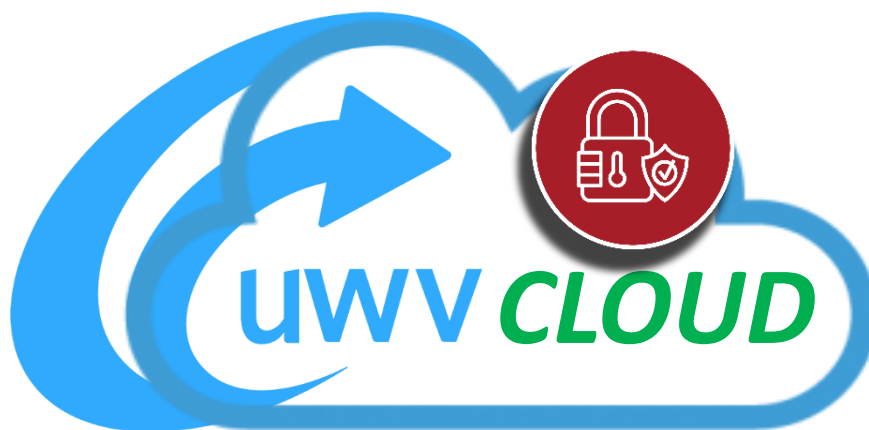


;



UWV Cloudbeleid 2.0

Chief Information Office / CISO
Versie: 2.0 definitief
Datum: 09-08-2023
Opstellers: René Zuidgeest / Nathalie Koopman

Managementsamenvatting

UWV is tot op heden terughoudend geweest in het gebruik van de publieke cloud. Hierin volgde UWV het Rijksbrede cloudbeleid daterend uit 2011. De reden van deze terughoudendheid zijn zaken als privacy, gegevensopslag, beveiliging en beschikbaarheid. Deze zaken zijn voor overheidsinstanties in het algemeen en voor UWV in het bijzonder belangrijk. Daarnaast bracht het gebruik van publieke cloudoplossingen in het verleden onacceptabele risico's met zich mee.

Echter, gezien de huidige marktontwikkelingen, het afnemende aanbod in alternatieven en de voordelen die publieke cloudoplossingen kunnen bieden, wordt het tijd om de visie op het gebruik op publieke cloudoplossingen te herzien. Dit past ook bij de overheidsbrede beweging richting publieke cloudoplossingen (en daarmee ook belangrijke partners van UWV).¹ Op EU-niveau wordt zelfs het uitgangspunt 'Cloud-first' gehanteerd, waarbij het gebruik van cloud positief ontvangen wordt mits passend bij de risico's.² UWV wil mee in deze beweging, maar wel op een wijze dat niet zozeer de vraag is of we gebruik maken van publieke cloudoplossingen

“maar vooral op welke manier we veilig en betrouwbaar applicaties en data beschikbaar maken in een hybride situatie van on-premise, private en public cloud”

Cloud dient daarbij als een serieuze optie te worden overwogen bij het inkopen van leveranciersdiensten en wordt niet als minder veilig dan on-premise alternatieven beschouwd. Dat betekent dat de visie op het gebruik van public cloud als volgt is:

UWV maakt op een verantwoorde manier gebruik van publieke cloud en de daarin aangeboden diensten. Verantwoord gebruik houdt in dat de toepassing van een publieke cloudoplossing een meerwaarde (bv in functionaliteit, in toekomstvastheid, in kosten, ...) moet bieden en veilig en risicogebaseerd gebeurt. De verwachting is dat het gebruik van publieke cloud bij UWV in de toekomst zal toenemen. Hierbij zullen diensten geïntegreerd zijn met de traditionele on-premise omgevingen van UWV waardoor sprake is van een hybride omgeving.

In dit document worden verder de voorwaarden neergelegd hoe UWV gecontroleerd, zorgvuldig en veilig gebruik kan maken van publieke cloudoplossingen bij UWV-dienstverlening. Afwegingen in de keuze voor public cloud zullen per situatie, per (bedrijfs)functie, of per applicatie worden gemaakt, wanneer een applicatie end-of-life is of nieuwe functionaliteit gewenst is. De conclusie kan dan ook zijn om geen public cloudoplossing toe te passen, maar een installatie in UWV's private cloud, mits deze geschikt is om de nieuwe functionaliteit te hosten. Het beleid geeft daarmee een afwegingskader om verantwoord (met beheersing van risico's) naar de cloud te bewegen. Elke overweging moet beginnen met hoe gegevens op een eenvoudige en veilige manier beschikbaar worden gesteld, bewerkt en opgeslagen. Waarbij de gedachte is dat cloud één van de mogelijkheden wordt bij het inkopen van dienstverlening. Wel bereiden we ons als UWV voor op cloud, door applicaties cloud-native te ontwikkelen. Het ontwikkelen van applicaties op basis van cloud-native technologieën stelt organisaties in staat schaalbare applicaties te bouwen en uit te voeren in public, private en hybrid clouds.³

Leeswijzer

In het eerste hoofdstuk wordt kort ingegaan op wat publieke cloudoplossingen zijn en wat de aanleiding is geweest om de visie op het gebruik hiervan binnen UWV, te wijzigen. In het tweede hoofdstuk wordt uitgelegd hoe dit document zich verhoudt tot kaders vanuit de overheid en binnen UWV en wat de reikwijdte van het document is. In het derde hoofdstuk worden vervolgens de randvoorwaarden weergegeven voor het toepassen van publieke cloudoplossingen bij UWV-dienstverlening. In het vierde hoofdstuk wordt een afwegingskader geformuleerd aan de hand van een stappenplan.

¹ Quint Group, <https://www.quintgroup.com/nl-nl/consulting/enterprise-cloud/marktonderzoek-cloud-overheid-2022/>, geraadpleegd op 28-09-2022

² Europese Commissie, European Commission Cloud Strategy: Cloud as an enabler for the European Commission Digital Strategy, 16-05-2019, p. 3

³ [Cloud Native Computing Foundation](#).

Inhoud

Managementsamenvatting	2
1. Achtergrond en aanleiding	5
1.1. Wat wordt bedoeld met cloud?	5
1.2. Waarom deze verandering van beleid op cloud?	5
2. Positionering en besturing	6
2.1. Positionering	6
2.2. Besturing	6
2.3. Reikwijdte	7
3. Voorwaarden	7
3.1. Richtinggevende principes	7
3.2. Informatiebeveiliging en Privacybescherming	9
3.3. Architectuur	11
4. Afwegingskader	15
4.1. Fase 1 – Verkenning	16
4.2. Fase 2 – Snelle risicoscan	16
4.3. Fase 3 – Inhoudelijke risicoanalyse	17
A. De Cloud uitgelegd	18
A.1. Definitie en afbakening	18
A.2. Kenmerken	18
A.3. Leveringsmodellen	19
A.4. Deploymentmodellen	20
B. Cloudmigratiestrategie	21

Wijzigingshistorie			
Datum	Versie	Actie	Status
3-10-2022	0.1	Eerste versie beleid opgesteld op basis van eerdere Cloudrichtlijn 2.0	Draft
6-10-2022	0.2	Afstemming CISO	Draft
	0.3	Afstemming ICT Services	Draft
	0.4	Afstemming CISO	Draft
	0.5	Afstemming Simone Werner	Draft
	0.6	Afstemming CISO	Draft
29-11-2022	0.7	Afstemming André van Alphen, Simone Werner en Raymond Groenewoud	Draft
18-01-2023	0.8	Afstemming CIO, met Alex Kooistra en Bas Hazewinkel	Draft
04-04-2023	0.86	Afstemming RIO en AB	Draft

09-08-2023	2.0	Een notitie is opgesteld voor de RvB op basis van dit document. Deze notitie is goedgekeurd door de RvB. Dit document dat meer toelichting bevat is in lijn met deze notitie. In lijn met de titel geven we de definitieve versie versienummer 2.0 mee.	Definitief
------------	-----	---	------------

1. Achtergrond en aanleiding

Dit UWV-beleid op publieke cloudoplossingen bij UWV-dienstverlening is opgesteld na het verschijnen van de Kamerbrief Rijksbreed cloudbeleid 2022. In deze Kamerbrief wordt aan overheidspartijen die niet tot de Rijksdienst behoren, gevraagd het Rijksbrede cloudbeleid te volgen⁴. Daarnaast noodzaken recente ontwikkelingen een herijking van het beleid van UWV op publieke cloudoplossingen. UWV volgt het Rijks cloudbeleid.

1.1. Wat wordt bedoeld met cloud?

Voor de definitie van 'cloud computing', hanteert UWV de definitie van het NIST⁵. Zij omschrijven het concept als een variatie tussen een complete eindgebruikersfunctionaliteit tot aan een model voor het mogelijk maken van alomtegenwoordige, gemakkelijke, on-demand netwerktoegang tot een gedeelde pool van configureerbare computerresources (bijvoorbeeld netwerken, servers, opslag, applicaties en services) die snel kunnen worden geleverd en vrijgegeven met minimale beheerinspanning of interactie met de serviceprovider⁶. Gebruikers van de cloud betalen alleen maar voor een specifiek gebruik van die resources.

Cloud kent verschillende leveringsmodellen, waarin je als UWV in meer of juist mindere mate nog zelf beheer doet binnen de cloud. Drie basismodellen zijn van belang. In het ene geval neem je een operationele applicatie af (SaaS), maar het kan ook zijn dat je infrastructurele voorzieningen (IaaS) of een platform (PaaS) afneemt en deze onder eigen verantwoordelijkheid verder inricht en gebruikt om applicaties mee te bouwen en te draaien. Mocht er behoefte zijn voor een nadere uitleg wat cloud computing nu eigenlijk inhoudt, met een aantal basisbegrippen uitgelegd, dan raden we aan om eerst *Bijlage A - De Cloud uitgelegd* door te nemen.

1.2. Waarom deze verandering van beleid op cloud?

De markt van cloud computing is de laatste jaren verder ontwikkeld. De voordelen van cloud computing worden door de markt ingezien en zijn versterkt, de aangeboden functionaliteit is sterk gegroeid en de inherente risico's die kleven aan het gebruik van cloudoplossingen zijn of worden geadresseerd.

Cloud kent onmiskenbaar voordelen⁷. Snellere beschikbaarheid van ICT-diensten, lagere investeringen, verschuiven van vaste naar variabele kosten en een betere, goed beheerde, meer gestandaardiseerde en daardoor meer robuuste en wendbare ICT-dienstverlening, worden doorgaans als belangrijkste voordelen genoemd⁸. Tevens biedt de markt – gedragen door deze succesfactoren – in toenemende mate alleen functionaliteit aan in de cloud en ontbreekt de on-premise optie, waardoor UWV gedwongen wordt om clouddiensten af te nemen en te integreren in haar ICT-landschap. Innovatie vindt plaats in de cloud.

De kanttekening is wel dat de beloofde voordelen pas worden gerealiseerd als cloud op een juiste manier wordt ingezet. Net als bij de on-premise optie, waar de organisatie wel bekend mee is, kleven aan de inzet van cloudoplossingen risico's, vergelijkbare maar ook andersoortige waarop de organisatie nieuwe of extra maatregelen moet implementeren. De eigen data bevindt zich niet meer in je eigen datacenter, wat een andere kijk op financiële, gegevensbeveiligings- en compliance-vraagstukken met zich meebrengt. Verder liggen er risico's op het gebied van verregaande leveranciersafhankelijkheid, kostenbeheersing, gebruik van nieuwe technologie zonder dat de organisatie er klaar voor is en met een gebrekkige architectuur en governance aan de slag gaat.

De verantwoordelijkheden en de (implementatie van) maatregelen zijn veelal anders dan bij de on-premise situatie, wat kan leiden tot andere, nieuwe operationele risico's, waarvan een aantal voorbeelden volgen. Zo is het zicht op kwetsbaarheden in de technologie afhankelijk van wat de leverancier deelt in plaats van dat dit tijdens een release inzichtelijk wordt. Daarnaast, als er geen

⁴ Kamerbrief Rijksbreed cloudbeleid, p.2

⁵ Deze definitie luidt: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

⁶ NIST SP 800-145 The NIST Definition of Cloud Computing

⁷ Daarbij wel opmerkende dat dezelfde voordelen ook nadelen kunnen worden wanneer niet beheerst wordt geoutsourcet. Denk hierbij aan standaardisering – we maken dan veelal gebruik van dezelfde producten. Het gevolg hiervan is dat we allen binnen de overheid ook dezelfde kwetsbaarheden overnemen van die gestandaardiseerde producten.

⁸ <https://digital-strategy.ec.europa.eu/en/library/cloud-and-edge-computing-different-way-using-itbrochure>

duidelijke afspraken tussen UWV en leverancier worden gemaakt over toegangsbeheer, kan dit leiden tot ongeautoriseerde of geen toegang tot gegevens en diensten. Verder kan een verregaande afhankelijkheid worden gecreëerd door het afnemen van een clouddienst en het verwerken door en opbouwen van een gegevensset extern, bij deze dienst. Als er vooraf geen heldere exit-strategie wordt afgesproken waardoor hoge kosten in rekening kunnen worden gebracht om de data weer in bezit te krijgen en de interoperabiliteit van de gegevens tekortschiet, is een harde vendor-lockin een feit⁹. Tot slot kunnen de kosten van het gebruik van clouddiensten wel inzichtelijk, maar complex en moeilijk voorspelbaar zijn. Dit heeft als financieel risico dat UWV geen helder zicht meer heeft op het gebruik en daarmee samenhangende kosten van cloudoplossingen.

Het nieuwe cloudbeleid zal een boost moeten geven aan cloudadoptie binnen het UWV door de voordelen te benutten en de risico's te mitigeren tot een acceptabel niveau. Diverse stakeholders en processen spelen een belangrijke rol in deze adoptie, zoals softwareontwikkelaars, servicedeskmedewerkers, inkopers, leveranciersmanagers, service-eigenaren en architecten. Deze zullen zodanig moeten worden opgeleid en gaan functioneren in een cloud-gerichte organisatie, zodat een juiste clouddienst wordt afgenomen met een juiste inrichting, op een juiste wijze geïntegreerd in het bestaande UWV ICT landschap. Ook hiervoor is in dit beleid aandacht.

Het nieuwe cloudbeleid van UWV volgt het Rijksbrede cloudbeleid 2022. In het Rijksbrede beleid wordt gesteld dat alle departementen hun eigen cloudbeleid en cloudstrategie formuleren op basis dit beleid. Onderdelen van de overheid die niet tot de Rijksdienst behoren wordt geadviseerd om dit ook te doen¹⁰. UWV volgt dit advies op en adopteert het Rijksbrede cloudbeleid, resulterend in dit document.

2. Positionering en besturing

2.1. Positionering

Het UWV-beleid op publieke cloudoplossingen bij UWV-dienstverlening staat niet op zichzelf, maar staat in relatie tot wet- en regelgeving buiten UWV en beleid binnen UWV. Intern past het cloudbeleid in de doelstelling van de UWV-strategie om het ICT-landschap op orde te krijgen door lange-termijn investeringen te doen.

UWV ziet de cloudstrategie van de Europese Commissie (EC)¹¹ als een aanbeveling en volgt het Rijksbrede cloudbeleid. De cloudstrategie van de Europese Commissie (EC) heeft als visie een verantwoord cloudgebruik met de inzet van veilige hybride/multi-cloud diensten. Op basis van deze uitgangspunten, is de Kamerbrief Rijksbreed cloudbeleid 2022 opgesteld. Deze Kamerbrief vormt tezamen met Nederlandse wet- en regelgeving het uitgangspunt voor het UWV cloudbeleid.

Op basis van het Rijksbreed cloudbeleid werkt CIO Rijk ook aan een Implementatierichtlijn met tevens een verplichtend karakter. Deze is eind 2022 gepubliceerd. De intentie is dat UWV deze ook zal volgen en zal worden opgenomen in een nog op te stellen UWV cloud Richtlijn.

Daarna zal CIO Rijk de Handreiking Risicobeheersing Publieke Clouddiensten afronden naar een definitieve versie. Deze heeft een adviserend karakter die in de basis door UWV zal worden gevolgd. Het concept, versie 0.99, 31 maart 2022 is mede input voor UWV's cloudbeleid.

2.2. Besturing

De eigenaar van het cloudbeleid is de CIO van UWV, ter vaststelling door de Raad van Bestuur.

De opdrachtgever voor beheer en doorontwikkeling hiervan is de CIO, in nauwe samenwerking met Chief information Security Office, Leveranciersmanagement, ICT Services en Inkoop.

Het UWV cloudbeleid kan niet los gezien worden van strategie- en beleidsvorming op Rijks- en Europees niveau. Er dient een herijking van het beleid plaats te vinden wanneer op deze niveaus wijzigingen worden doorgevoerd.

⁹ Tegenover een eventuele kostbare exit en migratie naar een andere clouddienst staat dat met het meer en meer afnemen van clouddiensten, de footprint van een eigen datacenter afneemt. Daardoor zal een grootschalige, complexe, dure datacenter migratie met een lange doorlooptijd, zoals deze nu wordt ervaren bij de migratie van IBM naar DXC, in de toekomst vermeden kunnen worden.

¹⁰ Kamerbrief Rijksbreed cloudbeleid, p.2

¹¹ https://ec.europa.eu/info/publications/european-commission-cloud-strategy_en

Richtlijnen over de concrete toepassingen van de uitgangspunten in dit beleid, volgen na vaststelling van het beleid.

Voor het toepassen van het beleid geldt de generieke governance:

- Het informatiebeveiligingsbeleid wordt ontwikkeld door CISO-Office, waaruit beveiligingsmaatregelen gedestilleerd worden;
- Divisies verifiëren compliance aan AVG (GEB-check/rapport) samen met de FG;
- Divisies verifiëren compliance aan overige IB&P wet- en regelgeving (zoals o.a. de BIO). Hiervoor moet een information security requirements analyse gedaan worden door de IB&P-organisatie van de divisie (al dan niet in samenwerking met CISO);
- Decentraal adviseert de Business Security Officer over de toepassing van beveiligingsmaatregelen en besluit de directie in hoeverre het advies wordt overgenomen;
- de 'afnemer', het organisatieonderdeel van UWV dat de clouddienst gaat gebruiken, verifieert of de rest-risico's acceptabel zijn op basis van een risicoanalyse die zij uitvoeren en zorgt dat de gebruikers worden opgeleid, geïnstrueerd en aangestuurd.
- ICT Services voert regie op DXC – de Cloud-Broker van UWV - als leverancier. Deze rol als Cloudbroker houdt in dat DXC public cloudoplossingen beschikbaar stelt conform de vereisten van IB&P en architectuur. Daarnaast monitoren zij het gebruik (frequentie van gebruik) en kosten van de public cloudoplossing.

2.3. Reikwijdte

Alle organisatieonderdelen van UWV conformeren zich aan het cloudbeleid bij het nemen van beslissingen over het gebruik van cloudoplossingen. Het is overkoepelend beleid dat randvoorwaarden en kaders meegeeft die moeten worden toegepast bij het maken van beslissingen en overwegingen tijdens het aanbesteden en afnemen van clouddiensten.

Een clouddienstleverancier zal ook moeten opereren in lijn met dit beleid. Ook is clouddienstverlening een vorm van outsourcing. Dit houdt in dat het UWV-beleid rond outsourcing ook van toepassing is op clouddienstverlening en de achterliggende leveranciers.

3. Voorwaarden

Voorwaarden bij gebruik van publieke cloudoplossingen komen vanuit verschillende invalshoeken, te weten architectuur, informatiebeveiliging en privacybescherming, inkoop en leveranciersmanagement. De vereisten vanuit de algemene inkoopvoorwaarden ICT SaaS, architectuur en IB&P worden dan ingebed bij inkooptrajecten en afspraken met leveranciers. Gezamenlijk vormen zij een integraal kader dat kan worden toegepast bij het verantwoord en optimaal inzetten van Cloudoplossingen bij UWV-dienstverlening.

3.1. Richtinggevende principes

In lijn met het Rijksbrede beleid voor publieke cloudoplossingen wordt een aantal uitgangspunten benoemd dat richting geeft bij het toepassen van de cloudoplossingen. Deze zijn:

- Het rubriceringsniveau mag maximaal Departementaal Vertrouwelijk oftewel BBN 2 zijn. Voor informatiesystemen binnen UWV vormt BBN2 het uitgangspunt. Voor deze classificatie is standaard een cloudoplossing toegestaan;
- Passende, standaard maatregelen moeten getroffen worden;
- Wanneer er persoonsgegevens worden verwerkt, wordt de leverancier gezien als verwerker zoals bedoeld in het kader van de AVG;
- De clouddienst dient te passen binnen bestaande wet- en regelgeving, beleid en architectuur.
- De BIV-classificatie dient toegepast te worden voor de classificatie van gegevens die worden verwerkt binnen de cloudoplossing;
- Verder is cloud een vorm van outsourcing en is het beleid aangaande outsourcing bij UWV ook op cloudoplossingen van toepassing.

- De combinatie van clouddienst, -leverancier¹² en de inrichting¹³ door UWV moeten alle voldoen aan de richtinggevende principes.

Specifiek voor cloud dient verder te worden uitgewerkt:

- Het opnemen van de dienst in het Register van uitbesteding ('cloudregister') en het onderhouden van een volledig dossier met daarin geadresseerd de risico's zoals opgesomd in 'Handreiking risicobeheersing public clouddiensten, concept, versie 0.99, 31 maart 2022'.

3.2. Organisatie

De organisatie dient te worden ingericht en versterkt, zodat het de uitdagingen die cloudtechnologie met zich meebrengt kan aangaan, de voordelen kan benutten en risico's kan mitigeren tot aan acceptabel niveau. Het volgende wordt geborgd:

- UWV volgt het generieke inkoopproces voor de verwerving van een clouddienst, maar dient een aantal punten verder uit te werken zodat het inkoopproces voldoet aan de eisen zoals gesteld in het Rijksbrede cloudbeleid en er aandacht is voor de specifieke risico's die cloud met zich meebrengt. De volgende aspecten verdienen extra aandacht:
 - het opstellen van een risicoassessment dat verfijnd moet worden naar cloud-specifieke aspecten,
 - het opstellen van een duidelijke bedrijfsarchitectuur met de nadruk op integratie van de clouddienst in het UWV landschap,
 - een duidelijke vastlegging van taken, verantwoordelijkheden en bevoegdheden ten aanzien van proces, systeem, mens en data, inclusief de rol van de cloudleverancier en/of de cloud broker hierin meenemend¹⁴
 - beschrijving hoe de cloudoplossing integreert binnen UWV's security architectuur (o.a. toegangsbeheer, logging/monitoring)
 - inregelen van een exit-strategie, risicospreiding en/of escrow
- Een Cloud Center of Excellence (CCoE)¹⁵ wordt 'virtueel' ingericht om kennis en ervaring te bundelen en deze in te zetten en te delen in de organisatie en om verandering richting cloud teweeg te brengen en te ondersteunen.
- De Architectuur Board (met aanvulling van kennishouders) beoordeelt het Programma van Eisen op cloud-relevante aspecten. De Architectuur Board is daarmee kaderstellend voor het Programma van eisen.
- CIO-Office (LM) houdt een cloudregister bij met materieel publiek cloudgebruik en de risico's daarvan.
- Een partij is verworven in de rol van cloud broker – voor UWV is dit DXC¹⁶. Deze partij kan het gebruik, de performance en de levering van clouddiensten beheren en daarmee de complexiteit van het beheren van meerdere cloudoplossingen voor UWV als gebruikersorganisatie afschermen. Grofweg ligt de verantwoordelijkheid van beleid en eisen aan de architectuur (cloud governance) bij UWV, maar de technische uitwerking, implementatie en beheer van cloudoplossingen bij de cloud broker.
- De best practices van een cloud governance framework¹⁷ worden gebruikt. Dit type raamwerk biedt richtlijnen, documentatie en hulpprogramma's bij het maken en implementeren van bedrijfs- en technologiestrategieën voor de cloud. Uitdagingen in deze context zijn:

¹² Er kan sprake zijn van méér dan één leverancier of meerdere onderaannemers. Bijv. de partij die de SaaS-dienst aanbiedt en de leveranciers van onderliggende SaaS, PaaS en IaaS-diensten. Eenieder dient te voldoen.

¹³ Een clouddienst is generiek, maar biedt vaak ruimte voor een specifieke inrichting door de afnemer, afhankelijk van de dienst en het leveringsmodel. De wijze van inrichting, als ook de integratie met UWV-systemen, bepaalt mede of het gewenste beveiligingsniveau wordt gehaald.

¹⁴ DXC is reeds gecontracteerd voor deze rol m.b.t. de IaaS en PaaS leveringsmodellen, exclusief SaaS.

¹⁵ Bron: [How to Build a Cloud Center of Excellence \(CCoE\) | Gartner](#)

¹⁶ Bron: [Cloud broker - Wikipedia](#).

¹⁷ Bron: [Cloud Management and Governance \(gartner.com\)](#)

- o kostenmanagement en budgettering, financiën inzichtelijk hebben en in control zijn over de uitgaven, additionele implementatie van controls die andere leveringsmodellen adresseren
- o nieuwe business en IT rollen om risico's te beheersen en diensten te integreren
- o transparante interactie tussen afnemer en aanbieder
- o overbruggen van tekortkomingen in kennis en besluitvorming over architectuur- en technologiekeuzes
- o ontbreken van operationele kennis en support, van 'IT Operations' naar 'Cloud Operations'.¹⁸

3.3. Informatiebeveiliging en Privacybescherming

Het informatiebeveiligingsbeleid van het UWV vindt zijn basis in wet- en regelgeving. De beveiligingseisen aan cloudoplossingen zijn niet anders zijn dan bij on-premise, maar door de aard van een clouddienst liggen de risico's echter anders dan bij de traditionele (oftewel on-premise) oplossingen¹⁹:

- Zo is de mate van directe invloed op de genomen beveiligingsmaatregelen bij de cloudleverancier beperkter dan bij on-premise oplossingen (in eigen hand).
- En is het zicht en de invloed op de implementatie van beveiligingsmaatregelen bij clouddiensten lastiger.

Compliance met deze maatregelen zal daarom meer moeten rusten op algemene certificeringen en verklaringen van onafhankelijke auditors. Om alsnog beheerst publieke cloudoplossingen in te zetten bij UWV-dienstverlening, worden de volgende uitgangspunten vanuit IB&P gehanteerd, naast de reeds door UWV gehanteerde IB&P kaders:

1 - UWV houdt zich aan de wet- en regelgeving aangaande de verwerking van gegevens

Opslag en verwerking van privacygevoelige gegevens vindt plaats binnen de Europese Economische Ruimte (EER). Dit gebeurt op basis van het principe 'pas toe of leg uit'. Buiten de EER moeten extra maatregelen worden genomen om aan de verplichtingen van de AVG te voldoen (tenzij er een adequaatheidsbesluit is afgegeven door de European Data Protection Board). Wat betreft bedrijfsgevoelige gegevens dient ook in ogenschouw genomen te worden dat aan de Archiefwet wordt voldaan (dus tijdige vernietiging van de gegevens – wat ook geldt voor de persoonsgevoelige gegevens).

- Bij het verwerken van persoonsgegevens, dient eerst een Gegevensbeschermingseffectenbeoordeling (GEB) op het proces te worden uitgevoerd, waarbij de cloudoplossing wordt gebruikt;
- Opslag en verwerking van privacygevoelige gegevens vindt plaats binnen de EER
- Gegevens worden niet langer gebruikt dan noodzakelijk voor het uitvoeren van een wettelijke taak (conform de Archiefwet, de Selectielijst UWV 2014 en de AVG)
- UWV voert geen basisregistratie²⁰ en is geen bron van gegevens voor een basisregistratie. Indien dit in de toekomst wel het geval is, mag in principe geen gebruik worden gemaakt van clouddiensten als het gaat om een basisregistratie.
- De voorwaarden rond opslag en verwerking van gegevens door clouddiensten vanuit het UWV-perspectief worden als volgt samengevat:

Soort gegevens	BBN	Verantwoordelijke	Naar CIO	In publieke cloud?	Anders besluit door	Toezicht
Staatgeheime informatie	3	N.v.t	N.v.t	N.v.t	N.v.t	N.v.t
Persoonsgegevens	2	UWV	Rapporteur - negatief advies GEB-check/rapport	Ja, mits voldaan aan IB&P-beleid	RvB	FG UWV en CIO UWV

¹⁸ Dit gat wordt opgevuld door de cloud broker.

¹⁹ Bron: [Cloud computing and the internal audit function](#)

²⁰ Bron: <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/10-basisregistraties/>

			- Hoog (rest)risico('s) uit risico-analyse			
Bijzondere persoonsgegevens	2	UWV	Rapporteur - positief advies GEB-check/rapport - (rest)risico('s) uit risico-analyse	Nee, tenzij voldaan aan IB&P-beleid met uitleg	RvB	FG UWV en CIO UWV
Basisregistratie	3	N.v.t.	N.v.t	N.v.t	N.v.t	N.v.t

2 - Mogelijke risico's moeten zijn geïdentificeerd, geanalyseerd en waar mogelijk gemitigeerd en aantoonbaar beheerst.

Hierbij zijn de te beschermen belangen en de BIV-classificatie leidend. Vertrekpunt is dat de organisatie inschat hoe kritiek de eigen processen zijn en de bijbehorende data die daarin verwerkt wordt. Uiteindelijk gaat het erom welk risico de organisatie bereid is te nemen – hiervoor zal dan ook een risicoanalyse gedaan moeten worden. Veel gehanteerde frameworks zijn de ISO 31000, de ISO 27005 en de IRAM-methodiek. De ISO 31000 en ISO 27005 zijn voor risicomanagement breed geadopteerd binnen UWV. CISO-Office heeft op basis van deze frameworks een risicomanagementmethodiek ontwikkeld die toegepast kan worden voor het analyseren van risico's bij de inzet van cloud.²¹

Op hoofdlijnen bestaat deze risicoanalyse uit de volgende stappen:

- Doel bepalen o.b.v. context en assets
- Risico-identificatie en classificeren (groot/klein)
- Risicoanalyse en bepalen al dan geen maatregelen treffen
- Risico-evaluatie en –behandeling m.b.t. effectiviteit en efficiëntie
- Afronden van het assessment d.m.v. communiceren en rapporteren

Alle risico's worden in bovenstaande methodiek systematisch beoordeeld. Hierbij moet per risico vastgesteld worden hoe dit risico beheerst wordt en of de geïdentificeerde en getroffen beheersmaatregelen afdoende zijn.

3 - UWV maakt gebruik van leveranciers die passende technische en organisatorische informatiebeveiligingsmaatregelen treffen

Voor informatiesystemen waarbij het te beschermen belang op BBN3 wordt ingeschaald, zijn sterk risico-mitigerende maatregelen noodzakelijk indien gebruik wordt gemaakt van de public cloud. Echter kan algemeen worden gesteld dat het te beschermen belang binnen UWV op BBN2 kan worden ingeschaald. Voor passende technische en organisatorische maatregelen is de IB&P-wijzer van belang. Dit is het verplichte informatiebeveiligingsbeleid. De IB&P-wijzer maakt de vertaalslag van BIO-maatregelen naar concrete beveiligingsmaatregelen (controls) die kunnen worden toegepast als set aan eisen voor het verwerven en gebruik van clouddiensten, vanuit de optiek van de afnemer, UWV. De 31 controls van de IB&P-wijzer (die onder andere gebaseerd is op de NIST, BIO, SSD) moeten terugkomen in contractuele afspraken tussen Cloud Service Consumer (CSC, dus UWV) en Cloud Service Provider (CSP) en deze moeten periodiek hertoetst worden. UWV neemt de 31 maatregelen uit de IB&P-Wijzer als basis voor de inrichting van controls bij Inkoop en Leveranciersmanagement.

- Wet- en regelgeving is verplicht om toe te passen, de IB&P-wijzer helpt om IB&P-maatregelen voor de leverancier te herleiden uit deze wet- en regelgeving;
- Naast de IB&P-wijzer kunnen diverse handreikingen en kaders gebruikt worden om tot passende organisatorische en technische maatregelen te komen, zoals o.a.
 - Handreiking risicobeheersing public clouddiensten, concept, versie 0.99, 31 maart 2022',
 - Uitwerking BIO Thema Clouddiensten²² en

²¹ Voor de risicomanagementmethodiek: https://samenwerken.sharepoint.uwv.nl/sites/DWU/ConcernICT/IBenP/CISO-Office/_layouts/15/start.aspx#/SitePages/4.%20Risicomanagement/Risicomanagement.aspx

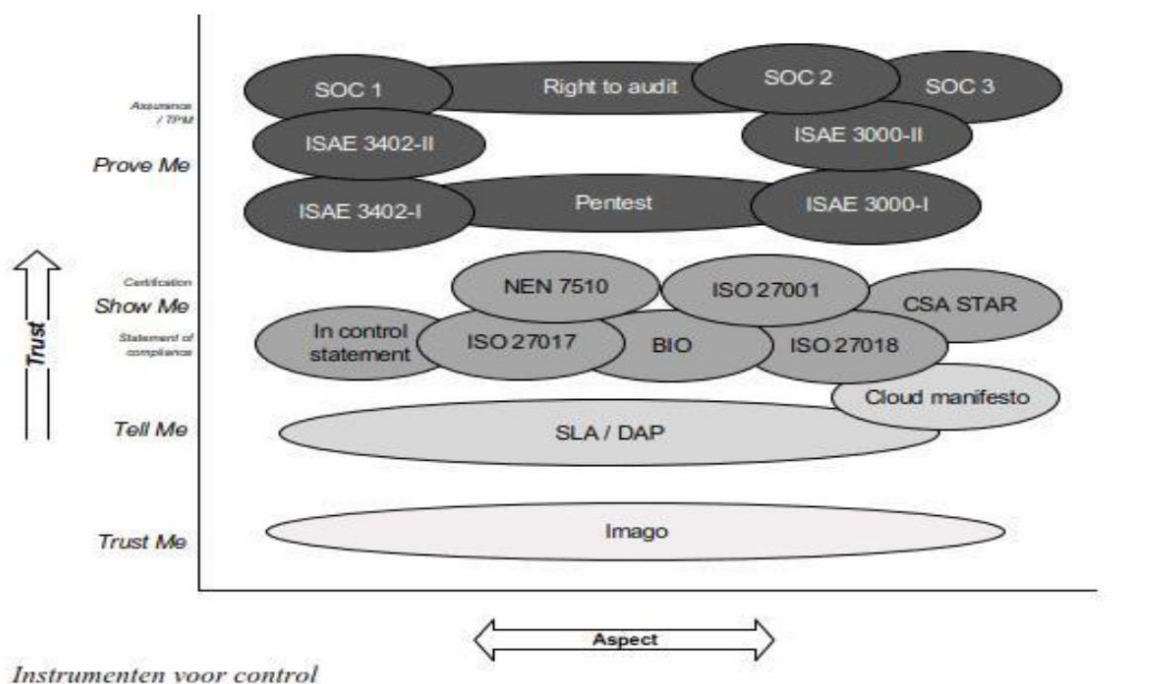
²² [BIO Thema-uitwerking Clouddiensten - NORA Online](#)

- Handreiking Cloud Computing voor overheden.²³

4 - UWV zorgt voor een duidelijke vastlegging van taken, verantwoordelijkheden en bevoegdheden ten aanzien van proces, systeem, mens en data met de cloudleverancier

Verantwoordelijkheden moeten duidelijk belegd zijn – waarbij al eerder is gesteld in dit document dat UWV eindverantwoordelijke is. Afspraken over taken, verantwoordelijkheden en bevoegdheden (voor zover al niet vastgelegd in de standaardvoorwaarden van de cloudleverancier) kunnen worden vastgelegd middels een beveiligings- en verwerkersovereenkomst (BVO) en/of een Service Level Agreement (SLA).

- Afspraken over taken, verantwoordelijkheden en bevoegdheden tussen UWV en leverancier zijn schriftelijk overeengekomen.
- Er dient rekening te worden gehouden met het feit dat als een clouddienst wordt geleverd door een derde de contractuele bepalingen niet alleen met de contractant “de verwerker” maar ook door al haar onderaannemers aantoonbaar moeten worden onderschreven.
- Controls zijn of worden ingericht die de naleving hiervan toetsen. Instrumenten voor control zijn aangegeven in de volgende figuur:



5 - UWV zorgt voor inbedding van de vereisten voor informatiebeveiliging vanaf het eerste moment bij de selectie én inrichtingskeuzes voor de cloud.

Dit uitgangspunt heeft een grote samenhang met uitgangspunt 5 van architectuur. Gedurende aanbestedingen en andere inkooptrajecten is het van belang IB&P te consulteren wat betreft passende maatregelen. Eerste aanspreekpunt bij een organisatieonderdeel is de Business Security Officer.

- Betrek IB&P vanaf het eerste moment bij de selectie en inrichtingskeuzes voor de cloud.

3.4. Architectuur

Inzet van cloud is in haar algemeenheid in lijn met de ICT-principes. Tevens dienen de inrichting en/of implementatie van cloudoplossingen gebaseerd te zijn op deze principes of een afweging hiervan. In onderstaand overzicht zijn de principes die het meest relevant zijn bij de toepassing van cloud bij UWV, aangegeven met een korte toelichting en verdere uitwerking in de context van cloudgebruik. Zo slaan we een brug tussen architectuurprincipes en de inzet van cloudoplossingen.

²³ [Handreiking CloudOverheden Taskforce LR 1](#)

1 - UWV stelt stabiliteit, continuïteit en informatiebeveiliging voorop

Een stabiel, betrouwbaar en toekomstbestendig ICT-landschap is een belangrijke voorwaarde voor de uitvoering van onze maatschappelijke taak en het bieden van de persoonlijke dienstverlening. Standaardisatie is een basisprincipe in de cloud dat inherent stabiliteit levert in het applicatielandschap (beperking van configuratiemogelijkheden en geen afwijkingen). De continue updates door de leverancier waarborgen de continuïteit.

In de geest van dit architectuurprincipe stellen we:

- Basisprincipes als security-by-design en availability-by-design dienen bij de cloudleverancier aantoonbaar hoog in het vaandel te staan²⁴ en in de architectuur van zowel de clouddienst als in de totale (hybride) cloudoplossing, de inrichting van en koppelingen met de clouddienst, duidelijk aanwezig te zijn. Dit laatste duidt op een gedeelde verantwoordelijkheid, waarin UWV een (eind)verantwoordelijkheid heeft om met een gepaste architectuur en capabele organisatie (governance) te komen die deze basisprincipes nastreeft.
- Wanneer gekozen wordt voor een cloudoplossing (XaaS, zowel public als private cloud), dient de standaardisatie (functies, processen, etc.) te worden omarmd, geaccepteerd; er is geen ruimte voor maatwerk of afwijkende vraag op het gebodene (de functionele baseline van de clouddienst), daar waar bij een on-premise installatie die optie vaak nog wel bestaat, middels een aparte aangepaste versie van het product of een sterk (niet-geüpdatete) verouderde versie. UWV zal haar processen willen en moeten aanpassen aan de standaard processen van de clouddienst (en bij geringe afwijking niet willen terugvallen op maatwerkoplossingen). Dit geldt vooral voor public SaaS-diensten.
- Wanneer gekozen wordt voor een on-premise oplossing (maatwerk of pakketinstallatie), dient de implementatie wel te landen in UWV's private cloud, dus sterk gestandaardiseerd en cloud-native²⁵. Dit borgt compatibiliteit met en portabiliteit naar de public cloud²⁶, om integraties en eventuele latere migraties te vergemakkelijken. Een applicatie laten landen op een (Kubernetes) container platform of op een private/public-compatibele cloud stack²⁷ helpt hierbij. Het softwarevoortbrengingsproces en de private cloud als landingszone wordt ook zodanig ingericht dat UWV cloud-native applicaties ondersteunt en alleen ondersteunt/toelaat.

2 - UWV kiest voor tijdig en geleidelijk vernieuwen

Dit principe ondersteunt de ambitie om meer proactief dan reactief te vernieuwen en dit op een beheersbare manier te doen. Het brengt de portfolio in balans en geeft focus op de langere termijn. Cloudproducten worden continu en evolutionair geüpdatet, waardoor UWV 'automatisch' meelift, maar ook dient UWV zijn applicatielandschap mee te laten bewegen in de lijn der vernieuwing. Door het gebruik van een diversiteit aan clouddiensten neemt de footprint van een 'eigen' datacenter af, en daardoor de noodzaak van een intensieve, risicovolle datacenter-migratie. Tijdig en geleidelijk vernieuwen en innoveren worden meer intrinsieke eigenschappen van het ICT-landschap.

In de geest van dit architectuurprincipe stellen we:

- UWV kiest ervoor om een applicatie pas te vervangen door een eventuele cloudoplossing wanneer deze end-of-life is, mits dit het best passende aanbod uit de markt is. End-of-life kan zijn omdat de applicatie niet meer ondersteund wordt of omdat ingrijpende functionele of architecturale wijzigingen noodzakelijk zijn waarvan de kosten niet meer opwegen tegen de baten (zie verder Bijlage B).
- We hanteren het principe SaaS boven PaaS boven IaaS. Bij voorkeur kiezen we voor public SaaS-oplossingen, tenzij de marktverkenning aangeeft dat er onvoldoende aanbod is. In dit

²⁴ Aan de hand van (audit-)rapportages over de diverse instrumenten genoemd in voorgaand figuur onder paragraaf 3.3 kan een beeld hiervan worden gevormd.

²⁵ [Cloud Native Computing Foundation](#): Cloud-native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach. These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.

²⁶ Dit houdt o.a. in dat de applicaties blijven/meelopen met de laatste versies van de cloudstack, wat nu binnen het UWV's softwareontwikkel-/onderhoudsproces niet geborgd is, met intensief groot onderhoud tot gevolg.

²⁷ Op IaaS niveau heeft Microsoft Azure Stack dat een Azure-compatible platform creëert in een Private Cloud, AWS adverteert met AWS Outposts. OpenStack is een open source variant.

geval kiezen we voor PaaS boven IaaS en public cloud boven private cloud en vermijden we non-cloud installaties.

- Een SaaS-oplossing ontzorgt het meest: UWV hoeft geen infrastructuur te regelen, geen software-installaties te verzorgen en geen onderhoudsinspanning te leveren t.b.v. updates, patches, doorontwikkeling, beveiliging of capaciteit (opschaling).
- Een SaaS oplossing biedt echter geen ruimte voor maatwerk, dan alleen configureren. Als er geen aanbieder in de markt is met een SaaS-oplossing die de gewenste functionaliteit levert, dan zou een 'lagere' vorm gekozen kunnen worden en dient UWV de functionaliteit zelf te ontwikkelen. Maar mocht de functionele dekkingsgraad hoog genoeg zijn, kies dan voor de standaard SaaS oplossing en accepteer de 'tekortkomingen' (en pas je hierop aan).
- Als er geen SaaS-oplossing voor handen is, kies dan voor een PaaS-oplossing. Ontwikkelaars krijgen dan een platform, waar ze zelf aan de slag kunnen met het testen, uitrollen en verder optimaliseren van software. Wanneer je gebruik maakt van PaaS regelt de leverancier de infrastructuur (IaaS) maar ook de besturingssystemen en middleware, als ontwikkelaar heb je daar geen omkijken naar en kan worden geconcentreerd op het ontwikkelproces zelf.
- Mocht een PaaS-platform niet voldoen, dan kan gekozen worden maatwerk te leveren op een IaaS platform. Je hebt meer controle, maar vaak ook meer werk om een applicatie te ontwikkelen en te installeren op virtuele servers in een netwerk. Vaak wordt voor IaaS gekozen in een lift-and-shift migratiestrategie van legacy systemen.

3 - UWV richt innovatie met ICT primair op het realiseren van zijn opdracht en bedrijfsdoelstellingen

Ons doel om cliënt en medewerker voorop te stellen rechtvaardigt zowel functionele als technische innovatie. Innovatie vindt steeds meer plaats in de cloud, de markt beweegt zich af van on-premise oplossingen en installaties. We stellen specifiek:

- UWV zal een hybride cloudarchitectuur nastreven, waarin (vooralsnog) on-premise legacy systemen, private cloud en public cloud applicaties worden geïntegreerd, zoveel mogelijk naadloos met standaard componenten en interfaces.
- Voor wat betreft keuzen in PaaS en IaaS diensten zal de vrijheidskeuze beperkt moeten zijn om een complexe hybride cloudarchitectuur te voorkomen. Daarmee stelt UWV eenvoud en innovatiekracht boven lock-in.

4 - UWV kiest voor security & privacy by design/default

UWV past informatiebeveiliging en privacy-borging toe bij het ontwerpen en inrichten van processen en systemen. Dit wordt ook wel security & privacy by design/default genoemd en wordt toegepast bij zowel nieuwbouw, verbouw als evaluatie en is afgeleid van het tactisch en strategisch beleidskader. In lijn met dit principe passen cloudleveranciers in het algemeen security-by-design toe en maken cloud niet minder veilig dan on-premise.

- De beveiligingseisen aan cloudleveranciers en –diensten en aan de totale oplossing (koppelingen e.d.) zijn niet anders dan wat UWV nu eist aan een on-premise oplossing. Wel is de invulling anders, op het gebied van maatregelen (en mogelijkheden). De gestelde eisen met de genomen maatregelen moeten ook verifieerbaar zijn en aangetoond worden door de cloudleverancier. Zie verder paragraaf 3.3.
- Generieke infrastructuur en met name de beveiligingsmaatregelen zullen conform BIO BBN2 centraal worden aangebracht, specifiek voor beveiligingsdiensten als data protectie en cryptografie, end-point protection, identiteit en toegang (IAM), monitoring, (security) logging. Standaard koppelvlakken worden ingericht t.b.v. afstemming, synchronisatie en federatie met clouddiensten.

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

Dit principe stelt in algemene zin dat we kiezen voor partners waarvoor deze dienstverlening core business is en die continuïteit en marktconformiteit kunnen garanderen, zodat UWV zich kan concentreren op zijn core business en functionele regievoering. In lijn met dit principe stellen we vast:

- Cloud is een gepaste vorm van outsourcing voor UWV (standaardisatie van infra en applicaties), mits voldaan wordt aan de gestelde randvoorwaarden op het gebied van IB&P.
- UWV heeft DXC als cloud broker verworven die een belangrijke rol speelt in het inrichten en beheren van een hybride cloudarchitectuur met daarin geïntegreerd on-premise legacy systemen en private/public IaaS en PaaS platformen, het landen van applicaties in de private cloud of public cloud op IaaS en PaaS platformen en het koppelen van en met public SaaS clouddiensten.

6 - UWV bouwt aan een wendbaar en beheersbaar ICT-landschap

Wij werken onder architectuur aan vereenvoudiging en wendbaarheid van het ICT-landschap om sneller te kunnen reageren op veranderingen. Met gestandaardiseerde, ontkoppelde en vervangbare bouwblokken creëren we een wendbaar en beheersbaar landschap, zowel in infrastructuur als applicaties. Hierop voortbordurend, stellen we specifiek:

- Een juist gebruik en inrichting van hybride cloudtechnologie draagt bij aan de ont koppeling en beheersing van de gekoppelde clouddiensten.
- Het hanteren van een cloud adoption/governance framework²⁸, inrichting van een 'cloud center of excellence' (CCoE) en educatie van medewerkers draagt bij aan een wendbaar en beheersbaar ICT-landschap in de cloud en vormen de sleutel voor een succesvolle uitvoering van het cloudbeleid. Een cloud adoption framework biedt richtlijnen, speciaal ontworpen om te helpen de juiste bedrijfs- en technologiestrategieën te ontwikkelen en te implementeren om succesvol in de cloud te werken. Zo'n plan biedt best practices, documentatie en hulpprogramma's die cloudarchitecten, IT-professionals en zakelijke besluitvormers nodig hebben om hun doelstellingen voor korte en lange termijn te realiseren. De inrichting van een CCoE is zo'n best practice, een multidisciplinair team²⁹, om kennis en kunde rond het thema cloud te centraliseren en uit te dragen naar de rest van de organisatie.
- Er wordt door UWV slechts één operationeel model gehanteerd voor de operatie, beheer en regie van het gebruik van public cloud en dit operationeel model is UWV-breed afgesproken en gedragen. Dit operationele model definieert bij welke organisatieonderdelen en teams welke ITIL-activiteiten en verantwoordelijkheden zijn belegd.
- Er is een UWV-breed gedragen financieel model en bijbehorend proces voor cost-accounting (en beheersing hiervan) voor het gebruik van public cloud services.
- Op de infrastructuur-/platformlaag (in deze context betreft het private/public IaaS/PaaS modellen) wordt verregaande standaardisatie doorgevoerd. Standaardiseer en beperk de mogelijkheden – voorkom wildgroei en schaduw IT - wat betreft de inrichting van deze laag ten behoeve van wendbaarheid en beheersbaarheid

7 - UWV realiseert ICT met bewezen technologieën

Bewezen technologieën zorgen voor lagere risico's en betere voorspelbaarheid. UWV hanteert technologiebeleid waarop getoetst wordt in het architectuurproces. Hiertoe rekenen wij overigens

²⁸ Voorbeelden:

- [OpenGroup Cloud Governance Framework](#)
- [Weolcan Cloud Governance](#)
- [Microsoft Cloud Adoption Framework voor Azure](#)
- [AWS Cloud Adoption Framework](#)
- [ISO - ISO/IEC 17789:2014 Cloud Computing Reference Architecture](#)
- [Cloud Security Alliance \(Cloud Controls Matrix\)](#)

²⁹ Bron: [How to Build a Cloud Center of Excellence \(CCoE\) | Gartner](#)

Bron: [Cloud Center of Expertise - Cloud Governance \(weolcan.eu\)](#)

Het is een centraal ingericht team dat de cloudarchitectuur implementeert en decentrale teams (divisies) faciliteert en adviseert, maar zeker niet namens de decentrale teams bedrijfsoplossingen implementeert. Te denken valt aan de volgende samenstelling:

- Een vertegenwoordiger van Enterprise Architectuur (voorzitter)
- Een vertegenwoordiger van Leveranciersmanagement
- Een vertegenwoordiger van ICT Services (de Lead Architect)
- Een vertegenwoordiger van CISO/IB&P
- Een vertegenwoordiger van de Cloud Broker
- Een aantal Cloud Architecten / Engineers (van UWV en Cloud Broker)

ook technologieën op basis van overheids-, open- en marktstandaarden. In lijn hiermee zeggen we:

- Cloud in vele vormen is inmiddels een bewezen technologie.
- UWV gaat in zee met cloudleveranciers die zich bewezen hebben. De afspraken die SLM Rijk maakt met cloudleveranciers zijn ondersteunend in de keuzes van UWV³⁰.

8 - UWV verkiest hergebruik boven standaardoplossingen; standaardoplossingen boven maatwerk

Bij het (her)invullen van functionele wensen geldt bij het maken van een keuze als prioritering: 1) hergebruik; 2) standaardoplossing; 3) maatwerk. Onder hergebruik wordt herhaalde inzet van middelen en functionaliteiten uit de UWV-organisatie verstaan, maar ook die van keten- en overheidsbrede bouwstenen. Clouddiensten zijn per definitie standaard bouwblokken. Ze zijn immers ontworpen voor en worden geleverd aan zoveel mogelijk afnemers.

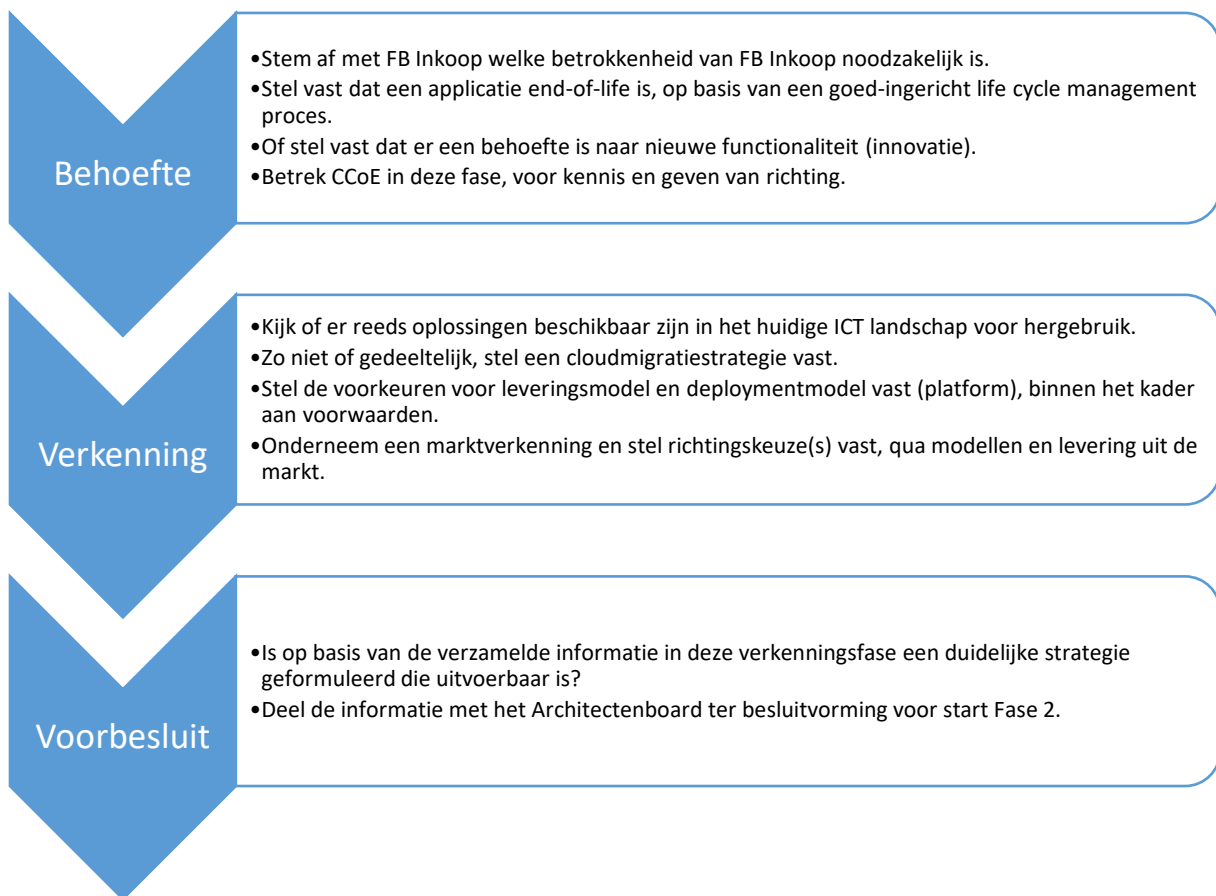
- Dus prefereer hergebruik van bestaande applicaties boven het inrichten van een nieuwe cloudoplossing, tenzij deze end-of-life is. En natuurlijk, hergebruik clouddiensten die reeds in gebruik zijn bij UWV.
- De voorkeur voor standaardoplossingen boven maatwerk is ook geborgd in het beleid '(public) SaaS voor PaaS voor IaaS voor private/on-premise' (zie #2). We kiezen voor een standaardoplossing (SaaS) dat het meest ontzorgt en waar maatwerk nodig is kiezen we voor een platform (PaaS) wat meer ontzorgt en het snelst producten kan releasen.

4. Afwegingskader

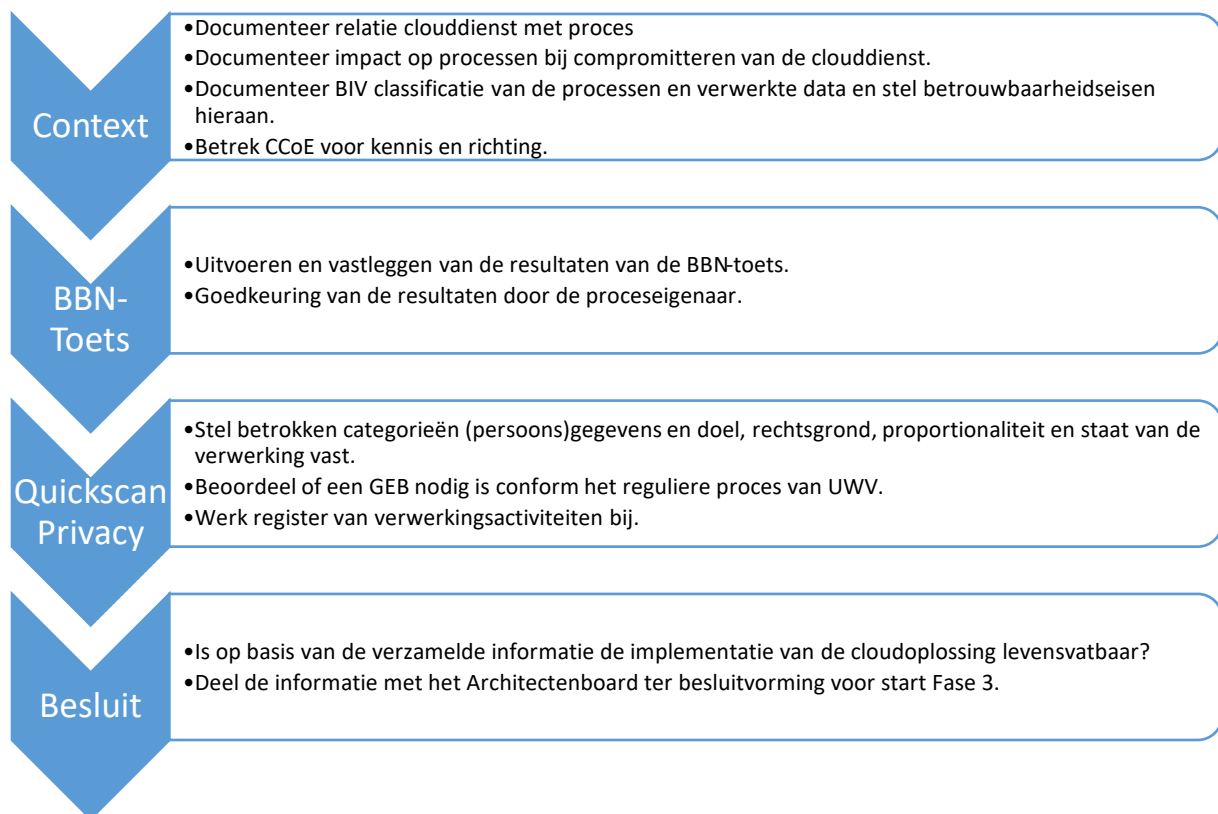
Op basis van het vorige hoofdstuk en de 'Handreiking risicobeheersing toepassing public clouddiensten' (versie 0.99) komen we tot het volgende afwegingskader in de vorm van een aantal stappen voor de verkenning en werving van clouddiensten, ingezet als vervanging van end-of-life applicaties of pure innovatie. Dit afwegingskader zal worden geïmplementeerd in de UWV-organisatie.

³⁰ <https://slmmicrosoftrijk.nl/>

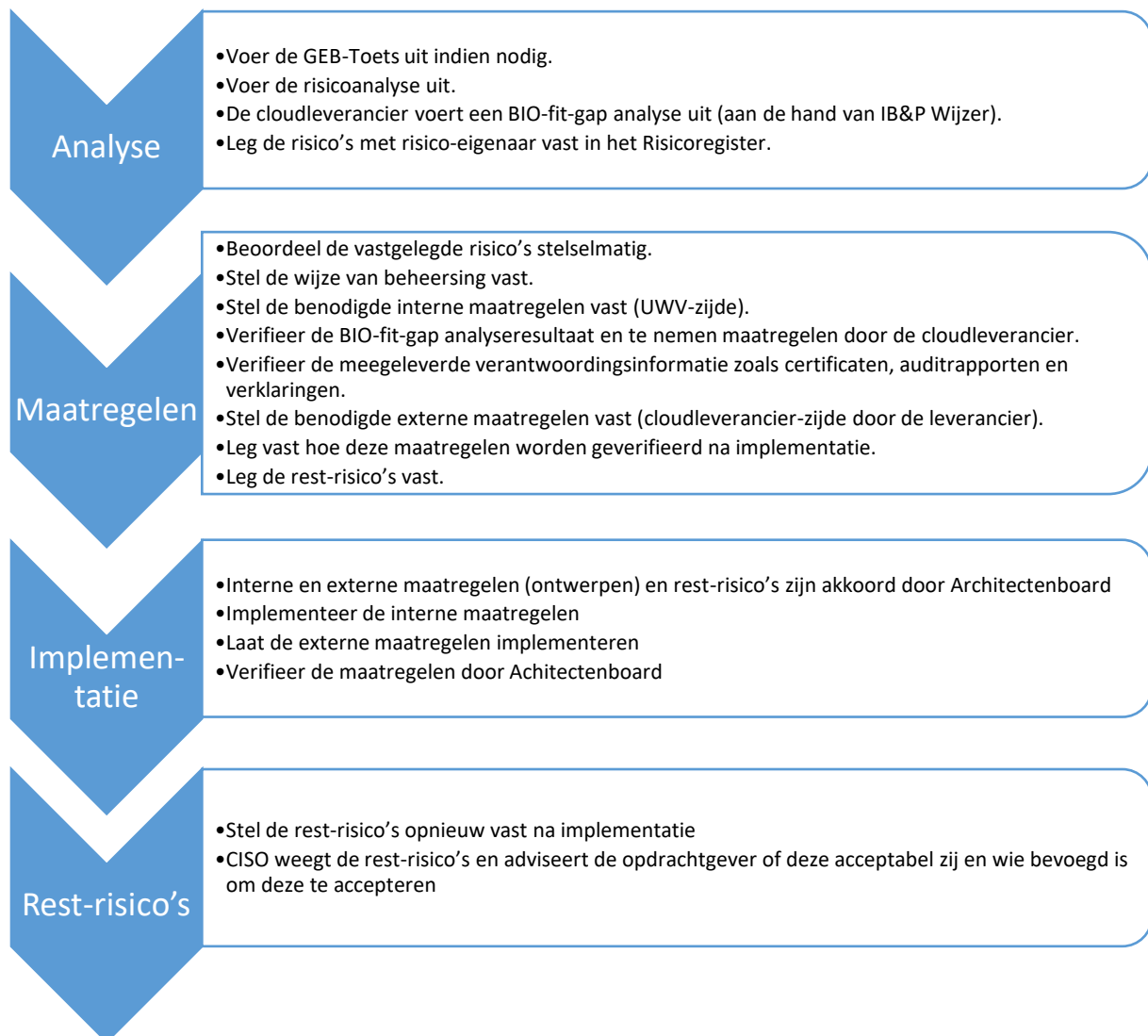
4.1. Fase 1 – Verkenning



4.2. Fase 2 – Snelle risicoscan



4.3. Fase 3 – Inhoudelijke risicoanalyse



A. De Cloud uitgelegd

Zie ook [The NIST Definition of Cloud Computing](#) voor een internationaal geaccepteerde uiteenzetting van Cloud Computing. Dit hoofdstuk volgt de NIST-definitie.

A.1. Definitie en afbakening

De Cloud is een containerbegrip. Cloud Computing is een ontwikkeling die het mogelijk maakt om complexe IT-functionaliteit via een netwerk gebaseerd op internettechnologie (veelal Internet zelf, maar kan ook een privénetwerk zijn) af te nemen. Deze functionaliteit is vergelijkbaar met de functionaliteit die wordt geleverd vanuit applicatie(keten)s die nu in een 'eigen' rekencentrum (in het geval van UWV ge-outsourced aan DXC) geïnstalleerd zijn, maar qua onderliggende architectuur en technologie vaak totaal verschillen.

Met de applicatie zit in de meeste gevallen ook de data die wordt bewerkt in de Cloud. Ook met het migreren van functionaliteit van een eigen (zgn. on-premise) omgeving naar die van een clouddienstverlener gaat meestal de data waar men mee werkt ook mee.

Cloudcomputing is een model voor het mogelijk maken van alomtegenwoordige, gemakkelijke, on-demand netwerktoegang tot een gedeelde pool van configureerbare computerresources (bijvoorbeeld netwerken, servers, opslag, applicaties en services) die snel kunnen worden geleverd en vrijgegeven met minimale beheerinspanning of interactie met de serviceprovider. Dit cloudmodel bestaat uit vijf essentiële kenmerken, drie servicemodellen en vier implementatiemodellen.

A.2. Kenmerken

Cloud computing heeft de volgende kenmerken:

Karakteristieken / kenmerken van Cloud Computing
♦ Elastisch, flexibel en schaalbaar (rapid elasticity and scalability): 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 (on-demand selfservice): Het is mogelijk de dienst af te nemen op het moment dat die gewenst is/er een noodzaak toe is, via een netwerk, zonder de tussenkomst van partijen (zelf doen) en de onderliggende complexiteit te hoeven doorgronden (levering als dienst, niet als een installatiepakket). Selfservice vergroot de wendbaarheid (agility) van de business & IT.
♦ Breed-beschikbare netwerktoegang: clouddiensten zijn beschikbaar over een netwerk van meestal hoge bandbreedte, zoals Internet of een LAN (als naar een Private Cloud). Bandbreedte en vertraging (latency) spelen een grote rol bij de gebruikservaring.
♦ 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). De kosten verschuiven van CAPEX naar OPEX.
♦ Gedeeld met derden (multi-tenancy and resource pooling): Dienstverleners gebruiken de infrastructuur om meerdere cliënten te bedienen. Het delen van infrastructuur en software levert voordelen op financieel vlak en qua flexibiliteit (i.e. de kosten worden over meerdere cliënten gedeeld, en upgrades op het gebied van software en hardware wordt één keer aangepast, voor alle cliënten 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*) met een nog hogere graad van ontzorging, waarbij de voorzieningen/diensten de grote stap van cliënt-specifiek (maatwerk) naar standaard zetten. Vanuit een financieel perspectief is het benutten van schaalgrootte de voornaamste drijfveer. Dit betreft niet alleen het efficiënt gebruik van servercapaciteit (betaal wanneer nodig), maar ook voor compliance, certificerings-, onderhoud- en beheerkosten.

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.

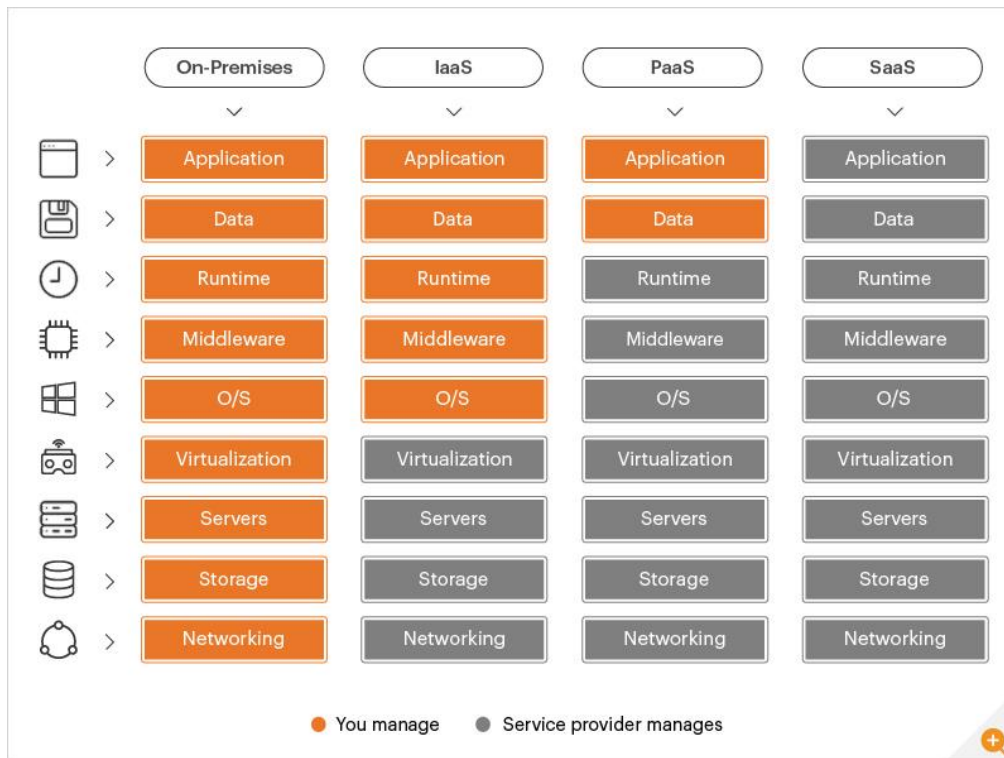
Cloud Computing is inmiddels zeer volwassen geworden en kan worden beschouwd als een de facto. Nieuwe aanbieders, aanbieders van nieuwe functionaliteit, zullen hun systemen bouwen volgens een cloudarchitectuur en de functionaliteit alleen aanbieden als 'as-a-service', de on-premise variant is commercieel niet interessant. Dit wordt ook erkend door bestaande aanbieders, die zelf een transitie maken naar Cloud en/of hun functionaliteit aanbieden als een service, terwijl de on-premise variant richting end-of-life gaat.

A.3. Leveringsmodellen

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.

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: Microsoft Azure, Google Cloud, Amazon EC2 & S3, GoGrid en Rackspace Cloud (zij beiden overigens ook PaaS- en SaaS-diensten aan).
- **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, en Tibco Silver, low-code, container en serverless platforms, maar ook IaaS providers bieden PaaS componenten aan, vaak als abstractie op hun IaaS laag (b.v. Azure SQL Database).
- **SaaS:** *Software as a Service* is het meest vergaande leveringsmodel. Hierbij bestaat de dienstverlening uit een kant-en-klare applicatie, waar maatwerk niet mogelijk is dan alleen middels beschikbare configuratie. Voorbeelden zijn: Basecamp, Dropbox, Google Apps, Microsoft OneDrive en Salesforce.com.



De grens van beheer en verantwoordelijkheden schuiven van een on-premise naar een SaaS situatie (van links naar rechts) meer en meer op richting de leverancier. Daarbij neemt de graad van standaardisatie toe en neemt de mogelijkheid tot implementeren van maatwerk af. Waar je als organisatie in de klassieke on-premise situatie volledig in control bent over je ICT-voorziening, maatwerk kan toepassen, maar ook alles moet beheer, neemt de SaaS variant je alles uit handen en dien je de standaard aanbieding van de dienst te accepteren.

UWV dient ermee rekening te houden dat al deze leveringsmodellen zullen en blijven worden afgenomen in de (nabije) toekomst.

A.4. Deploymentmodellen

Haaks op de leveringsmodellen kent cloud computing een aantal deploymentmodellen:

- **Public Cloud:** cloud computing is bereikbaar voor het publiek, voor individuen en bedrijven. Voorbeelden zijn Gmail, Microsoft 365, Dropbox, Microsoft Azure en Amazon AWS.
- **Community Cloud:** cloud computing is alleen bereikbaar voor en gebruikt door een selecte groep met eenzelfde belang. Voorbeelden zijn Microsoft Azure Germany en Government (US), typisch overheid-specifiek om risico's van een public cloud te mitigeren. Rekening moet worden gehouden dat er ook een EU variant komt en er bestaat Gesloten Rijks Cloud (GRC) waar onder andere Logius DigiD wordt gehost.
- **Private Cloud:** cloud computing dat alleen gebruikt wordt één organisatie, compleet afgeschermd. Voorbeelden zijn private clouds gebaseerd op Microsoft Azure Stack, open source OpenStack, of containerplatform OpenShift.
- **Hybrid Cloud:** cloud computing dat een private cloud combineert met één of meerdere public clouddiensten. Een voorbeeld is Azure VMs verbonden met on-premise infrastructuur via ExpressRoute of site-to-site VPN. Merk op dat Microsoft Azure en Azure Stack naadloos integreren met elkaar, wat het maakt tot een ideaal tandem voor het opzetten van een Hybrid Cloud omgeving.

UWV dient rekening te houden met alle deploymentmodellen en de integratie hiervan, inclusief de (huidige) on-premise omgevingen om de huidige (legacy) applicaties te kunnen blijven draaien.

B. Cloudmigratiestrategie

Het cloudbeleid is niet alleen van toepassing op het werven van nieuwe functionaliteit. UWV dient ook een heldere migratiestrategie uit te werken als het gaat om vervanging van huidige ICT op termijn. Er bestaan grofweg zes migratiestrategieën (6R model), waarin per voorziening een keuze moet worden gemaakt, wanneer deze aangemerkt wordt als end-of-life:

1. Rehost (lift-and-shift)

UWV verhuist een systeem met zo min mogelijk aanpassingen naar het (IaaS) cloudplatform van keuze. Oppakken en de cloud inschuiven. Dit klinkt als een aantrekkelijke keuze: relatief snel klaar met weinig risico. Toch kleeft er een groot nadeel aan deze keuze: de operationele kosten zijn relatief hoog, zeker op de lange duur. Monitor de cloudkosten dus nauwgezet. Daarnaast kost het inrichten van de nieuwe omgeving en het aansluiten van bijvoorbeeld bestaande CI/CD-oplossingen tijd en geld. Meestal betreft deze optie korte termijn en is geen eindstation.

- Pas Rehost toe
 - ✓ bij een grote datacenter migratie
 - ✓ als je nieuw bent met de Cloud (minste impact)
 - ✓ bij off-the-shelf applicaties
 - ✓ als er een strakke deadline is.

2. Replatform (lift-tinker-and-shift)

UWV verandert de functionaliteit van het systeem nog steeds niet, maar het onderliggende platform wel. Een databaseserver met dure licenties verhuizen naar een database-as-a-service leverancier is in meerdere opzichten een hele verbetering. UWV betaalt alleen voor het echte gebruik en is meteen van het beheer van het systeem af (of de outsourcingkosten daarvan). Er zijn vele voorbeelden, in het algemeen betreft het een verhuizing van applicaties van een server omgeving naar een PaaS omgeving. Deze optie biedt UWV niet alleen kansen om het kostenmodel te kantelen, er wordt ook aan wendbaarheid gewonnen, zonder aan de architectuur van systemen te sleutelen.

- Pas Replatform toe
 - ✓ als dat snel moet gebeuren
 - ✓ als je voordelen van de Cloud wil benutten zonder ingrijpende aanpassingen
 - ✓ als je een complexe on-premise applicatie met kleine aanpassingen kan migreren om cloudvoordelen te benutten.

3. Repurchase (naar een ander product)

Deze migratieoptie is om systemen die veel kosten maar weinig opleveren te vervangen door een SaaS-oplossing. Een cluster van mailservers en harde schijven vol met spreadsheets kan vaak worden vervangen door Office 365 of G Suite. Salesforce of Dynamics kan een CRM-systeem vervangen en er zijn genoeg cloud-alternatieven voor een CMS dat nu on-prem draait. Het ontwikkelen van software kost al genoeg tijd, energie en geld. Wees slim en spaar de krachten om systemen te bouwen die UWV onderscheidt in haar overheidsfunctie (core business).

- Pas Repurchase toe
 - ✓ als je applicaties aan het vervangen bent die commodity zijn, standaard bedrijfsfuncties of secundaire processen ondersteunen zoals financy, accounting, CRM, HRM, ERP, Email, CMS, etc.
 - ✓ als een legacy applicatie niet compatibel is met de Cloud.

4. Refactor/re-architecture (maak kernapplicaties cloud-ready)

Deze optie is vaak het meest ingrijpend, maar biedt ook de meeste potentie. UWV maakt met deze strategie optimaal gebruik van wat de cloud te bieden heeft, denk aan ongekende schaalbaarheid voor minimale kosten, het gebruik van services die anders grote materiële en personele investeringen zouden betekenen en/of meer en sneller releasen. Hoe ingrijpend deze strategie is hangt af van de huidige staat van het systeemlandschap en systeem, met name qua modulariteit en stack. De stap naar microservices, containers of serverless zou optimaal zijn in deze strategie. De winst is navenant.

➤ Pas Refactor toe

- ✓ als een applicatie het meest profiteert van / rendeert in de Cloud
- ✓ als een sterke behoefte is aan schaalbaarheid, snelheid en prestatie
- ✓ als een on-premise applicatie niet cloud-ready (incompatibel) is.

5. Retire

Tijdens het plannen en uitvoeren van een migratie komt men altijd wel iets tegen dat met pensioen mag. De winst kan flink oplopen in een aantal systemen.

➤ Pas Retire toe

- ✓ als een applicatie overbodig of redundant is
- ✓ als een legacy applicatie niet cloud-compatibel is en weinig toegevoegde waarde meer heeft
- ✓ als je besloten hebt om een applicatie te 'refactoren' of te 'repurchasen', of de functionaliteit toe te voegen aan een andere applicatie.

6. Retain (doe niks, de nul-optie)

Sommige stukken hoeven niet per se mee naar de cloud binnen een bepaalde termijn. Die doen het prima als ze nog even doorpruttelen op de plek waar ze nu staan. Later kun je ze alsnog migreren, of misschien zelfs uitzetten. Ook als UWV de datacenter migratie achter de rug heeft, is voorlopig iets te laten voor wat het is vaak een goede optie.

➤ Pas Retain toe

- ✓ als je een hybride cloud model hebt geadopteerd
- ✓ als je flink geïnvesteerd hebt in on-premise applicaties (nog niet afgeschreven)
- ✓ als een legacy app niet cloud-ready is en prima werkt on-premise
- ✓ als je besluit om de migratie van een applicatie voor je uit te schuiven.

De migratiestrategie laat de keuze voor deployment in private cloud of public cloud in het midden. Er is reeds gesteld dat een private cloud compatibel moet zijn met de public cloud variant en portabiliteit gewaarborgd is als het gaat om IaaS en PaaS leveringsmodellen. SaaS-oplossingen zijn vooral public cloud.

