UWV Cloud Beleid

CIO Office / CISO Office
Versie: 1.01 final
Datum: 22 juni 2020
Opsteller: Dagmar Boer i.s.m. Richard Floor

Inhoud

Management samenvatting

Dit stuk is een samenvoeging van twee eerdere documenten, te weten het '*UWV Beleid Cloud Computing* (2018-2019)' en '*IB&P Richtlijn Clouddiensten* (2016)'. Omdat het in de praktijk is gebleken dat er bij de divisies behoefte is aan meer handvatten op het gebied van Clouddienstverlening, zijn beide documenten samengevoegd.

De 'Cloud' is anno nu een niet meer weg te denken fenomeen. Ook bij UWV-divisies en stafafdelingen worden Cloud oplossingen meegenomen bij het zoeken naar (verbeteringen van) ICT-oplossingen. Naast de functionele en financiële consequenties dienen ook de InformatieBeveiliging en Privacy, IB&P, consequenties in die afweging te worden meegenomen. Deze richtlijn reikt de daarbij te benutten kaders aan t.b.v. (voorbereiding van) zowel besluitvorming als van de contractering van de Clouddiensten. Onder **Cloud computing** wordt in Wikipedia verstaan het *via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van hardware, software en gegevens, ongeveer zoals elektriciteit uit het lichtnet. De term is afkomstig uit de schematechnieken uit de informatica, waar een groot, decentraal netwerk (zoals het internet) met behulp van een wolk wordt aangeduid.*

Cloud kent onmiskenbaar voordelen. Snellere beschikbaarheid van ICT-diensten, lagere kosten en een betere meer gestandaardiseerde en daardoor meer robuuste en wendbare ICT-dienstverlening worden doorgaans als belangrijkste voordelen gezien. Ook voor UWV klinkt die belofte aanlokkelijk, behoedzaamheid is echter geboden.

1. Leeswijzer

Voor UWV-divisies en stafafdelingen is bij het zoeken naar (verbeteringen van) ICT-oplossingen de overgang naar een Cloud oplossing een optie die steeds vaker in de afwegingen wordt meegenomen. Echter het Cloud-aanbod kent grote diversiteit, wat het lastig maakt om het kaf van het koren ofwel van het meer volwassen aanbod, te onderscheiden. In hoofdstuk 2 worden eerst een aantal essentiële begrippen en algemene uitgangspunten m.b.t. de Cloud beschreven. Ook worden kenmerken van Clouddiensten en leveringsmodellen (SaaS, PaaS en IaaS) beschreven.

Cloud gebruik is bovendien niet zonder risico's. Vooraf dienen dan ook de IB&P-consequenties in die afweging van Cloudgebruik te worden meegenomen. In hoofdstuk 3 worden enkele hoofdelementen van de relevante IB&P-context aangereikt, zoals de meest relevante delen uit de BIR.

Hoofdstuk 4 is de kern van de IB&P-richtlijnen: Hierin worden de eisen aangereikt die dienen te worden gesteld bij (de voorbereiding van) de besluitvorming en bij de contractering van de Clouddiensten. De te stellen eisen zijn ingedeeld in 5 categorieën:

1. Leveranciersrelatie
2. Transparantie en Wet en regelgeving
3. Incidentbeheer
4. Toegangsbeheer
5. Gegevensafscherming en -uitwisseling

1.1. Wijzigingshistorie

Wijzigingshistorie			
Datum	***Versie***	***Actie***	***Status***
28-4-2020	1.0	Samenvoeging oude 'UWV Beleid Cloud Computing 2018-2019' en oude 'IB&P Richtlijn Cloud diensten 2016' en nadere toelichting (beide delen eerder geaccordeerd).	Akkoord AB en IV-Board

2. De Cloud: definities, kenmerken en leveringsmodellen

2.1. Definitie en afbakening Cloud

De Cloud is een containerbegrip. Cloud Computing is een ontwikkeling die het mogelijk maakt om complexe IT-functionaliteit via het Internet af te nemen, vergelijkbaar met de functionaliteit die wordt geleverd vanuit applicatie(ketens) die nu in een 'eigen' rekencentrum (in het geval van UWV ge-outsourced) geïnstalleerd zijn. Met het verplaatsen van bijvoorbeeld een applicatie van deze eigen (zgn. on-premise) omgeving naar die van een Cloud-dienstverlener gaan meestal de data waar men mee werkt ook mee.

Cloud Computing betreft het via het Internet gebruiken van hardware, software om gegevens te verwerken, en dat wordt door sommigen vergeleken met betrekken van stroom uit het elektriciteitsnet. De gebruiker (UWV) hoeft op deze manier geen eigenaar meer te zijn van die hard- en software en is niet langer verantwoordelijk voor het onderhoud. Hiermee wordt de ICT een nutsvoorziening.

2.2. Kenmerken Cloud

Cloud computing heeft de volgende kenmerken:

Karakteristieken / kenmerken van Cloud Computing
♦ **Elastisch, flexibel en schaalbaar**: de gebruiker beschikt snel over de gewenste dienst en kan er ook weer snel vanaf. Daarbij lijkt het of diensten 'tot in het oneindige' schaalbaar zijn.
♦ **Geleverd als dienst (Self Service)**: Het is mogelijk de dienst af te nemen op het moment dat die gewenst is / er een noodzaak toe is. Selfservice vergroot de wendbaarheid (Agility) van de business & IT
♦ **Betalen naar gebruik (Measured Services)**: Dienstverleners rekenen naar gebruik, de hoeveelheid en duur van de afgenomen dienst. Gebruikers betalen alleen voor de diensten die ze gebruiken en verhogen zo de IT ROI (Return On Investment).
♦ **Gedeeld met derden (Multi-tenancy)**: Dienstverleners gebruiken de infrastructuur om meerdere klanten te bedienen. Het delen van infrastructuur en software levert voordelen op financieel vlak en qua flexibiliteit (i.e. de kosten worden over meerdere klanten gedeeld, en upgrades op het gebied van software en hardware wordt één keer aangepast, voor alle klanten tegelijk) ,
♦ **Gebaseerd op internettechnologie, gevirtualiseerd en dynamisch**: Internettechnologie en virtualisatie creëren een dynamische omgeving die een snelle provisioning en een beter resourcemanagement mogelijk maakt. Dit kan tot gevolg hebben dat de locatie waar verwerking en opslag van de gegevens plaatsvindt niet bekend is. Hetzelfde kan gelden voor een eventuele onderaannemer waaraan de verwerking en opslag uitbesteed kan zijn.

Cloud Computing is vanuit het perspectief van de sourcing van ICT-voorzieningen en diensten een volgend niveau van uitbesteding (*outsourcing*), waarbij de voorzieningen/diensten de grote stap van klant specifiek naar standaard zetten.

Vanuit een financieel perspectief is het benutten van schaalgrootte de voornaamste driver. Bij Cloud Computing spelen de continuïteit- en beveiligingsrisico's bij externe opslag van (bedrijfskritische) data, het delen van applicaties/infrastructuur (*Multi-tenancy*) en juridische

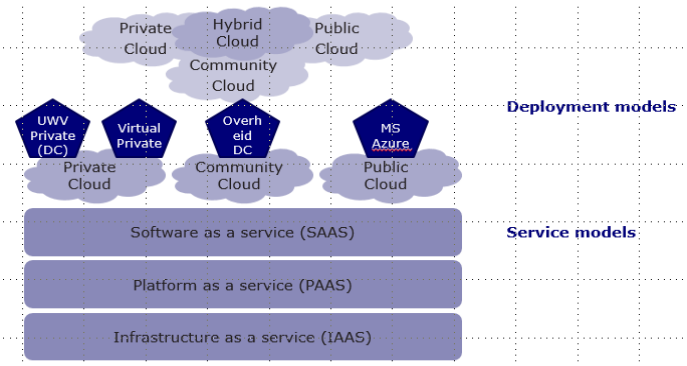
complicaties van het Internet een belangrijke rol. Daarbij zijn de kenmerken en leverings- en afnamemodellen en de daaraan verbonden risico's belangrijk.

2.3. Leveringsmodellen Cloud

De definities en referentiemodellen van het NIST (National Institute of Standards and Technology) zijn door de markt en veel organisaties algemeen geaccepteerd als een werkbare basis voor de ontwikkeling van een visie en strategie ten aanzien van Cloud Computing[1].

NIST onderkent de volgende drie leveringsmodellen:

- **IaaS**: *Infrastructure as a Service* is de basis variant. Hierin wordt pure reken- of opslagcapaciteit ter beschikking gesteld. Voorbeelden zijn: Amazon EC2 & S3, GoGrid en Rackspace Cloud.
- **PaaS**: *Platform as a Service* gaat een stap verder. Hierbij wordt een ontwikkelomgeving ter beschikking gesteld, op basis waarvan gebruikers zelf applicaties kunnen (laten) ontwikkelen, beheren en exploiteren. Voorbeelden zijn: Appian, Cordys, Microsoft Azure en Tibco Silver.
- **SaaS**: *Software as a Service* is het meest vergaande leveringsmodel. Hierbij bestaat de dienstverlening uit een kant-en-klare applicatie. Voorbeelden zijn: Basecamp, Dropbox, Google Apps, Microsoft OneDrive en Salesforce.com.



Figuur 1.0

[1] Als voorbeelden gelden het initiatief voor de ontwikkeling van de Gesloten RijksCloud (GRC), de ontwikkeling van een Europese Cloud strategie en activiteiten van het CIO-platform Cloud Interest Group (CIG).

3. Risicobeheersing vanuit IB&P en architectuur bij toepassing Cloud

3.1. Algemene uitgangspunten voor gebruik Cloudoplossingen

De algemene uitgangspunten van het UWV Cloudbeleid zijn:

- ***Informatiebeveiliging en privacy:*** inzet van Clouddiensten mag geen risico's opleveren voor de stabiliteit, continuïteit en informatiebeveiliging van het ICT-landschap (zie 3.2);
- ***Architectuur:*** UWV kiest voor een restrictief beleid v.w.b. het gebruik van Clouddiensten als het gaat om voorzieningen die gegevens verwerken van vertrouwelijkheidsklasse 2 of hoger (voor toelichting zie 3.3). Deze voorzieningen wil UWV bij voorkeur in het eigen datacenter plaatsen c.q. in een omgeving die niet met derden wordt gedeeld. Hierdoor heeft UWV meer grip op deze voorzieningen en loopt minder risico's op het gebeid van veiligheid, privacy en continuïteit te garanderen;
- ***Technologie:*** UWV wil aansluiting hebben bij marktstandaarden qua technologie. Wanneer UWV nieuwe maatwerkapplicaties laat ontwikkelen, wil zij gebruik maken van technologieën die ook vanuit de Cloud geleverd worden. Hier worden deze applicaties geschikt om *potentieel* in de Cloud te draaien en worden risico's op het vormen van legacy verminderd (zie 3.3).

3.2. Risicobeheersing vanuit IB&P-perspectief

3.2.1. Uitgangspunten voor gebruik Cloudoplossingen vanuit IB&P-perspectief

IB&P (Informatiebeveiliging en Privacy) is het aandachtsgebied dat continuïteit en betrouwbaarheid van informatie(systemen) betreft.

De scope van IB&P omvat de zogenaamde BIVC:
- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Controleerbaarheid

Deze 4 te borgen eigenschappen vormen de basis voor de in hoofdstuk 4 beschreven maatregelen. Voor vertrouwelijkheid is de indeling in vertrouwelijkheidklassen zeer essentieel. Deze worden hieronder beschreven. Controleerbaarheid richt zich op de maatregelen om o.a. te kunnen vaststellen of met de IB&P-borging kan worden voldaan aan de geldende Wet en regelgeving.

Risico's c.q. aandachtspunten bij de Cloud benutting voor UWV zijn er ook, bijvoorbeeld:

- Ontstaan/verergeren van een ongewenste Vendor lock-in en de daaraan verbonden continuïteitrisico's.
- Voor de goede werking van een Clouddienst die aan de voorkant is gepositioneerd kunnen gegevens uit het UWV-gegevens achterland vereist zijn. Dit vergt koppelingen tussen Cloud en bestaande ICT-voorzieningen.
- Het UWV ICT landschap kan er minder overzichtelijk en daardoor minder beheersbaar door worden waardoor o.a. weer veiligheidsrisico's kunnen ontstaan.
- Er moet opnieuw worden aangetoond dat er ook in de nieuwe situatie-met-cloud-benutting wordt voldaan aan wettelijke (certificerings-)eisen van de UWV dienstverlening

Vanuit IB&P zijn er daarnaast de volgende aandachtspunten:

- Afscherming van de UWV gegevens in de Cloud van andere benutters van 'dezelfde' Cloud
- Cloud dienstverlening staat nog meer op afstand van de UWV organisatie. Er is om die reden extra aandacht vereist voor transparantie/monitoren. Zo dient transparant te zijn dat er wordt voldaan aan de juridische eis dat de UWV gegevens alleen worden opgeslagen in vertrouwde landen binnen de EER, Europese Economische Ruimte.

- Voorbereid zijn op forensisch onderzoek in het kader van bijv. de meldplicht datalekken is steeds meer vereist en dient te worden geborgd.
- De mate waarin Clouddiensten goed gewapend zijn tegen Cybercrime varieert. Er zijn sterke aanwijzingen dat in het goede, mature, deel van het aanbod die wapening zeer adequaat en kosteneffectief is ingericht. Dat heeft te maken met de vergaande standaardisering en het toepassen van security-by-design principes.

Verwijderd:

Dit laatste punt kan betekenen dat Cloud verbeterde mogelijkheden kan bieden aan UWV om bij te blijven in de cyber crime wedloop. Dit voor IB&P in potentie zeer belangrijke voordeel kan alleen worden benut als het goed gewapende aanbod effectief kan worden geselecteerd. Deze richtlijn geeft een aantal belangrijke te stellen eisen waarmee dat kan worden bereikt. Consequentie van de toepassing daarvan is dat het aantal aanbod-opties wordt beperkt. Ook zal het stellen van die eisen kostenverhogend kunnen (lijken te) werken.

De in hoofdstuk 4 genoemde maatregelen bieden UWV een set van te stellen requirements om bij het afwegen en contracteren van Clouddiensten valkuilen op IB&P vlak te voorkomen en verbeterkansen beter te kunnen benutten. Op de benutting van deze richtlijn door de divisies van UWV is het pas-toe of leg-uit principe van toepassing. Niet opvolgen ervan dient wel te kunnen worden uitgelegd.

Bij kleine toepassingen kan deze afweging compact plaatsvinden. Bij grote toepassingen zal er doorgaans meer bij komen kijken.

3.2.2. Risicobeheersing en Cloud leveringsmodellen

Elk leveringsmodel (zie § 2.3 “Leveringsmodellen Cloud”) kent een andere uitgangspositie voor de noodzakelijke risicobeheersing:

- In het SaaS model waarbij nagenoeg alles is uitbesteed, is de Cloud leverancier operationeel verantwoordelijk voor praktisch alle beveiligingsaspecten, met uitzondering van het beheren van gebruikers en gebruikersaspecten (functioneel beheer). Op moment van selectie en contractering worden alle IB&P keuzes door UWV gemaakt. Later toevoegen van IB&P beheermaatregelen is niet mogelijk of in elk geval zeer lastig. Ook de (goed beveiligde) uitwisseling van gegevens tussen de UWV-eigen omgeving en de SaaS dient vooraf goed geregeld te zijn.
- In het PaaS model liggen de beveiligingsopties redelijk vast binnen het platform en de bijbehorende configureerbare omgeving (ontwikkelomgeving). Hierbij hebben zowel de Cloud leverancier als UWV beiden een verantwoordelijkheid.
- In het IaaS model is UWV voor een groot deel verantwoordelijk voor het adequaat implementeren van beveiligingsmaatregelen. De Cloud leverancier is in dit model nog steeds operationeel verantwoordelijk voor de fysieke beveiligingen van de hardware en dient te acteren als verkeersregelaar voor het netwerk dat gedeeld wordt door UWV met de andere organisaties die de betreffende Clouddiensten afnemen.

Het is zeer gewenst de Cloudoplossing op IB&P gebied te laten toetsen, eventuele restrisico’s dienen daarbij te worden geduid en opgenomen in het UWV risicoregister. Deze dienen te worden aangemeld in de centrale mailbox: ICTSecurityArchitectuur@uwv.nl .

Het zal voorkomen dat Cloud leveranciers, om hun diensten aan UWV te leveren, zelf ook gebruik maken van Clouddiensten (d.w.z. onderaannemers). Het UWV Cloud beleid is dan ook van toepassing. Met name als gegevens van UWV-klanten of van UWV-medewerkers daardoor in de Cloud terecht komen dan geldt hier dezelfde zorgvuldige afweging.

3.2.3. Het UWV ICT landschap en inzet van Clouddiensten

Het meer gaan benutten van Clouddiensten zal consequenties hebben voor het UWV ICT landschap. Twee situaties zijn daarbij van belang:

Situatie	Beschrijving	Koppeling met bestaand ICT-landschap
1	Clouddiensten die op zichzelf staan en waarbij er geen koppeling plaatsvindt met andere UWV-applicaties.	In de regel zal de impact op het ICT-landschap beperkt zijn.
2	Clouddiensten waarbij een koppeling tussen bestaande ICT-toepassingen (het bestaande ICT-landschap) met de nieuwe Clouddienst (of uitbreiding van een reeds bestaande Clouddienst) een vereiste is.	Voor de benodigde koppelingen dient in deze situatie een oplossing te worden getroffen.

In de niet-Cloud-setting zijn tot nu toe koppelingen tussen applicaties binnen hetzelfde rekencentrum, het UWV-HRC, in veel gevallen verre van eenvoudig gebleken. Koppelen vanuit gegevensbronnen/applicaties in het HRC met Cloud toepassingen kan nog lastiger (lijken te) zijn. Bij de bepaling van de impact op het ICT-landschap van de toepassing van Clouddiensten (die vooraf plaats dient te vinden, zie daarover ook verderop in hst. 4.5) dient daarom die noodzaak tot koppelen tijdig in kaart te worden gebracht en van een goede oplossing te worden voorzien, ook beheermatig voor in de toekomst. De kwaliteit van die oplossing is van invloed op de resulterende complexiteit van het ICT-landschap. Die complexiteit kan afnemen door:

- Het aantal vereiste koppelingen beperkt te houden, en;
- De koppelingen die er komen zo standaard mogelijk te houden.

In zijn algemeenheid kan hier niet veel meer over gezegd worden maar situationeel wel. Om die reden zijn in de bijlage een achttal praktijkvoorbeelden c.q. use cases nader uitgewerkt ter illustratie.

3.2.4. Vertrouwelijkheidsklassen

De richtlijn om de Vertrouwelijkheid te classificeren geldt voor alle gegevens, zowel digitaal als fysiek en is daarmee niet specifiek voor Cloud. Voor elk gegeven wordt de Vertrouwelijkheid vastgesteld, gericht op de aard van het gegeven[2]. Dit betreft de 'V' van de BIVC-classificatie. De Vertrouwelijkheidsklassen zijn gerelateerd aan de aard van de gegevens.

Aard van de gegevens
Vertrouwelijkheidsklasse 3 - Strikt vertrouwelijk ♦ Strikt vertrouwelijke gegevens waarvan ongeautoriseerde onthulling direct of indirect tot ernstige (politieke) schade kan leiden;

[2] De indeling voor Vertrouwelijkheid sluit aan bij de indeling zoals gehanteerd in de Forum Standaardisatie: 'Een handreiking voor overheidsorganisaties – Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten (versie 3)', augustus 2014.

- Zeer gevoelige gegevens, zoals gegevens waarop een bijzondere of een wettelijk bepaalde geheimhoudingsplicht rust, of gegevens die onder een beroepsgeheim vallen (bijvoorbeeld medisch) in de zin van Wbp Artikel 9, lid 4;
- Gegevens van personen naar wie een onderzoek is ingesteld in verband met een mogelijke wetsovertreding.

Vertrouwelijkheidsklasse 2 - Vertrouwelijk
- Vertrouwelijke gegevens die niet voor brede kennisneming zijn bedoeld;
- Gevoelige informatie waaronder bijzondere persoonsgegevens als genoemd in Wbp Artikel 16 en financieel-economische gegevens in relatie tot de betrokkene.

Vertrouwelijkheidsklasse 1 - Basisniveau
- Gegevens die niet zijn bedoeld voor het publiek, maar waarvan ongeautoriseerde onthulling geen schade zal veroorzaken;
- Reguliere persoonsgegevens zolang deze niet kunnen worden gerekend tot de bijzondere persoonsgegevens conform Wbp Artikel 16.

Vertrouwelijkheidsklasse 0 - Publiek niveau
- Niet vertrouwelijke gegevens die publiekelijk beschikbaar kunnen worden gesteld;
- Openbare persoonsgegevens waarvan algemeen is aanvaard dat deze geen privacy risico opleveren voor de betrokkene.

De vuistregels voor de Vertrouwelijkheidsclassificatie van gegevens zijn:
- Naarmate gegevens gevoeliger of waardevoller zijn, hebben deze een hogere vertrouwelijkheidsklasse en wordt toegang tot deze gegevens sterk gelimiteerd;
- Bij UWV is, behoudens bij medische gegevens, de standaardwaarde ('default') de Vertrouwelijkheidsklasse 2, waarvoor het regulier toepassen van de gebruikelijke beveiligingsmaatregelen binnen UWV volstaat.

3.2.5. Normenkaders

IB&P maakt gebruik, of is een verdere uitwerking, van standaard geldende normenkaders. Een belangrijk normenkader voor UWV is de Baseline Informatiebeveiliging Rijksdienst (BIR:2012) [1].

De BIR gaat zelf niet specifiek in op Cloud maar geeft een algeheel normenkader voor informatiebeveiliging. Bepaalde onderwerpen zijn echter ook in de Cloudcontext van belang. Zo wordt in hoofdstuk 6.2 van het Tactisch Normenkader (TNK) van de BIR, aandacht besteed aan Externe partijen (zoals Cloud dienstverleners en klanten die gebruik maken van de Cloudoplossing).

6.2.1 Identificatie van risico's die betrekking hebben op externe partijen
De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.

1. *Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.*
2. *Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.*
3. *(R) Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie (bijv. risicoklasse van WBP of vertrouwelijkheidklasse volgens VIRBI) heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.*
4. *Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.*

5. *(R) Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform WBP artikel 14) afgesloten.*
6. *Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd (zie ook 6.2.3.3). Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.*

In hoofdstuk 4.1 wordt de relatie met de Cloud leverancier als externe partij nader uitgewerkt. Door aan de in 4.1 gestelde eisen te voldoen (of er geargumenteerd van af te wijken) kan aan deze BIR-maatregelen een passende uitvoering worden gegeven.

6.2.2 Beveiliging behandelen in de omgang met klanten

Alle geïdentificeerde beveiligingseisen behoren te worden behandeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.

1. *Alle noodzakelijke beveiligingseisen worden op basis van een risicoafweging vastgesteld en geïmplementeerd voordat aan gebruikers toegang tot informatie op bedrijfsmiddelen wordt verleend.*

In hoofdstuk 4.4 wordt bij toegangsbeheer dit nader uitgewerkt. Door aan de in 4.4 gestelde eisen te voldoen (of er geargumenteerd van af te wijken) zal aan deze BIR-maatregelen een passende uitvoering kunnen worden gegeven.

6.2.3 Beveiliging behandelen in overeenkomsten met een derde partij

In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.

1. *De maatregelen behorend bij 6.2.1 zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd.*
2. *Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.*
3. *In contracten met externe partijen is vastgelegd hoe men dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.*
4. *In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding.*
5. *Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid en integriteit.*
6. *In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.*
7. *Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.*
8. *De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.*

Toelichting: In 6.2.3 is bij punt 2 sprake van uitbesteding van software. Clouddiensten zijn meer dan dat, maar wat er staat kan worden benut als een goede basis.

In hoofdstuk 4 wordt deze eisen in de verschillende deelhoofdstukken nader uitgewerkt. Door aan de betreffende gestelde eisen te voldoen (of er geargumenteerd van af te wijken) zal aan deze BIR-maatregelen een passende uitvoering kunnen worden gegeven.

3.3. Risicobeheer vanuit architectuurperspectief

Inzet van Cloud (zowel Public als Private = Cloud technologie vanuit het eigen datacenter) is in lijn met de het UIP en de IV-principes. In onderstaand overzicht zijn de principes die het meest relevant zijn bij de toepassing van Cloud bij UWV, aangegeven met een korte toeliching:

01 UWV stelt stabiliteit, continuïteit en informatiebeveiliging voorop

- Standaardisatie van Clouddiensten levert inherent stabiliteit in het applicatielandschap (beperking configuratiemogelijkheden).
- Continue updates door leverancier waarborgen de continuïteit.
- Cloud leveranciers hebben een inherente drive om diensten goed te beveiligen (beperking van eigen imagoschade).

03 UWV kiest voor tijdig en geleidelijk vernieuwen

- Cloud standaardproducten worden continu en evolutionair ge-update (UWV lift automatisch mee, applicatielandschap moet meebewegen).

04 UWV zet gepaste outsourcing in voor applicatieontwikkeling en –beheer en volledige outsourcing voor exploitatie van infrastructurele voorzieningen

- Cloud kan een gepaste vorm van outsourcing zijn voor UWV (standaardisatie van infra èn applicaties) mits voldaan wordt aan de gestelde randvoorwaarden op het gebied van IB&P.

07 UWV kiest voor het gebruik van gemeenschappelijke en generieke voorzieningen

- Clouddiensten worden bij voorkeur gemeenschappelijk of generiek ingezet bij UWV. Ook voor Clouddiensten moet UWV streven naar uniformiteit. Het principe hierbij moet zijn dat het proces de standaard aangeboden functionaliteit volgt. Geldt zowel voor Public afgenomen Clouddiensten als ook diensten die uit het eigen datacenter beschikbaar worden gesteld)

08 UWV kiest voor een inrichting van het ICT-landschap met gestandaardiseerde en vervangbare bouwblokken, zowel in de infrastructuur als in de software

- Clouddiensten zijn per definitie standaard bouwblokken (Public èn Private). Ze zijn immers ontworpen voor en worden geleverd aan zoveel mogelijk afnemers.
- Public Clouddiensten leveren daarom elasticiteit en schaalbaarheid (betalen naar gebruik).

09 UWV kiest bij de selectie van een IV-oplossing voor hergebruik boven standaardoplossing, en standaardoplossing boven maatwerk

- Dus ook hergebruik van bestaande Clouddiensten die reeds in gebruik zijn bij UWV.
- Bij verwerving van nieuwe ICT-middelen wordt 'Cloud Readiness' een eis, inzetbaar in zowel het eigen datacenter ('on-premise') alsook in de Public Cloud inzetbaar.

Het UWV Cloud Beleid Cloud formuleert een voorkeur voor de hostingvorm van een softwareoplossing. Bij vertrouwelijkheidsklasse 2 of hoger is opslag en verwerking in het eigen datacenter altijd het vertrekpunt. De essentie van de voorkeur is gelegen in:

- UWV heeft meer grip op software-oplossingen die exclusief door of voor UWV worden gehost waarop geen andere klanten van een leverancier aanwezig zijn. Het gaat dan om zaken als het beperken van gegevensuitwisselingen en versnippering van het applicatielandschap;
- Bovengenoemde grip eist UWV om de risico's op datalekken en andere IB&P-issues te beperken.

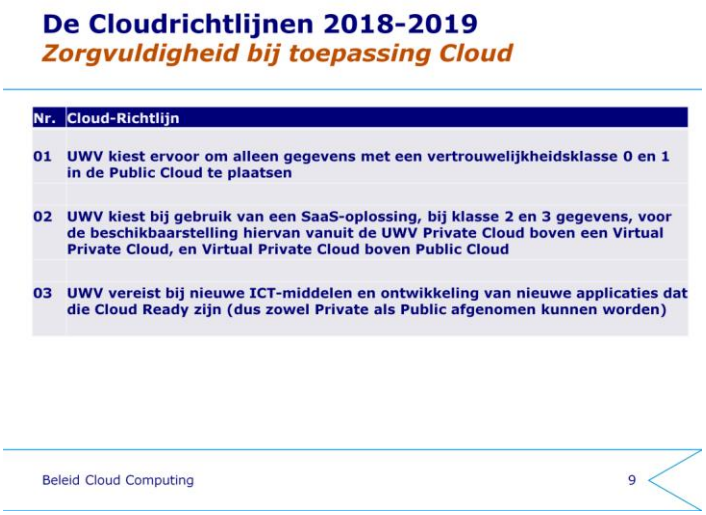
Concreet worden de volgende drie hostingvormen voor een software-oplossing onderscheiden:

1. Hosting in het UWV Data Center (IBM of DXC);
2. Hosting in een (single-tenant) Virtual Private Cloud bij de leverancier van de applicatie (of een onderaannemer);
3. Hosting in een (multi-tenant) Public Cloud omgeving.

Voor SaaS-applicaties (dus incl. hosting) met alleen klasse 0 of 1 gegevens geldt deze voorkeur niet. *Voor standaardapplicaties die zonder hosting worden ingekocht geldt dat ICT-S de opties voor hosting bepaalt!*

Echter voor maatwerkapplicaties, die dus niet in de markt gevonden kunnen worden, wil UWV de aansluiting vinden bij marktstandaarden qua onderliggende technologie. Wanneer UWV nieuwe maatwerkapplicaties laat ontwikkelen, wil zij daarbij gebruik maken van technologieën die ook vanuit de Cloud geleverd kunnen worden. Hiermee worden deze applicaties geschikt om *potentieel* in de Cloud te draaien en worden de risico's op het vormen van nieuwe legacy verminderd. De term 'Cloud Ready' wordt verder ingevuld door de Cloud *ontwerprichtlijnen* die in beheer zijn bij BS-GIV.

De onderstaande dia vat de richtlijnen vanuit architectuurperspectief samen:



De Cloudrichtlijnen 2018-2019
Zorgvuldigheid bij toepassing Cloud

Nr.	Cloud-Richtlijn
01	UWV kiest ervoor om alleen gegevens met een vertrouwelijkheidsklasse 0 en 1 in de Public Cloud te plaatsen
02	UWV kiest bij gebruik van een SaaS-oplossing, bij klasse 2 en 3 gegevens, voor de beschikbaarstelling hiervan vanuit de UWV Private Cloud boven een Virtual Private Cloud, en Virtual Private Cloud boven Public Cloud
03	UWV vereist bij nieuwe ICT-middelen en ontwikkeling van nieuwe applicaties dat die Cloud Ready zijn (dus zowel Private als Public afgenomen kunnen worden)

Beleid Cloud Computing 9

4. Te nemen IB&P-maatregelen: vijf categorieën

Borging van Cloudtoepassingen op IB&P-gebied dient plaats te vinden middels het treffen van een set van maatregelen. Deze maatregelen worden in dit hoofdstuk beschreven met daarbij aangegeven wanneer voor de betreffende maatregel kan, c.q. dient, te worden gekozen.

De maatregelen zijn ingedeeld in 5 categorieën:

1. Leveranciersrelatie
2. Transparantie en Wet en regelgeving
3. Incidentbeheer
4. Toegangsbeheer
5. Gegevensafscherming en -uitwisseling

Elk van deze aspecten wordt hierna nader uitgewerkt. Zoals in hoofdstuk 3.2 aangeduid dient elke maatregel de borging van een of meer van de 5 BIVC eigenschappen van de te leveren Clouddiensten.

4.1. Aspect 1: Leveranciersrelatie

De relatie die UWV met een Cloud leverancier aangaat verdient extra aandacht. Vendor lock-in (kritieke afhankelijkheid van de leverancier) is daarbij een risico. Cloudleveranciers maken niet altijd gebruik van hulpmiddelen die volledige portabiliteit (uitwisselbaarheid) garanderen. UWV zou daardoor dan niet gemakkelijk kunnen overstappen naar een andere oplossing, wat trouwens ook geldt voor softwarepakketten en technologieën. Ook de Clouddiensten weer terug migreren naar de eigen (of ge-outsourcede) ICT-omgeving kan veel impact hebben in termen van kosten, tijd of functionaliteit. Het gevolg kan zijn dat UWV afhankelijk wordt van de betreffende Cloud leverancier. Op IB&P-gebied levert dit riscio's op wanneer er zich ernstige beveiligingsincidenten voordoen bij de leverancier. Een goed voorbeeld hiervan is de Citrixproblematiek waar UWV in 2020 mee te maken kreeg.

Belangrijkste te treffen maatregelen in de contractering van Clouddiensten betreffen:

- Stel de eis dat de Cloud leverancier (open) standaardtechnologieën en –oplossingen benut (zie ook 4.1 hierboven). Hierdoor kan beter worden vastgesteld of de Cloud leverancier voldoet aan de gestelde beveiligingseisen.
- Stel de eis dat de Cloud leverancier voldoende transparantie biedt:
    - over de aangeboden Clouddiensten en achterliggende (Cloud) architectuur, standaarden, processen en procedures om deze risicoafweging te maken
    - met betrekking tot het gehanteerde rekenmodel voor het vaststellen van prijzen, zodat het aanbod en de prijzen van verschillende Cloud leveranciers beter vergelijkbaar zijn
- Stel de eis dat de Cloudleverancier kan aantonen dat zijn diensten voorzien zijn van effectieve beveiligingsmaatregelen.
- Voorkom het ontstaan van een ongewenste mate van afhankelijkheid van de Cloud leverancier (let wel: dit geldt met name voor Cloudhosting en in mindere mate voor SaaS-leveranciers die een dienstverleningspakket leveren):
    - Stel de eis tot het kunnen restoren van de hele configuratie bij een andere Cloud leverancier. Het periodiek middels bijv. een calamiteit-test daadwerkelijk vaststellen van de goede werking van zo'n restore maken belangrijk onderdeel uit van deze maatregel.
    - Stel de eis van de restore ook aan het geheel aan OTA voorzieningen indien en voorzover dat van toepassing is. De goede werking van o.a. deployment- en testprocessen in de OTAP-keten dient te worden zeker gesteld ook bij uitval van de expertise van de huidige Cloud leverancier. Stel daarom in het kader van portabiliteit extra eisen aan de documentatie van de OTA-processen.
- Stel de eis dat de Cloud leverancier beschikt over een disaster recovery plan, zodat deze adequaat op calamiteiten kan inspelen. Het hierboven beschreven restore aanpak kan daar een zeer belangrijk onderdeel van vormen.
- Stel de eis dat er een back-up beleid is waarbij ook zorg wordt gedragen voor wissen c.q. vernietigen van de gegevensdragers aan eind van de back-up life-cycle.

- Stel de eis dat beheerprocessen afdoende worden ingericht door de Cloud leverancier: Qua IB&P is voldoen aan de ISO 27001 norm daarbij het uitgangspunt.
- Human Resourcing: Stel de eis van garanties voor de betrouwbaarheid van de medewerkers van de Cloud Leverancier.
- Keten aansprakelijkheid: De Cloud Leverancier kan een deel van de dienstverlening hebben uitbesteed aan derden. Stel de eis dat hierover transparantie wordt betracht en dat er regelmatig audits (kunnen) worden uitgevoerd. Deze audit dient mede om vast te stellen dat verwerkersovereenkomst zijn afgesloten met deze derden die kloppen met de contractuele afspraken tussen UWV en de hoofdaannemer..
- Stel de eis dat de Cloudleverancier, risk-based en aantoonbaar, voldoende maatregelen heeft getroffen en deze ook onderhoudt om te voorkomen dat kwaadwillenden met succes een aanval op de Cloud leverancier uit kunnen voeren, bijvoorbeeld door middel van de (distributed) Denial-of-Service ((d)DoS) aanval
- Stel de eis dat de software die de Cloud leverancier benut nu en in de toekomst voldoet aan de SSD normen van UWV, zie [5]. Een goede mogelijkheid tot sluitende controle op het nakomen hiervan dient te worden geboden.
- Stel de eis dat de Cloud leverancier UWV het periodiek (i.e. (half) jaarlijks) uitvoeren van pentesten op haar product toestaat. Eventueel daglijkse geautomatiseerde tests kunnen deel uitmaken van de te maken afspraken, afhankelijk van het risicoprofiel van de te leveren dienst.
- Stel de eis dat de Cloud leverancier op zijn minst eens per jaar externe audits toestaat, waardoor UWV een onafhankelijk beeld krijgt of de Cloud leverancier voldoet aan de geldende eisen. Alternatief hiervoor kan zijn het jaarlijks afgeven van een TPM, Third Party Mededeling.

4.2. Aspect 2: Transparantie en Wet- en regelgeving

- UWV biedt bij de contractering de Cloud leverancier inzicht in de geldende wet- en regelgeving, standaarden, richtlijnen, gedragscodes en certificeringen waaraan UWV moet voldoen en in welke mate. Stel de eis dat de opvolging daarvan door de Cloud leverancier in de contractering wordt vastgelegd. De Cloud leverancier dient o.a. middels certificeringen deze opvolging te kunnen aantonen.
- Stel de eis dat de Cloud leverancier het UWV classificatieschema mbt. vertrouwelijkheid, zie [4], ondersteunt.
- Stel bij hogere vertrouwelijkheid-klassen, klasse 2 en 3 met name in de UWV-setting, extra eisen aan de Cloud leverancier:
    - Stel de eis dat de Cloud leverancier transparante informatie biedt over de fysieke locatie van alle UWV-data.
    - Stel de eis dat de Cloud leverancier voldoende garanties biedt dat de IT faciliteiten die UWV benut in afdoende mate zijn afgescheiden van andere organisaties die door de Cloud leverancier worden bediend
    - Als fysieke (gegevens)servers worden gedeeld met andere klanten, stel dan de eis dat opslag, geheugen en andere data-sporen volledig worden vernietigd alvorens de servers aan andere klanten ter beschikking worden gesteld. Bewijs hiervan dient aan UWV aangeleverd te worden.
    - Stel de eis dat de producten/ de tooling die de Cloud leverancier toepast gecertificeerd zijn tot het juiste niveau, wat betreft IB&P vereisten.
    - Stel de eis dat een PIA, Privacy Impact Analyse, zie ook [3], wordt uitgevoerd voor de definitieve contractering van de Cloud dienstverlening. Deze PIA dient binnen 1 jaar na in werking treden van het contract te worden herhaald. Een gunstig eind oordeel is een knock-out criterium voor voortzetting van de dienstverlening. Via ICTSecurityArchitectuur@uwv.nl kan deze PIA worden aangevraagd.
- Stel de eis dat de Cloud leverancier en/of onderaannemers het uitvoeren van digitaal (forensisch) onderzoek en audits toestaan (zie ook paragraaf 4.1). De vereisten voor zulk onderzoek, op het vlak van Logging en Monitoring bijv., dienen in de contractering van de Cloud dienst vastgelegd te worden om zeker te stellen dat UWV een goede analyse en evaluatie kan (laten) uitvoeren van opgetreden incidenten.

4.3. Aspect 3: Beheer van incidenten

T.a.v. Incidentbeheer zijn volgende maatregelen vereist:

- Stel de eis dat de UWV-service desk tijdig door de Cloud leverancier wordt geïnformeerd over incidenten, waardoor deze adequaat kan reageren.
- De verplichting tot tijdig melden geldt in versterkte mate als het incident onder de meldplicht datalekken valt of er een vermoeden is dat dat het geval zou kunnen zijn. Voor UWV geldt daarbij een termijn van 72 uur waarbinnen uiterlijk melding dient plaats te vinden. De leverancier van de Clouddienst dient zo'n incident binnen 24 uur aan UWV te melden.
- Stel de eis dat afspraken worden gemaakt en contractueel worden vastgelegd over het classificeren van incidenten (bepalen soort, impact, urgentie en prioriteit) en de maximale termijn waarbinnen ze verholpen moeten zijn.
- Stel de eis dat de Cloud leverancier goed versiebeheer uitvoert waardoor een incident kan worden gekoppeld aan de juiste versie van benutte configuratie-instellingen en van benutte applicatie-componenten c.q. andere benutte IT-middelen die voor reproduceren en verhelpen van de incidenten relevant kunnen zijn.

4.4. Aspect 4: Toegangsbeheer

Cloud dienstverlener dient voldoende capaciteit te kunnen bieden voor toegang tot de geboden diensten.

- Stel de eis dat de internetverbinding (zoals throughput, up- en downloadsnelheid) waarlangs de Cloud leverancier haar diensten levert berekend is op de hoeveelheid dataverkeer en/of het aantal connecties. Ook dient de capaciteit van de netwerkcomponenten (zoals routers, switches en firewalls) voldoende te zijn.

De toegang tot (vertrouwelijke) informatie en ICT voorzieningen moet worden gecontroleerd en beperkt zijn tot geautoriseerde personen.

- Stel de eis dat de authenticatie van UWV medewerkers tenminste plaats dient te kunnen vinden a.d.h.v. username/wachtwoord. Voor toegang tot vertrouwelijke gegevens tot max klasse 2 kan daar bij toegang via het interne UWV netwerk mee worden volstaan. Bij toegang direct via Openbare Internet is sterke authenticatie een vereiste, zeker bij gegevens van klasse 2 en hoger.
- Stel de eis dat voor extra vertrouwelijke gegevens (klasse 3: medisch, maar ook VIP-ers en bulk data met BSN's) of bijzondere handelingen (privileged voor beheer bijv.) sterke authenticatie wordt ondersteund. Zie [7] voor nadere beschrijving daarvan.
- Als extra eis kunnen LoMo, Logging en Monitoring, afspraken worden gemaakt. De gelogde gegevens dienen aan UWV ter beschikking te kunnen worden gesteld t.b.v. analyses en audits.
- Stel de eis dat het autorisatiebeheer voor benutting van de Clouddiensten compliant is met:
  - SSO, Single Sign On, via ABS voor UWV medewerkers
  - SSO o.b.v. DigiD of opvolger daarvan voor burger-klanten
  - SSO o.b.v. E-herkenning voor zakelijke klanten,
  - (andere) UWV eigen autorisatie beheer voorzieningen t.b.v. andere zakelijke relaties c.q. klantgroepen.
- Stel de eis dat voor de SSO aanpak een federatieve oplossing op basis van de SAML 2.0 standaard het uitgangspunt is.
- Stel de eis dat de provisioning van gebruiker Id's en bijbehorende autorisaties goed geregeld is, overeenkomstig de richtlijnen van SAB, Sluitend Autorisatie beheer zie [6]. Deze eis geldt ook als een federatieve autorisatie niet zou kunnen worden geboden.
- Stel de eis dat de autorisatie structuur fijnmazig genoeg is om te kunnen voldoen aan eisen van proportionaliteit en doelbinding die UWV stelt. Dit geldt met name voor toegang tot gegevens van vertrouwelijkheidsklasse 2 en hoger.

M.b.t. bijzondere handelingen/privileged accounts:

- Stel de eis dat de fysieke beveiliging van het data center afdoende geregeld is. Hiermee wordt voorkomen dat niet geautoriseerde personen toegang kunnen krijgen tot computerruimten en apparatuur
- Stel de eis dat de Cloud leverancier aantoonbaar een adequate I&AM voorziening benut voor bijzondere beheer-handelingen. Cloud provider dient transparantie te bieden welke accounts er zijn met bijzondere rechten en hoe benutting daarvan wordt gemanaged.
- Stel de eis dat de Cloud provider transparantie biedt welke afspraken er zijn over benutting van deze accounts in noodsituaties of andere uitzonderlijke situaties.
- Stel de eis dat UWV voldoende mogelijkheden heeft om privileged accounts te kunnen benutten. De autorisaties van die account dienen passend te zijn (bijv. wel voor toevoegen gebruikers maar niet voor wijzigen van gegevensopslag).

4.5. Aspect 5: Gegevensopslag en gegevensuitwisseling

De bescherming van gegevens in de Cloud is een van de belangrijkste aspecten van Clouddiensten. Belangrijkste te treffen maatregelen specifiek voor gegevensopslag betreffen:

- Stel de eis tot afscherming van de UWV gegevens van andere organisaties die de betreffende Cloud omgeving benutten. Versleutelde opslag van gegevens is daarbij een te overwegen maatregel, m.n. bij gegevens van klasse 3.
- Stel de eis van strikte fysieke beveiliging van de datacentra van de Cloud leverancier
- Stel de eis dat de Cloud leverancier niet opslaat buiten de EU. Binnen de EU dient opslag bij voorkeur plaats te vinden in vertrouwde landen in de EER, Europese Economische Ruimte. Zie hierover memo van JZ in bijlage A. Plus NATO gebied? = Militair fysieke beveiliging

Belangrijkste maatregelen bij gegevensuitwisseling zijn:

- Stel eisen aan de kwaliteit van de gegevensuitwisseling. Gegevensuitwisseling tussen de Cloud leverancier en UWV dient bijv. goed afgeschermd te zijn middels versleuteling. Ook gegevensuitwisseling tussen de Cloud leverancier en UWV klanten of UWV relaties dient aan strikte kwaliteitseisen te voldoen. Versleuteling met TLS (zie [7]) tijdens transport geldt daarbij als minimum vereiste.
- Stel de eis van adequaat key management als versleuteling van transport of opslag van gegevens plaatsvindt. Hiervoor zijn de volgende maatregelen vereist:
    - Voorzieningen voor het wegschrijven en het kunnen lezen van de sleutels
    - life cycle management van uitgegeven sleutels
    - Passende set van voorziene maatregelen in geval van diefstal van sleutels en ter preventie van sleuteldiefstal
    - Gebruiker credentials (usernames/wachtwoorden) dienen versleuteld opgeslagen c.q. afgeschermd te zijn
    - Duidelijkheid wordt geboden t.a.v. welke gegevens op welke wijze versleuteld worden bij transport c.q. bij opslag ervan
- Deze maatregelen dienen zo te worden getroffen en afgestemd met de Cloudleverancier dat wordt voldaan aan het UWV encryptie beleid, zie [7].
- Omdat in de loop der tijd wijzigingen in de gegevensuitwisseling kunnen/zullen optreden dienen er afspraken over wijzigingsbeheer te worden gemaakt:
    - Stel de eis dat de cloud leverancier bereid is om de vanuit UWV gewenste wijzigingen in de gegevensuitwisseling door te voeren in de geboden Clouddiensten. De voorwaarden die daarbij zullen gelden dienen vooraf goed te worden afgestemd en in de contractering te worden opgenomen.
    - Stel de eis dat geplande wijzigingen in de gegevensuitwisseling tijdig tussen UWV en de Cloud leverancier worden afgestemd
    - Stel de eis dat elke wijziging in de gegevensuitwisseling in voldoende mate getest wordt alvorens deze in bedrijf wordt genomen.
- In gebruik nemen van Clouddiensten heeft impact op het UWV ICT-landschap. Deze impact is met name van belang als er sprake is van gegevens uitwisseling van de Cloud dienst met andere bestaande UWV ICT voorzieningen. Stel deze impact vast alvorens tot contractering ervan over wordt gegaan. Belangrijke criteria bij die impact bepaling zijn:
    - Aantal ongelijksoortige componenten
    - Aantal niet standaard koppelingen tussen deze ongelijksoortige componenten
    - (Perspectief op) convergentie naar meer eenduidig ICT-landschap middels de toe te voegen c.q. af te bouwen componenten (als gevolg van de overgang naar Clouddiensten)

  De impact op het ICT-landschap dient per saldo positief te zijn: Het UWV ICT-landschap is na de in gebruik name van de Clouddiensten minder gefragmenteerd en meer robuust. In de bijlage met de use cases wordt aan de impact op het ICT-landschap middels o.a. een plaat de nodige aandacht besteed

  Let wel: er zijn ook Clouddiensten die zeer nuttig (kunnen) zijn zonder noemenswaardige connecties met het (overige) ICT-landschap van UWV. Voor deze Clouddiensten is geen verdere impact bepaling noodzakelijk. Die zijn neutraal en dat is prima.

5. Referenties:

1	BIR
2	NCSC White paper
3	PIA document
4	Richtlijn Classificatie Vertrouwelijkheid IB&P, versie 0.99 d.d. 30 nov 2015
5	SSD richtlijn
6	SAB proces beschrijving / richtlijn
7	Encryptie beleid

Cost Management
Exit Strategie
Migratie
Softwareontwikkeling

Kijk naar CAF e.d.