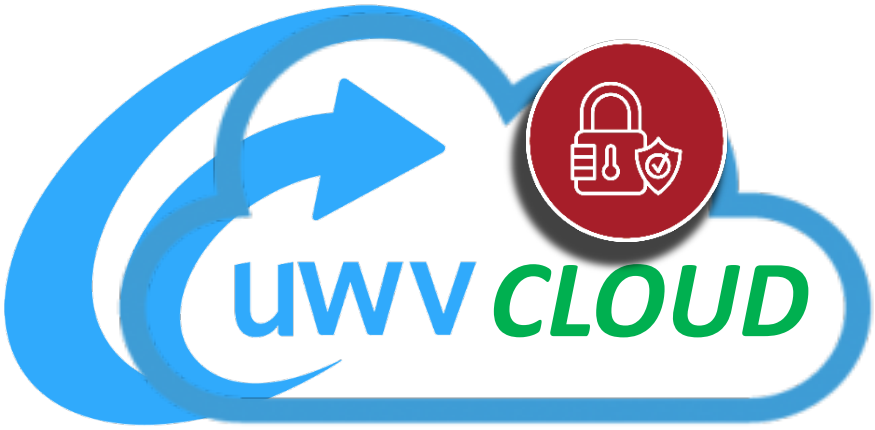


UWV Cloudbeleid 2.0

- RvB Notitie -

Chief Information Officer / Chief Information Security Officer
Versie: 2.0 definitief
Datum: 09-08-2023
Opstellers: 5.1 lid 2 sub e

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). UWV hanteert onverkort het nieuwe Rijksbrede cloudbeleid (inclusief het volgen van de aanpassingen in de toekomst). Op EU-niveau wordt zelfs het uitgangspunt 'cloud-first' gehanteerd, waarbij het gebruik van cloud positief ontvangen wordt mits passend bij de risico's. 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 deze notitie aan de RvB 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.

Inhoud

Managementsamenvatting 2
1. Achtergrond en aanleiding 4
1.1. Wat wordt bedoeld met cloud? 4
1.2. Waarom deze verandering van beleid op cloud? 4
2. Positionering en besturing 4
2.1. Positionering 4
2.2. Besturing 5
2.3. Reikwijdte 5
3. Voorwaarden 6
3.1. Richtinggevende principes 6
3.2. Organisatie 6
3.3. Informatiebeveiliging en Privacybescherming 7
3.4. Architectuur 8
A. De Cloud uitgelegd 10
A.1. Definitie en afbakening 10
A.2. Kenmerken 10
A.3. Leveringsmodellen 11
A.4. Deploymentmodellen 12
B. Instrumenten voor control 12
C. Verklarende woordenlijst 12

Wijzigingshistorie			
Datum	***Versie***	***Actie***	***Status***
13-01-2023	0.1	Eerste versie beleidsnotitie voor RvB opgesteld op basis van Cloudbeleid 2.0.	Draft
16-01-2023	0.2	Review 5.1 lid 2 sub e verdere inkorting.	Draft
24-01-2023	0.4	Bespreking in DT-ICT, enkele aanpassingen in terminologie doorgevoerd.	Draft
13-02-2023 28-02-2023	0.6	Bespreking in RIO en AB, enkele aanpassingen doorgevoerd ter verduidelijking	Draft
03-04-2023	0.8	Afstemming FG.	Draft
20-04-2023	0.82	Bespreking in IV-Board.	Draft
03-05-2023	0.83	Additioneel commentaar CIO verwerkt.	Draft
14-06-2023	0.99	Naar IV-Board als hamerstuk	Draft
29-06-2023	0.999	Naar RvB als hamerstuk	Draft
09-08-2023	2.0	Goedgekeurd door RvB. 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 gevraagd aan overheidspartijen die niet tot de Rijksdienst behoren, het Rijksbrede cloudbeleid te volgen[1]. 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 NIST. Bij 'cloud computing' krijgt men makkelijk en on-demand toegang tot 'computing resources' zoals netwerken, servers, opslag, applicaties en services. Deze resources oftewel bronnen worden beheerd, bijgehouden en vernieuwd door de 'cloud providers'. Gebruikers van de cloud betalen alleen maar voor een specifiek gebruik van die resources[2].

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: Software as a Service (SaaS) - de situatie dat je een volledige applicatie as-is afneemt die in de cloud werkt en zelf geen beheer doet; Infrastructure as a Service (IaaS) - de andere uiterste variant dat je de infrastructuur (hardware, databases, …) uit de cloud afneemt, maar alle IV daarop verder zelf beheert; en Platform as a Service (PaaS) - een tussenvorm, waar een platform, bv een Java, .Net, low-code of ODM/BAW omgeving wordt afgenomen 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 zoals welke leverings- en deploymentmodellen er zijn en welke kenmerken er zijn van Cloud, dan raden we aan om eerst *Bijlage A - De Cloud uitgelegd* op pagina 10 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 voordelen. 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 genoemd[3]. 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 compliancy-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.

Het nieuwe cloudbeleid volgt het Rijksbrede cloudbeleid 2022, 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

[1] Kamerbrief Rijksbreed cloudbeleid, p.2

[2] NIST SP 800-145 The NIST Definition of Cloud Computing

[3] https://digital-strategy.ec.europa.eu/en/library/cloud-and-edge-computing-different-way-using-itbrochure

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[4] van de Europese Commissie (EC) 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 uitgangpunt 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, 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.

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 compliancy aan AVG (GEB-check/rapport) samen met de FG;
- Divisies verifiëren compliancy 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 de 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 cloudleverancier 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.

[4] *https://ec.europa.eu/info/publications/european-commission-cloud-strategy_en*

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, -leverancier en de inrichting 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.
- Een Cloud Center of Excellence (CCoE)[5] 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 DXC[6]. 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

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

[6] Bron: Cloud broker - Wikipedia.

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 framework[7] worden gebruikt ter inspiratie voor het succesvol implementeren van de governance. Dit type raamwerk biedt richtlijnen, documentatie en hulpprogramma's bij het maken en implementeren van bedrijfs- en technologiestrategieën voor de cloud.

3.3. Informatiebeveiliging en Privacybescherming

De beveiligingseisen aan cloudoplossingen zijn niet anders dan on-premise, maar door de aard van een clouddienst liggen de risico's echter anders dan bij de traditionele (oftewel on-premise) oplossingen[8]:

- 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 specifieke uitgangspunten vanuit IB&P gehanteerd, naast de reeds door UWV gehanteerde IB&P kaders:

- Opslag en verwerking van privacygevoelige gegevens vindt plaats binnen de Europese Economische Ruimte.
- UWV voert geen basisregistratie[9] en is geen bron van gegevens voor een basisregistratie. Indien dit in de toekomst wel het geval is, mag geen gebruik worden gemaakt van clouddiensten.
- De voorwaarden rond opslag en verwerking van gegevens door clouddiensten vanuit het UWV-perspectief worden als volgt samengevat:

Soort gegevens	**BBN**	**Verant-woor-delijke**	**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	Rapporteer - negatief advies GEB-check/rapport - Hoog (rest)risico('s) uit risico-analyse	Ja, mits voldaan aan IB&P-beleid	RvB	FG UWV en CIO UWV
Bijzondere persoonsgegevens	2	UWV	Rapporteer - 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.

- De risicomanagementmethodiek ontwikkeld door CISO wordt toegepast voor het analyseren van risico's van de inzet van cloud.[10]

[7] Bron: Cloud Management and Governance (gartner.com)

[8] Bron: Cloud computing and the internal audit function

[9] Bron: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/10-basisregistraties/

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

- UWV maakt gebruik van leveranciers die passende technische en organisatorische informatiebeveiligingsmaatregelen treffen. Hierin is de BIO verplichtend. De afspraken die SLM Rijk maakt met cloudleveranciers zijn ondersteunend in de keuzes van UWV[11].
- Als een clouddienst wordt geleverd door een derde zullen 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 bijlage (B.).

3.4. Architectuur

Inzet van cloud is in haar algemeenheid in lijn met de architectuurprincipes van UWV. De volgende specifieke uitgangspunten worden vanuit architectuur gehanteerd bij de inzet van cloudoplossingen:

- UWV stelt stabiliteit, continuïteit en informatiebeveiliging voorop en dit principe dient bij de cloudleverancier aantoonbaar in de architectuur en werkwijze geborgd te zijn. Aan de hand van (audit-)rapportages over de diverse instrumenten genoemd in voorgaand figuur onder paragraaf 3.3 kan een beeld hiervan worden gevormd. Dit principe is ook van toepassing op de verdere inrichting van de clouddienst waar UWV verantwoordelijk voor is.
- Wanneer gekozen wordt voor een cloudoplossing 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) dan de inrichtingsruimte. 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, cloud-native[12] en continu onderhouden. Dit borgt compatibiliteit met en portabiliteit naar de public cloud, om integraties en eventuele latere migraties te vergemakkelijken.
- 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.
- 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 geval kiezen we voor PaaS boven IaaS en public cloud boven private cloud en vermijden we non-cloud installaties. Dit principe zorgt voor de meeste ontzorging (minder componenten en onderhoud erop), versnelling (sneller beschikbaar hebben van functionaliteit) en innovatie (clouddiensten, en vooral publieke, worden continue doorontwikkeld; private cloud diensten zijn vaak beperkt en lopen achter op de publieke trend).
- 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.
- Generieke infrastructuur en met name de beveiligingsmaatregelen zullen conform BIO BBN2 centraal worden aangebracht, specifiek voor beveiligingsdiensten als data protectie en encryptie, end-point protection, identiteit en toegang (IAM), monitoring, (security) logging. Standaard koppelvlakken worden ingericht t.b.v. afstemming, synchronisatie en federatie met clouddiensten.

---

[11] https://slmmicrosoftrijk.nl/

[12] 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.

- 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.
- 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 operationeel 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

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 zes 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 aan wie 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 driver. 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.

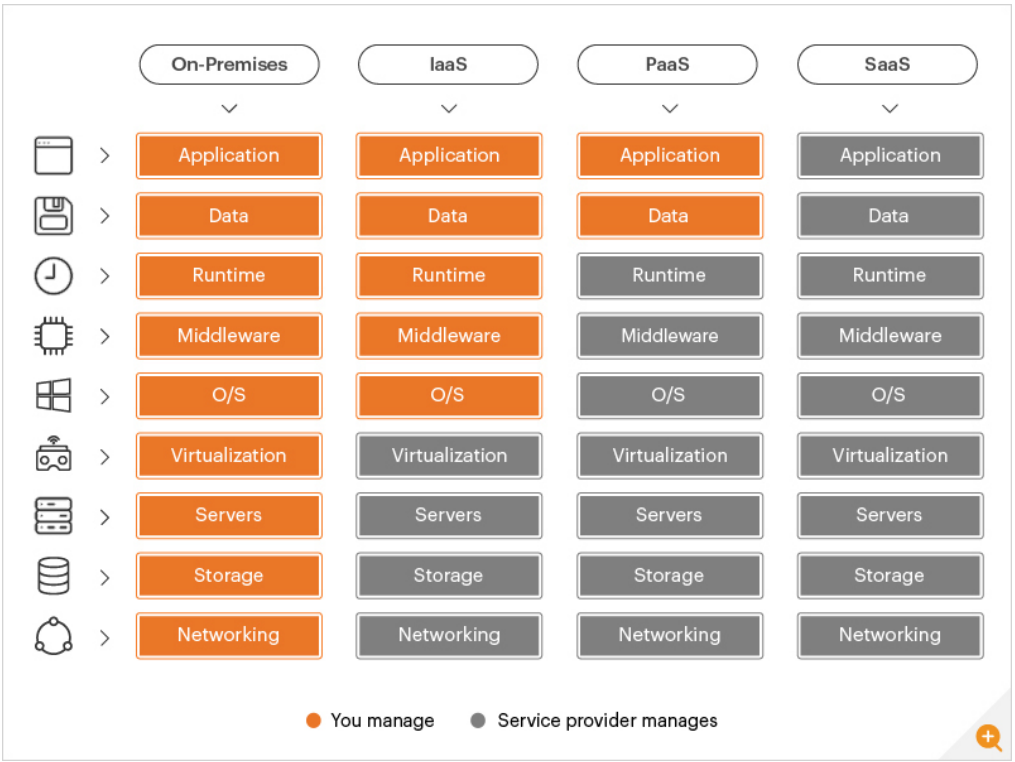
Cloud Computing is inmiddels zeer volwassen geworden en kan worden beschouwd als een de facto. Nieuwe aanbieders, aanbieders van nieuwe functionaliteit, zullen hun systemen bouwen volgens een cloudarchitectuur en de functionaliteit alleen aanbieden als 'as-a-service', de on-premise variant is commercieel 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 bieden 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 schuift 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 beheren, 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.

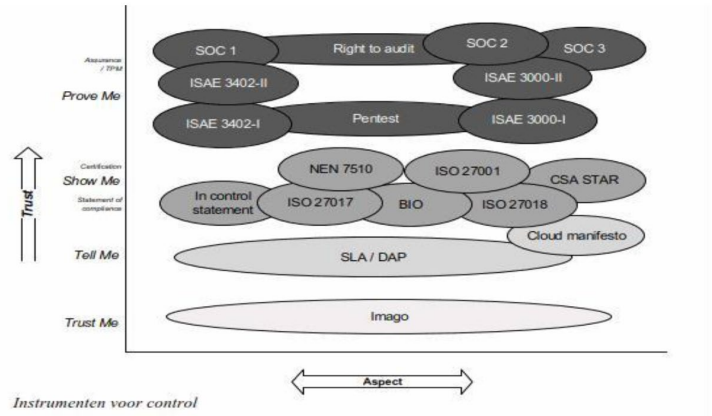
A.4. Deploymentmodellen

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 door 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. Instrumenten voor control



Instrumenten voor control

C. Verklarende woordenlijst

Cloud-Broker	Een entiteit die het gebruik, de prestaties en de levering van cloudservices beheert en onderhandelt over relaties tussen cloudproviders en cloudconsumenten. 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.
Cloud Center of Exellence	Een centraal ingericht team dat de cloudarchitectuur implementeert en decentrale teams (divisies) faciliteert en adviseert, maar zeker niet namens de decentrale teams bedrijfsoplossingen implementeert.
Cloud Computing	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.
Cloud (Service) Provider	Een leverancier die een platform, infrastructuur, toepassing of opslag in de cloud aanbiedt.
Containerplatform	
IaaS	Infrastructure as a Service (verdere uitleg – zie bijlage A.3.).
ITIL	Information Technology Infrastructure Library - is een framework bestaande uit een reeks best practices voor het leveren van efficiënte IT-ondersteuningsdiensten.
Legacy	Verouderde Software
On-premise	De software die een bedrijf gebruikt, is geïnstalleerd op servers en computers in het eigen bedrijfspand. De hardware én de softwarelicenties zijn eigendom van het bedrijf. In dit geval een leverancier voor UWV.
Outsourcing	Uitbesteding (in dit geval van diensten)
Open Source	
PaaS	Platform as a Service (verdere uitleg – zie bijlage A.3.)
Private Cloud	Cloud computing dat alleen gebruikt wordt door één organisatie, compleet afgeschermd. Voorbeelden zijn private clouds gebaseerd op Microsoft Azure Stack, open source OpenStack, of containerplatform OpenShift
Public Cloud	Cloud computing is bereikbaar voor het publiek, voor individuen en bedrijven. Voorbeelden zijn Gmail, Microsoft 365, Dropbox, Microsoft Azure en Amazon AWS.
SaaS	Software as a Service (verdere uitleg – zie bijlage A.3.)
Stack	
VM	Virtual Machine - een computerprogramma dat een computer nabootst, waar andere programma's op kunnen worden uitgevoerd.
VPN	Virtual Private Network – een versleutelde, beveiligde verbinding