classificatie.	

3.13.3. Artikel 13c – Live menselijke ondersteuning in Engels en Nederlands

13c.	**Live menselijke ondersteuning in Engels en Nederlands**	*Vereist*
Criterium	De SaaS-leverancier biedt een live menselijke ondersteuning via telefoon of e-mail in het Engels en Nederlands.	
Toelichting	Terwijl SaaS-leveranciers zich wereldwijd uitbreiden, hebben (IT) organisaties als UWV ondersteuning in hun moedertaal nodig.	

3.13.4. Artikel 13d – Online selfservice-ondersteuning is gratis of inbegrepen

13d.	**Online selfservice-ondersteuning is gratis of inbegrepen**	*Vereist*
Criterium	De SaaS-leverancier biedt gratis online selfservice-ondersteuning met veelgestelde vragen (faq), een kennisbank en discussieforums voor zowel beheerders als eindgebruikers.	
Toelichting	De online selfservice-ondersteuning is gratis of inbegrepen bij de standaardservice. De discussieforums tonen bewijs van regelmatige deelname en moderatie door het ondersteunend personeel van de SaaS-leverancier. De meeste organisaties en gebruikers, inclusief UWV, geven er in eerste instantie de voorkeur aan om gebruik te maken van zelfservice-ondersteuning, dus is het een service in het standaard aanbod.	

3.13.5. Artikel 13e – Incidentbeheersysteem

13e.	**Incidentbeheersysteem**	*Vereist*
Criterium	De SaaS-leverancier heeft een online incidentbeheersysteem voor het identificeren, indienen en volgen van incidenten met de SaaS-dienst.	
Toelichting	Het systeem is online beschikbaar, toegankelijk via een API voor UWV, en biedt de mogelijkheid om incidenten in te dienen en de incidentstatus te volgen. Dit is voor UWV een belangrijk kenmerk, omdat het aangeeft dat een leverancier geïnteresseerd is in voortdurende verbetering van de dienstverlening.	

3.13.6. Artikel 13f – Cloudservicepartners

13f.	**Cloudservicepartners**	*Vereist*
Criterium	De SaaS-leverancier heeft een lijst met gevestigde en officiële partners (inclusief onderaannemers) beschikbaar voor klanten via een website of klantportaal. De partnerlijst is georganiseerd en uitgesplitst naar de dienst die een partner levert.	
Toelichting	UWV begrijpt dat de leverancier ecosysteempartners heeft die klanten en in het bijzonder UWV functionaliteit met toegevoegde waarde biedt, zoals verhoogde beveiliging, beheer, integratie, audit of controle. Het is echter tijdrovend en afleidend voor UWV om zelf de officiële partners te doorzoeken. Daarom heeft de SaaS-leverancier een lijst met gevestigde en officiële partners beschikbaar via een website of klantportaal, georganiseerd en uitgesplitst naar de dienst die een partner levert.	

3.13.7. Artikel 13g – Klantadviespanel en zelfbedieningssuggesties

13g.	**Klantadviespanel en zelfbedieningssuggesties**	*Vereist*
Criterium	De SaaS-leverancier evolueert en reageert voortdurend op de eisen van de klant middels een aantoonbaar klantadviespanel en zelfbedieningskanaal.	
Toelichting	De SaaS-leverancier evolueert en reageert voortdurend op de eisen van de klant. De SaaS-leverancier betrekt hierin zijn eco-systeem van software- en hardwareleveranciers middels een klantadviespanel dat inzicht en input biedt in opkomende vereisten en routekaarten voor functies. Hoe zo'n klantadviespanel moet functioneren is aan de SaaS-leverancier, maar om voor dit criterium in aanmerking te komen toont de SaaS-leverancier aan dat zo'n panel bestaat. Voor klanten die geen deel uitmaken van het officiële klantadviespanel biedt de SaaS-leverancier de mogelijkheid om via zelfbediening functieverzoeken, productverbeteringen, nieuwe klantvereisten of algemene feedback en suggesties in te dienen. UWV als klant krijgt toegang tot één van deze kanalen.	

3.13.8. Artikel 13h – Gedocumenteerde procedures voor wijzigingsbeheer

13h.	**Gedocumenteerde procedures voor wijzigingsbeheer**	*Vereist*
Criterium	De SaaS-leverancier biedt en volgt gedocumenteerde procedures voor wijzigingsbeheer, waaronder kennisgevingen aan zijn klanten over eventuele wijzigingen die een merkbare impact op de service zullen hebben.	
Toelichting	Een aantrekkelijk kenmerk van een SaaS-oplossing is het potentieel aan ontzorging aangaande upgrades, patches en ander onderhoud, dat een noodzakelijk ingrediënt is van on-premise oplossingen. De SaaS-leverancier stelt klanten en in het bijzonder UWV echter wel op de hoogte van aanstaande wijzigingen en mogelijke operationele problemen met nieuwe releases voor de dienst. Het is ook nuttig voor de SaaS-leverancier om UWV een test- en validatieprocedure te bieden als onderdeel van de wijzigingsbeheerinformatie. Dit helpt UWV ervan te verzekeren dat wijzigingen in de productieservice grondig zijn doorgelicht en getest voordat ze worden doorgevoerd.	

3.13.9. Artikel 13i – Gedocumenteerde procedures voor het prioriteren van incidenten

13i.	**Gedocumenteerde procedures voor het prioriteren van incidenten**	*Vereist*
Criterium	De SaaS-leverancier beschikt over een gedocumenteerde prioriteringsprocedure voor incidenten, die definities bevat voor de ernst van problemen (bijvoorbeeld kritiek, groot en klein) en de bijbehorende respons- en oplossingstijden.	
Toelichting		

3.13.10. Artikel 13j – Gedocumenteerde incidentresponsplannen

13j.	**Gedocumenteerde incidentresponsplannen**	*Vereist*
Criterium	De SaaS-leverancier heeft gedocumenteerde incidentresponsplannen waarin de rollen en verantwoordelijkheden van zowel de SaaS-leverancier als UWV gedetailleerd worden beschreven.	
Toelichting		

3.13.11. Artikel 13k – Migratieondersteuning

13k.	**Migratieondersteuning**	*Vereist*
Criterium	De SaaS-leverancier biedt UWV migratieondersteuning aan voor het verplaatsen van en naar de dienst.	
Toelichting	Omdat de meeste SaaS-oplossingen gebruikersinformatie en gegevens vereisen en opslaan, levert de SaaS-leverancier migratieondersteuning aan UWV voor het verplaatsen van en naar de dienst. Dit omvat expertise, hulpmiddelen (indien nodig) en, in sommige gevallen, financiële hulp. Het migreren van e-mail naar een SaaS-oplossing vereist bijvoorbeeld expertise in het migreren van het lokale systeem en een tool die de gegevens van de mailbox van de gebruiker in het bestaande systeem naar de cloudoplossing verplaatst. Het is vooral belangrijk dat de SaaS-leverancier bij het overstappen naar de dienst UWV de zekerheid biedt dat haar gebruikers en gegevens onder haar eigendom en controle blijven.	

3.13.12. Artikel 13l – Toegewezen supportmanager en accountvertegenwoordiger

13l.	**Toegewezen supportmanager en accountvertegenwoordiger**	*Vereist*
Criterium	De SaaS-leverancier biedt een toegewezen contactpersoon (supportmanager en/of accountvertegenwoordiger) aan als escalatiepunt voor ondersteunings- en accountproblemen, en een relatiebemiddelaar tussen UWV en de leverancier, als onderdeel van een enterprise- of premium-ondersteuningsovereenkomst.	
Toelichting	Afhankelijk van de SaaS-leverancier kunnen er voor deze service extra kosten in rekening worden gebracht.	

3.13.13. Artikel 13m – Optie voor premium ondersteuningsmodel

13m.	**Optie voor premium ondersteuningsmodel**	*Vereist*
Criterium	De SaaS-leverancier biedt een premium ondersteuningsmodel aan voor intensieve ondersteuning om een bovengemiddeld niveau van responsiviteit en actie van de SaaS-leverancier te ontvangen.	
Toelichting	UWV is bereid te betalen voor intensieve ondersteuning om een bovengemiddeld niveau van responsiviteit en actie van de SaaS-provider te ontvangen. De SaaS-leverancier biedt deze mogelijkheid, vooral voor SaaS-oplossingen die UWV als bedrijfskritisch beschouwt. Premium-ondersteuningsmodellen bevatten (minimaal) opties voor: • Toegewijde technische accountmanager • Onbeperkt benoemde contactpersonen binnen het bedrijf • Escalatie van incidenten met prioriteit • Jaarrekening- en SLA-beoordelingen	

3.13.14. Artikel 13n – Servicecredits voor gemiste ondersteuningsreacties

13n.	**Servicecredits voor gemiste ondersteuningsreacties**	*Vereist*
Criterium	In geval van premium-ondersteuning biedt de SaaS-leverancier ondersteuning-gebaseerde SLA in het contract aan dat gedetailleerde beschrijvingen bevat van ondersteuningsdiensten en bijbehorende credits voor gemiste ondersteuningsreacties en oplossingstijden.	
Toelichting	UWV kiest hierbij voor premium ondersteuning, veelal voor bedrijfskritische processen. Dit zorgt ervoor dat UWV gedurende de hele contractperiode onverminderde ondersteuning krijgt en in geval van verstoring wordt de leverancier aansprakelijk gesteld door het opleggen van overeengekomen boetes. Onderhandel over ondersteuning, sandboxes en andere belangrijke variabelen in SaaS-contracten om onvoorziene of verborgen kosten te minimaliseren. Denk aan: • Extra ondersteuning: onderhandel vooraf over de kosten voor uitgebreide SaaS-ondersteuningsopties. • Extra sandboxes: onderhandel vooraf over de kosten van extra sandboxen en documenteer dit duidelijk in het contract. • Opslag: leg type en hoeveelheid opslag en andere vergoedingen in het SaaS-contract vast, en onderhandel over de kosten voor extra volume. • Backup: sommige SaaS-leveranciers brengen extra kosten in rekening voor het maken van back-ups van gegevens; er kunnen ook extra kosten in rekening worden gebracht voor kortere perioden van herstelpuntdoelstellingen (RPO's) en hersteltijddoelstellingen (RTO's). • Encryptie: sommige leveranciers nemen encryptie op in de prijs, maar sommige brengen extra kosten in rekening, meestal als een percentage van de netto licentiekosten. • Extra API calls: sommige SaaS-leveranciers nemen een vast aantal API-aanroepen op bij de licentie en moeten er extra blokken API-aanroepen worden aangeschaft zodra dat aantal wordt overschreden. • Taalmodules: bepaalde talen zijn inbegrepen in de basislicentie van een SaaS-dienst. Voor eventuele extra taalpakketten betalen klanten een extra vergoeding. • Bandbreedte: sommige SaaS-providers beperken de hoeveelheid bandbreedte die gedurende een bepaalde tijdsduur wordt gebruikt. Nadat een klant deze limiet heeft bereikt, worden er extra kosten in rekening gebracht.	

3.13.15. Artikel 13o – Proefoptie beschikbaar

13o.	**Proefoptie beschikbaar**	*Gewenst*
Criterium	De SaaS-leverancier biedt proef- of proof-of-concept-opties aan waarmee UWV de dienst kan uitproberen voordat ze deze koopt.	
Toelichting	Een proefperiode is gratis en kan de metrische hoeveelheden en de tijdsduur beperken, maar zou idealiter de functionaliteit van de aangeboden kerndienst niet moeten beperken. Dit geeft UWV de mogelijkheid om de dienst of de nieuwe functionaliteit in een dienst grondig te testen en te evalueren. Bij aanbestedingen wordt in de regel nooit om een proefversie gevraagd. Dit past niet goed binnen een regulier aanbestedingsproces. Wat wel kan is dit voorafgaand aan een aanbestedingsproces doen via een marktconsultatie of marktverkenning. Of via een aanbesteding maar dan wordt het een gebruikerstest/demo en daarmee onderdeel van de beoordeling.	

3.13.16. Artikel 13p – Professionele diensten voor implementatie en ondersteuning

13p.	**Professionele diensten voor implementatie en ondersteuning**	*Gewenst*
Criterium	De SaaS-leverancier biedt professionele diensten voor implementatie en ondersteuning bij grote, bedrijfskritische implementaties.	
Toelichting	In het geval van grote implementaties van een SaaS-oplossing, vooral als de dienst bedrijfskritisch is voor UWV, biedt de SaaS-leverancier professionele diensten aan voor ondersteuning en implementatie. Als deze services worden geleverd door de partner van een SaaS-leverancier, heeft die partner training en speciale toegang tot de bronnen en omgeving van de SaaS-leverancier.	

3.13.17. Artikel 13q – Controls voor de toepassing van patches, upgrades en wijzigingen

13q.	**Controls voor de toepassing van patches, upgrades en wijzigingen**	*Gewenst*
Criterium	De SaaS-leverancier biedt controls voor selectieve toepassing van patches, upgrades en wijzigingen in de dienst.	
Toelichting	In sommige SaaS-oplossingen kan de SaaS-leverancier controlemogelijkheden bieden die UWV in essentie in staat stelt te kiezen welke versie van de SaaS-oplossing zij wil gebruiken. Dit omvat ook het dicteren van de toepassing van patches of upgrades van de dienst. Een andere optie die kan worden aangeboden is de mogelijkheid om nieuwe functies of wijzigingen aan de service in een beheerconsole in of uit te schakelen, met verfijningsopties die voor de ene groep gebruikers kunnen worden ingeschakeld en voor een andere groep gebruikers kunnen worden uitgeschakeld.	

3.13.18. Artikel 13r – 1e-lijns ondersteuning

13r.	**1e-lijns ondersteuning**	*Optioneel*
Criterium	De SaaS-leverancier biedt 1e-lijns helpdeskondersteuning.	
Toelichting	De meeste organisaties behouden 1e-lijns helpdeskondersteuning (directe interactie met de eindgebruiker in geval van een probleem) bij de implementatie van SaaS-oplossingen. In sommige gevallen wil UWV echter dat de SaaS-leverancier (eventueel inclusief een partner) alle ondersteunende verantwoordelijkheden voor de SaaS-oplossing op zich neemt. Het bieden van 1e-lijns ondersteuning betekent dat gebruikers voor alle problemen en vragen rechtstreeks contact opnemen met de SaaS-leverancier.	

3.13.19. Artikel 13s – Opleidingsondersteuning

13s.	**Opleidingsondersteuning**	*Optioneel*
Criterium	De SaaS-leverancier biedt opleidingsondersteuning.	
Toelichting	Naast technische en niet-technische ondersteuning kunnen SaaS-aanbieders onderwijsondersteuning opnemen in hun basisondersteuningsaanbod. Dit omvat instapcursussen, certificeringen en accreditaties voor meerdere tools, technologieën en modules in hun productportfolio's. Over het algemeen zijn geavanceerde of gespecialiseerde cursussen en certificeringen inbegrepen in de premium ondersteuningsniveaus.	

3.13.20. Artikel 13t – Statusgeschiedenis

13t.	**Statusgeschiedenis**	*Optioneel*
Criterium	De SaaS-leverancier biedt minimaal zes maanden aan statusgeschiedenis van de dienst.	
Toelichting	Het statusdashboard van de dienst van een SaaS-leverancier bevat minimaal zes maanden aan statusgeschiedenis bevatten, zodat potentiële klanten en klanten als UWV voldoende tijd hebben om de status en de SLA-status te beoordelen. Deze geschiedenis is openbaar zichtbaar. Er is geen login vereist om te bekijken. De geschiedenis van zes maanden biedt UWV de mogelijkheid om een claim te controleren of te betwisten (mocht zij een probleem met de systeemprestatie vermoeden) of om rekening te houden met cyclische SLA-problemen.	

A. Referenties

Deze referenties vormen inspiratie voor criteria die niet zijn benoemd in dit document, maar aan een case kunnen worden toegevoegd of alsnog aan dit document wanneer het een duidelijke verrijking betreft.

handreiking-risicobeheersing-toepassing-publieke-clouddiensten.pdf (sharepoint.com)

10 questions you should ask when choosing a SaaS provider (rydoo.com)

Handreiking_CloudOverheden_Taskforce_LR_1_.pdf

202212-Aandachtspu
nten-back-up-en-recc

20230322-bio-thema-uitwerking-clouddiensten-v22-def.pdf (cip-overheid.nl)

BIO Thema Clouddiensten - Inleiding - NORA Online

BVO 5.1:
https://uwvnl.sharepoint.com/:w:/r/sites/arb/Reviews/Dossiers/CCoE/Werk/PvE%20SaaS/BVO%205.1.docx?d=w54e30ad2220946cea65232a2cd3b98a5&csf=1&web=1

Hoe zorg je dat een SaaS-leverancier voldoet aan je beveiligingseisen? - Informatiebeveiliging & Privacy (ib-p.nl)

VISTA
PlannenRoosteren Bijl

Aanbevelingen bij
SaaS-aanbestedingen

Programma-van-Eisen-Toelichting.pdf (onderwijsgroeptilburg.nl)

Hoe een SaaS-aankoopproces beheren (clickup.com)

CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_nl-NL.pdf

Het contracteren van cloudcomputing (SaaS) – oplossingen · Contracteren · Open Access Advocate

810 (forumstandaardisatie.nl)

VNG Handreiking Inkoop Clouddiensten

Gartner Report: How to Create a SaaS Governance Policy (bettercloud.com)

Solution Path for a SaaS Adoption Framework (gartner.com)

How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria (gartner.com) / https://www.gartner.com/document/code/778126

Selectie van een SaaS-leverancier: Maak de eisen expliciet! - iBestuur

Hoe zorg je dat een SaaS-leverancier voldoet aan je beveiligingseisen? - Informatiebeveiliging & Privacy (ib-p.nl)

algemene-inkoopvoorwaarden-ict-saas_tcm94-459454.pdf