Extern verslag marktconsultatie

KWNTC

Inhoudsopgave

1 Aanleiding en doelstelling van de marktconsultatie

UWV heeft in het kader van project Vooronderzoek Kantoorautomatisering, Werkplek, Netwerk, Telefonie en Contact Center (hierna: KWNTC[1]) besloten een marktconsultatie uit te voeren. Er is gekozen voor een zogenaamde gesloten interactieve marktconsultatie bestaande uit een schriftelijke beantwoording van door UWV gestelde vragen, gevolgd door een 1-op-1 consultatie tussen UWV en de individuele deelnemers.

Voor de marktconsultatie zijn in willekeurige volgorde de volgende deelnemers uitgenodigd: KPN, Capgemini, Microsoft, Wortell, Content Guru, Cegeka, OGD, Vodafone-Ziggo en Fujitsu. De marktconsultatie is op 20 april 2020 bekend gemaakt via een aankondiging op Tenderned (Tenderned Kenmerk 262661). Na publicatie van de aankondiging hebben, naast de uitgenodigde deelnemers, andere marktpartijen aan UWV verzocht toegevoegd te worden aan de groep deelnemers. Na ampel beraad door UWV is besloten deze partijen niet toe te voegen aan de marktconsultatie, daar ze om verschillende redenen niet voldeden aan de criteria die UWV daarvoor had opgesteld en gepubliceerd in de hierboven genoemde aankondiging. De uitgenodigde deelnemers zijn geconsulteerd over een aantal onderwerpen die in onderstaande structuur worden teruggekoppeld in dit verslag.

Hoofdstuk 2: Toekomstvisie, verkaveling en aanbestedingsstrategie;
Hoofdstuk 3: Regie;
Hoofdstuk 4: Architectuur;
Hoofdstuk 5: Werkplek;
Hoofdstuk 6: Netwerk;
Hoofdstuk 7: Telefonie (vast en mobiel);
Hoofdstuk 8: Contact Center Dienst;
Hoofdstuk 9: Security en IAM;
Hoofdstuk 10: Maatschappelijk verantwoord ondernemen;
Hoofdstuk 11: Bijlagen.

Dit verslag geeft per hoofdonderwerp de essentie van de uitkomsten van de marktconsultatie weer op basis van de schriftelijke beantwoording én de 1-op-1 gesprekken met de respondenten. Per hoofdonderwerp wordt het marktbeeld op een aantal subonderdelen weergegeven. Als commercieel vertrouwelijk geclassificeerde informatie is daarbij weggelaten en conclusies zijn niet te herleiden naar specifieke partijen.

Omdat UWV in de marktconsultatie open vragen heeft gesteld zijn de formuleringen van de uitkomsten nooit één op één een weergave van wat individuele deelnemers letterlijk hebben gezegd/geschreven in reactie op de gestelde vragen van UWV. Soms hebben deelnemers antwoorden op vragen ook (deels) verwerkt in antwoorden op andere vragen. Dit verslag betreft dus een weergave van het dominante beeld per onderwerp zoals UWV dat uit alle antwoorden heeft gedestilleerd en geïnterpreteerd.

Indicatief zijn achter de betreffende onderwerpen de vraagnummers uit het UWV Marktconsultatie document KWNTC (zie Bijlage-001 bij dit verslag) weergegeven waar het onderwerp bij hoort.

[1] Tijdens de marktconsultatie heft UWV de afkorting KWNT gebruikt. Later is deze afkorting uitgebreid naar KWNTC om ook de CCD dienstverlening hier expliciet een plek te geven. Daar waar in het marktconsultatie document en de NvI KWNT staat vermeld, dient dit te worden gelezen als KWNTC.

UWV zal naar eigen inzicht de conclusies uit dit verslag verwerken in de definitieve aanbestedingsstrategie en de uitvoering van die strategie. Aan dit verslag kunnen geen rechten worden ontleend.

1.1 Bronnen voor dit verslag

Bij het opstellen van dit verslag zijn de onderstaande bronnen gebruikt:

- Het UWV Marktconsultatie document KWNTC zoals dit aan de deelnemers is gestuurd (zie Bijlage-001 bij dit verslag);
- De Nota van Inlichtingen bij het marktconsultatie document (zie Bijlage-002 bij dit verslag);
- Individuele schriftelijke beantwoording door de deelnemers aan de marktconsultatie op de vragen van UWV in het hierboven genoemde marktconsultatie document;
- Uitkomsten van de 1-op-1 consultatie tussen UWV en de individuele deelnemers naar aanleiding van hun beantwoording op de vragen in het marktconsultatie document;
- Uitkomsten van de aanvullende schriftelijke vragenronde n.a.v. de 1-op-1 consultatieronde.

1.2 Respondenten per vraag

In de onderstaande tabel zijn het aantal respondenten per vraag vermeld. De vragen zelf zijn, zoals hierboven ook vermeld, terug te vinden in het UWV Marktconsultatie document KWNTC (zie Bijlage-001 bij dit verslag). Tevens vindt u daar meer achtergrondinformatie bij de marktconsultatie en de gestelde vragen.

Onderwerp	Vraag	Aantal respondenten
Toekomstvisie & Verkaveling	**1**	8
	2	8
	3	8
	4	8
	5	8
	6	8
	7	8
	8	8
	9	8
	10	8
Aanbestedings-strategie	**11**	8
	12	8
Regie	**13**	8
	14	8
	15	8
	16	8
	17	8
Architectuur	**18**	8
	19	8
	20	8
	21	8
	22	8

Onderwerp	Vraag	Aantal respondenten
Werkplek	**23**	8
	24	8
	25	8
	26	8
	27	8
	28	8
	29	8
Werkplek	**30**	8
	31	8
Netwerk	**32**	5
	33	5
	34	4
	35	4
Telefonie	**36**	6
	37	5
	38	5
	39	6
CCD	**40**	5
	41	5
	42	5
	43	5
	44	5

Onderwerp	Vraag	Aantal respondenten
	45	5
Security & IAM	**46**	8
	47	8
	48	8
	49	8
	50	7
	51	8
MVO	**52**	8
	53	8
	54	8

2 Toekomstvisie, verkaveling en aanbestedingsstrategie (vraag 1 t/m 3)

2.1 Marktontwikkelingen en toekomstvisie

2.1.1 Marktontwikkelingen (vraag 1)

De door de respondenten genoemde relevante marktontwikkelingen met betrekking tot de diensten in scope zijn:

- KWNTC diensten van de (nabije) toekomst zijn SaaS (public cloud) diensten. De KWNTC SaaS oplossingen inclusief beveiliging zijn over de afgelopen jaren uitgegroeid tot volwassen producten;
- Collaboratie tooling (inclusief (video) bellen) is steeds belangrijker en biedt steeds meer functionaliteit in de werkplek, zoals MS Teams en MS SharePoint in MS Office365. Het perspectief van de gebruiker staat daarbij centraal;
- Een verandering van thin- naar fat-client werkplek-architectuur is nodig om met moderne (streaming) applicaties te kunnen werken en ook offline productief te kunnen zijn. Dit vergt een 'hybride' model voor applicatie ontsluiting waarbij de legacy applicaties die niet (veilig) op de fat client passen, als 'published app' naadloos in de lokale desktop geïntegreerd aan worden geboden.

2.1.2 Toekomstvisie (vraag 2 en 3)

De meeste respondenten onderschrijven in meer of mindere mate de KWNTC toekomstvisie en doelarchitectuur van UWV, zoals beschreven in het UWV Marktconsultatie document (Bijlage-001). De belangrijkste verschillen tussen respondenten zitten in het 'hoe' en 'wanneer' van de implementatie van de toekomstvisie.

Verschillen in 'hoe' zitten met name in:

- **Devices:** hoe ga je om met de aanschaf van en support op devices. Sommige respondenten pleiten voor aanschaf door UWV, anderen voor een lease constructie. Sommige pleiten voor alle devices bij één leverancier en anderen adviseren dit te beleggen bij de leverancier van de betreffende dienst of zelfs bij UWV zelf;
- **Beleid:** er zijn respondenten die aangeven dat vertrouwelijke data prima in de cloud kan gezien de beveiligingsmaatregelen die vandaag de dag genomen kunnen worden. Anderen pleiten voor opslag van gevoelige data in een private cloud omgeving. Heldere parameters voor dataclassificatie en een up-to-date data- en cloud beleid zijn hierbij van groot belang;
- **Organisatie:** de organisatorische kant van IT, dus wat beleg ik bij welke partij en hoe werkt dat met elkaar samen. Dit geldt in het bijzonder bij Identity & Acces Management (IAM) en service integratie diensten;
- **CCD:** voor CCD pleiten eigenlijk alle respondenten voor een cloud variant, maar is de ene leverancier sterk voorstander van 'SaaS, tenzij' en zien anderen een meer geleidelijke beweging naar SaaS diensten met als eerste stap private cloud.

Het tempo waarin de beweging naar (public) cloud diensten kan worden gemaakt voor de werkplek verschilt per respondent. Sommige respondenten pleiten er voor om de beweging naar public cloud diensten voor de werkplek nu al in te zetten. Daardoor kan UWV beheerst groeien en vernieuwen in technologie richting public cloud diensten. Hiermee groeit UWV ook geleidelijk in volwassenheid en kan ook al starten haar regieorganisatie hier op aan te passen. Dit kan volgens die respondenten binnen de bestaande contracten en maakt dat de weg vrij om voor de (eisen in de) aanbesteding voor het nieuwe contract eind 2023 te anticiperen op een meer moderne en toekomstvaste werkplek die al in belangrijke mate is geënt op SaaS functionaliteiten.

De meeste respondenten geven verder aan dat het zwaartepunt van adoptie in de werkplekomgeving zit en daarmee de grootste verantwoordelijkheid dus ligt bij de werkplekleverancier.

2.2 Verkaveling (vraag 4 t/m 10)

Het dominante beeld is dat de markt pleit voor het meer 'opknippen' van de KWNTC scope ten opzichte van de huidige verkaveling. Bijna alle respondenten geven aan dat netwerk als een apart kavel moet worden gezien (nu werkplek + netwerk één kavel). Bij IAM zijn de respondenten verdeeld. Sommigen pleiten ervoor dit bij een expert te beleggen. De meesten pleiten ervoor dit zo veel mogelijk bij de werkplekleverancier te beleggen vanuit integratie perspectief. Ten aanzien van telefonie wordt door de meeste respondenten ervoor gepleit om vast en mobiel in één kavel te stoppen. Dit in verband met de steeds verdergaande integratie tussen vast en mobiel. Daarnaast zijn er respondenten die er voor pleiten netwerk en telefonie in één kavel te brengen.

CCD zien alle respondenten als een zelfstandig kavel. Wel is er verschil per leverancier in welke mate integratie plaatsvindt met generieke telefonie- en werkplekdiensten. Demarcatiepunten liggen soms ook anders, bijvoorbeeld SIP Trunking (CCD verkeer) ondergebracht bij de CCD leverancier of juist de Telefonie leverancier.

2.3 Aanbestedingsstrategie (vraag 11 en 12)

2.3.1 Algemeen (vraag 11)

Respondenten zijn verdeeld over het aantal aanbestedingen dat nodig is om de geadviseerde verkaveling te implementeren. Logischerwijs komt dit doordat respondenten (mede door eigenbelang) ook verschillende verkavelingen adviseren. Het dominante beeld uit de markt is dat respondenten voor de meeste aanbestedingen een niet-openbare procedure adviseren. Verder is de markt verdeeld over de looptijd die UWV zou moeten hanteren voor de geadviseerde kavels.

2.3.2 Pilot als randvoorwaarde voor definitieve gunning (vraag 12)

Respondenten zijn verdeeld over nut en noodzaak van een pilot voor definitieve gunning. Iets meer dan de helft van de respondenten adviseert nog wel een vorm van pilot binnen de aanbestedingsprocedure. Het andere deel adviseert om dit niet te doen.

Als belangrijkste voordelen van een pilot worden de volgende zaken genoemd:

- Een oplossing kan in een pilot beter technisch en organisatorisch getoetst worden dan in een beproevingsfase;
- Een pilot verkleint voor UWV het risico dat de leverancier na defintieve gunning niet kan leveren;
- Voor de leverancier is een pilot een manier om aannames en uitgangspunten te toetsen;
- Een pilot kan de adoptie bevorderen indien functionele inrichting wordt meegenomen;
- Het piloten van deelgebieden kan binnen beperkte tijdskaders.

Als belangrijkste nadelen / risico's van een pilot worden de volgende zaken genoemd:

- Het uitvoeren van een pilot binnen de aanbestedingsfase kost veel geld en tijd;
- Een pilot biedt schijnzekerheid: een pilot met positieve uitkomst is geen garantie voor succes na definitieve gunning;
- Respondenten zetten veelal dezelfde tools in binnen het werkplek domein. Een pilot is daarmee niet echt onderscheidend tussen respondenten;
- Een pilot test met name de werking van de technologie terwijl de nadruk moet liggen op de kwaliteit van de dienstverlening en de organisatorische 'fit' met UWV;
- Het opstellen van objectieve criteria voor de pilot is uitdagend.

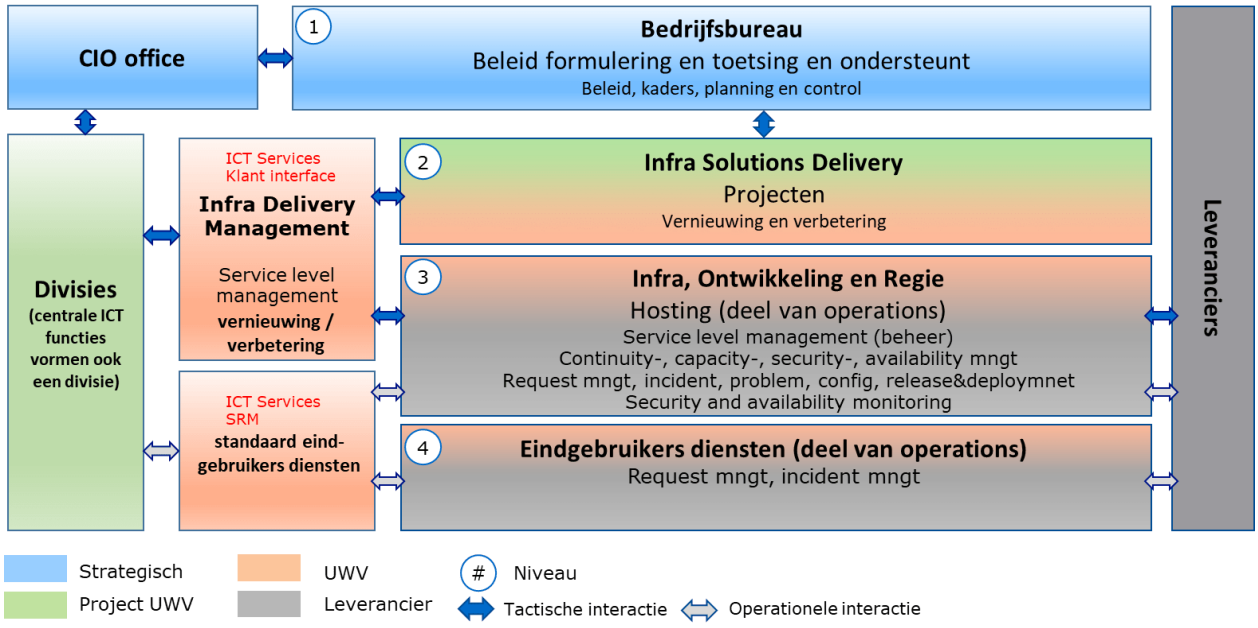
Als alternatieven voor het uitvoeren van een pilot worden de volgende zaken genoemd:

- Neem de ervaring van andere klanten met een bepaalde leverancier mee in de aanbesteding. Bijvoorbeeld aan de hand van referentiebezoeken met focus op verschillende aandachtsgebieden (functionaliteit, partnerschap en integrale kwaliteit);
- Laat de geselecteerde leverancier een functionele beproeving uitvoeren aangevuld met het delen van een technische detaillering van de oplossing;
- Betrek eindgebruikers bij het kwalificeren van de gevraagde dienst om acceptatie in een vroeg stadium te bewerkstelligen;
- Hanteer een “babysit” periode om na oplevering van diensten mogelijke restpunten succesvol op te lossen;
- Voer geen pilot uit maar pas een agile werkwijze toe met meerdere plateaus waarin dienstverlening in verschillende stappen wordt toegevoegd.

3 Regie (vraag 13 t/m 17)

3.1 Huidige situatie

Begin 2019 heeft een herijking van het regiemodel plaatsgevonden naar aanleiding van de aanbesteding van datacenter diensten door UWV. Op basis daarvan is het huidige regiemodel van de afdeling ICT Services vastgesteld inclusief de positie van haar leveranciers. Deze is weergegeven in figuur 1. Onder de term 'infra' vallen naast de datacenter ook de ICT werkplek-, netwerk- en telefonie (vast en mobiel) diensten.



Figuur 1 Schematisch het regiemodel

UWV heeft op dit moment een ICT die grotendeels aanbodgericht opereert met een beweging naar meer vraaggericht: UWV *ondersteunt* de business met ICT door het bieden van oplossingen en is steeds meer in staat tot het *beantwoorden* van de business-vraag naar ICT.

3.2 Algemeen (vraag 13)

De meeste respondenten zien geen significante impact op de regie organisatie als gevolg van de verkaveling. Wel kan UWV door de beweging richting Cloud/SaaS diensten volgens sommigen respondenten meer tijd vrijmaken in de regie organisatie om zich te richten op verbetering en innovatie.

3.3 Service integratie (vraag 14)

Het dominante marktbeeld t.a.v. service integratie is als volgt:

- Service integratie vindt in ieder kavel plaats door de leverancier van diensten in dat kavel;
- De meeste respondenten zien regie op tactisch en strategisch niveau ingevuld door UWV (incl. service integratie op dat niveau);
- Daar waar service integratie wordt 'uitbesteed' zijn alle respondenten het er over eens dat dit alleen de operationele service integratie betreft. Op tactisch/strategisch niveau ligt de verantwoordelijkheid altijd bij UWV al dan niet in samenwerking met één of meerdere externe leveranciers;

- Er zijn 3 dominante varianten die door de respondenten worden genoemd voor kavel overkoepelende service integratie op operationeel niveau:
    1. Service integratie (SIAM functie) uitbesteden aan een externe leverancier die niet ook diensten verleent aan één van de kavels;
    2. Service integratie uitbesteden aan een externe leverancier die de werkplek diensten levert;
    3. Service integratie door UWV zelf met hulp/advies van de leveranciers van diensten van de verschillende kavels.
- Voor zover respondenten expliciet daarop ingaan, kent hun advies voor het beleggen van het Licentieloket en Licentiemanagement min of meer dezelfde driedeling als hun advies voor de service integratie functie.

3.4 Functioneel beheer en ketenmonitoring (vraag 15)

Het dominante marktbeeld met betrekking tot functioneel beheer is dat met de transformatie naar cloud/SaaS diensten en standaardisatie de rol van UWV IT (nog meer) richting functioneel beheer verschuift.

Met betrekking tot ketenmonitoring raden respondenten aan, voor zover ze daar expliciet op ingaan, dat UWV voor ketenmonitoring centraal de oplossing en het beleid bepaalt terwijl de individuele leveranciers van de componenten hun monitoring op de centrale oplossing van UWV aansluiten.

3.5 Optimalisatie en innovatie (vraag 16)

- Meerdere respondenten geven aan dat de verkaveling op zichzelf geen garantie is voor het stimuleren van Advies, Implementatie, Beheer en Optimalisatie
- Meerdere respondenten benadrukken dat UWV zelf een belangrijke rol heeft als facilitator van advies en innovatie.
- Er moet ook op tactisch / strategisch niveau structureel met leveranciers worden gesproken waar het gaat om formuleren van visie, strategie en beleid.
- Meerdere respondenten wijzen ook op de mogelijkheid om in de contractfase afspraken te maken over innovatie bijvoorbeeld door daarvoor een incentive af te spreken

3.6 Service Levels (vraag 17)

Alle respondenten pleiten voor zowel een Service Level Agreement (SLA) als een Experience Level Agreement (XLA), waarbij de meeste respondenten aangegeven dat de XLA het belangrijkst is.

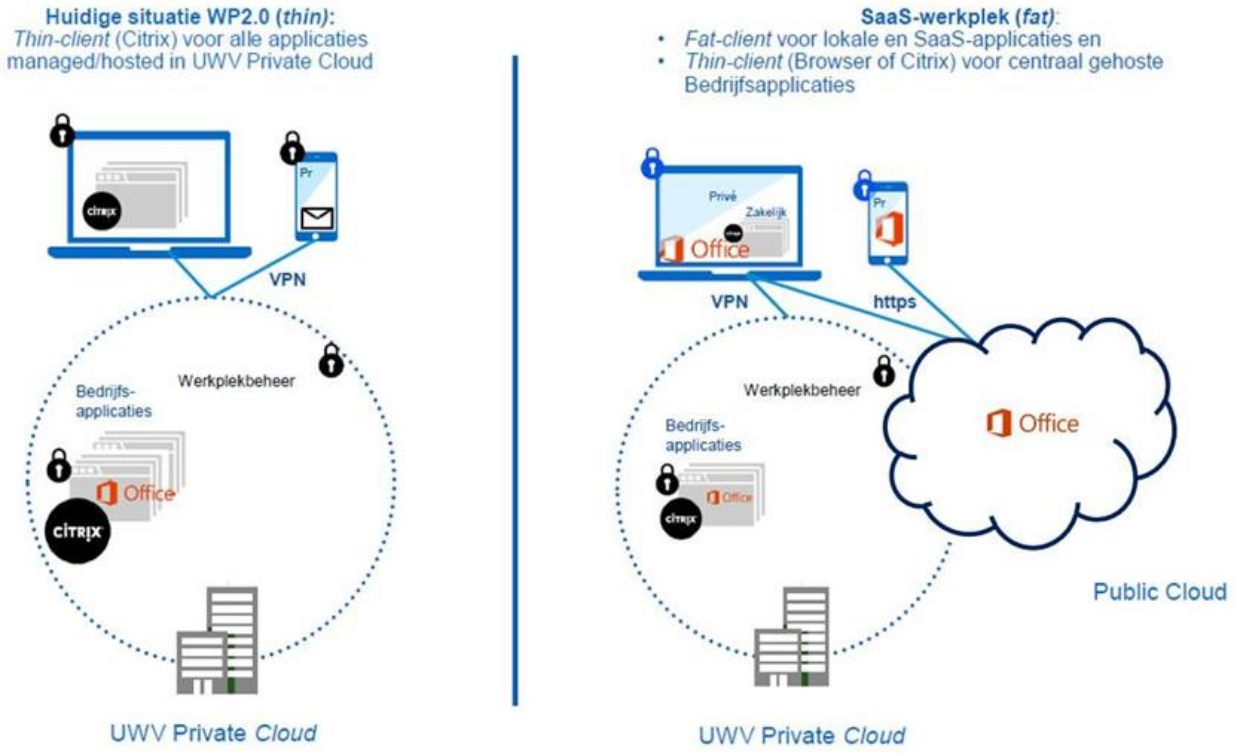
4 Architectuur (vraag 18 t/m 22)

4.1 Huidige situatie

De huidige architectuur van UWV typeert zich als 'een verregaand gestandaardiseerde omgeving, die als een door 'een slotgracht' omringd trusted domain is ingericht', en daarmee vooral infrastructureel beveiligd is. Zowel de werkplek, de data als de functionaliteit bevinden zich nu in de centrale datacentra.
Er wordt gebruik gemaakt van een virtuele (middels Citrix-SBC en VDI) gehoste online werkplek, die vanaf elke UWV-desktop (op kantoor) of UWV-laptop (overal) kan worden benaderd en waarop KA-, business- en internet-applicaties door elkaar gemengd worden aangeboden. De virtuele werkplek wordt als dienst afgenomen bij KPN, de fysieke werkplek (hardware) is op dit moment eigendom van UWV en in beheer bij KPN. Vanuit de optiek van standaardisatie en beveiliging kan de gebruiker in de huidige situatie geen wijzigingen doorvoeren. Elke medewerker heeft onafhankelijk van zijn functie dezelfde werkplek specificaties. Om de 3-4 jaar is een grote vernieuwing/migratie nodig om de omgeving actueel te houden. De businessapplicaties worden op dit moment gehost in de datacentra van IBM. In de komende periode worden de businessapplicaties gefaseerd gemigreerd naar de nieuwe leverancier voor datacenter dienstverlening DXC.

4.2 Hybride werkplek (vraag 18)

De hybride doelarchitectuur (zoals weergegeven in de onderstaande figuur rechts) van de werkplek wordt als onvermijdelijk gezien door respondenten om een transitie te kunnen maken naar werkplekconcept dat aansluit bij de doelen van het UWV ten aanzien van o.a. flexibiliteit en samenwerken (het is niet de vraag óf, maar wanneer). Office365 wordt door alle respondenten genoemd als hét platform om stapsgewijs, op basis van een roadmap, naartoe te migreren.



4.3 Public cloud beleid i.r.t. security en compliance (vraag 19)

De drie voornaamste aandachtspunten die de respondenten noemen ten aanzien van de inzet van public cloud diensten zijn:

1. Security: van technische maatregelen overstappen naar beleidsregels en maatregelen op data-niveau;
2. De geschiktheid van het applicatielandschap en de impact van periodieke updates;
3. Het adoptievermogen van gebruikers en de inrichting van een passende (structurele, vanwege de periodieke updates) adoptiestrategie.

Respondenten geven aan dat verschillende overheidsorganisaties inmiddels public-cloud toepassingen gebruiken en dat zij steeds vaker een "Public Cloud tenzij"-beleid volgen. Concrete voorbeelden van centrale overheden worden echter niet genoemd, wel enkele gemeenten.

Vanuit organisaties komt meer aandacht voor het classificeren van data, wordt voor werkplekken en identiteiten conditionele toegang ingeregeld en wordt de werkplek beveiligd tegen ongeautoriseerde handelingen en verlies van data.

Er zijn geen concrete voorbeelden gegeven van (overheids) organisaties met een duidelijk beleid (dataclassificatie) op ongestructureerde data.

4.4 Risico's en kansen t.a.v. public cloud (vraag 20)

Over het algemeen schetsen de respondenten een zelfde, algemeen beeld ten aanzien van de kansen die de public cloud kan bieden. Er wordt gesproken over flexibiliteit, snelheid, kostentransparantie, pay-per-use, standaardisatie, automation, innovatief platform en sterke beveiligingsmaatregelen.

Ten aanzien van de risico's rondom de Public Cloud (SaaS) wordt voornamelijk verwezen naar de door SLM Microsoft Rijk geschreven DPIA's (Data protection impact assessments). UWV kan daarnaast zelf nog een DPIA (GEB-analyse) uitvoeren.

Het adoptie- en absorptievermogen van UWV ten aanzien nieuwe ontwikkelingen, updates, in de public cloud kan zowel als een kans als een risico gezien worden.

UWV wordt sterk afhankelijk van internetverbindingen, het netwerk dient geschikt te zijn voor public cloud diensten.

4.5 Alternatieven voor public cloud (vraag 21)

De respondenten geven allen aan dat "private cloud" van leveranciers of de "Rijkscloud", met de "Rijkswerkplek" kan worden overwogen als alternatief voor de public cloud diensten. Voor private cloud wordt echter steeds minder ontwikkeld. Veel private cloud diensten leunen op technologie en producten die door de public cloud leveranciers worden ontwikkeld.

Ten aanzien van de public cloud diensten van Microsoft zijn er alternatieven maar dit zijn vaak wel oplossingen voor specifieke deeloplossingen (versnipperd). Denk aan Dropbox en Box.com. Ten aanzien van data-opslag is er, zolang dataclassificatie nog niet volledig is geïmplementeerd, geen andere optie dan een hybride oplossing voor data-opslag.

4.6 Beheeractiviteiten bij volledige cloud werkplek (vraag 22)

Respondenten geven over het algemeen aan dat activiteiten ten aanzien van de configuratie, releases & adoptie en applicaties te beleggen zijn:

- **Configuratie**
  Voor de werkplek (laptop & smartphone) zal de configuratie ingericht, beheerd en onderhouden moeten worden, evenals de inrichting van public cloud-gebaseerde office omgevingen (MS365), de koppeling van on-premises en cloud identity en inrichting van access control, en uiteraard de overkoepelende beheer (ITIL), monitoring en security over de keten heen (SIEM/SOC).
- **Releases & adoptie.**
  Respondenten geven aan dat het beheer van de releasekalender met de periodieke updates en de impact op de IT omgeving van UWV de juiste beheer-dienstverlening en een gedegen adoptie-aanpak vragen.
- **Applicaties**
  Het packagen en distribueren van de applicaties wordt ook als beheer bij een cloud-based werkplek gezien.

Respondenten adviseren om bovenstaande beheeractiviteiten ten aanzien van de werkplek zoveel mogelijk bij 1 leverancier te beleggen om afhankelijkheden te beperken en duidelijke verantwoordelijkheden te beleggen.

5 Werkplek (vraag 23 t/m 31)

5.1 Huidige situatie

De veranderende behoeften van medewerkers vergt meer dan UWV's huidige virtuele werkplek (Citrix) kan ondersteunen, want die is in full control van KPN en ongeschikt voor streaming media. De werkplek van UWV biedt toegang tot kantoorautomatisering functionaliteit en tot de bedrijfsapplicaties van UWV. De werkplek bestaat uit zowel een fysieke als een virtuele component, waarbij het uitgangspunt is dat zoveel mogelijk functionaliteit binnen de virtuele werkplek aangeboden wordt.
UWV maakt ook gebruik van een mobiele werkplek. De toegang tot UWV functionaliteit is in dit geval beperkt.
Daarnaast maakt UWV gebruik van een aantal speciale werkplekken. Deze werkplekken worden ingezet voor een specifieke doelgroep, vaak klanten of medewerkers met een ARBO-beperking.

5.2 Evergreen aanpak (vraag 23, 26 en 29)

De respondenten sluiten allemaal aan bij de "evergreen-aanpak" zoals UWV deze voorziet in haar concept toekomstvisie. Hierbij maken alle respondenten ook nadrukkelijk de opmerking dat deze aanpak aanzienlijke gevolgen heeft voor de organisatie van UWV (adoptiemanagement, periodieke deployment, DevOps-manier van werken). Hier wordt door sommige respondenten de opzet van een Cloud/MS365 Competence Center geadviseerd.

Het harde onderscheid zoals UWV dat in de werkplek types schetst, zal volgens de respondenten in de toekomst steeds meer verdwijnen. Alle respondenten adviseren uit te gaan van 1 werkplek-concept dat meerdere persona's kan ondersteunen. Dit concept geeft de UWV-medewerkers de vrijheid om de beschikbare tools te gebruiken al naar gelang behoefte, op ieder moment van de dag en vanaf iedere plaats. Toegang tot functionaliteit voor persona's wordt geregeld middels MDM en MAM.

Zolang nog niet alle bedrijfsapplicaties 'cloud-ready' zijn, is de hosted optie (published desktop op basis van RDS / Citrix) voor een specifieke persona mogelijk (nog) een goede keus, vanwege meer specifieke bedrijfsapplicaties met een hoge vertrouwelijkheid.

Het onderscheid in type werkplek zal op termijn verdwijnen. Het verschil zit in de functionaliteit die de persona aangeboden krijgt.

5.3 Integratie werkplek en telefonie (vraag 24)

De respondenten geven aan dat Unified Communications sterk in ontwikkeling is en inmiddels de telefonie-functie is op de werkplek voor intern gebruik. Voor specifieke telefoniefuncties (zoals CCD, baliemedewerkers, secretaresses maar ook 112 en noodnummers in bijv. liften) is momenteel nog een aparte telefoniecentrale nodig naast de UC-applicatie. Zie verder ook de marktbeelden zoals uitgewerkt onder hoofdstuk 7 'Telefonie'.

5.4 Samenwerkingsplatform (vraag 25)

Over het algemeen geven respondenten aan dat de functionaliteit van het samenwerkingsplatform apart benaderd moet worden (intranet, applicatie portaal en documenten). Het intranet zou deze functionaliteit visueel bij elkaar kunnen brengen en hierdoor een hub-functie vervullen, maar dan meer in het

samenbrengen van informatie, en niet persé als universeel startpunt van de werkplek. De meeste respondenten adviseren om aan te sluiten op de standaard werkplek propositie van Microsoft.

5.5 Shadow IT (vraag 27)

De respondenten onderschrijven een aanpak waarbij eindgebruikers meer rechten krijgen tot het installeren en gebruiken van Apps. Dit zou het gebruik van Shadow IT doen verminderen. Het is daarbij wel van belang dat UWV hier een stuk beheer en regie op inricht welke geënt is op adoptie en gebruik van de nieuwe functionaliteit en waarbij wordt gemonitord op het gebruik van alle App's.

5.6 Beheeractiviteiten (vraag 28)

Met betrekking tot werkplekconfiguratie, applicatiedistributie, releasemanagement & adoptie adviseren meerdere respondenten om dit bij één leverancier (extern of intern) te beleggen.

De servicedesk kan volgens de respondenten het beste worden gepositioneerd als onderdeel van het werkplek-domein. Functioneel beheer zou voornamelijk bij UWV kunnen worden belegd en misschien wel moeten worden belegd.

Mede in het kader van ondersteuning bij adoptiemanagement, functioneel beheer en continue verbetering wordt de opzet van een 'Cloud/Office365 Competence Centre' binnen UWV door meerdere respondenten geadviseerd. Hierbij wordt UWV geholpen door experts (niet alleen de leverancier van de dienst). De rol van externen kan worden afgebouwd op het moment dat interne voldoende kennis en ervaring is opgebouwd.

Tot slot geven de respondenten aan dat verantwoordelijkheden en taken t.a.v. de 'Service integrator rol' ten behoeve van de aansturing van functionele ketens duidelijk moeten worden belegd.

5.7 Ontsluiting bedrijfsapplicaties (vraag 30 en 31)

Respondenten adviseren een splitsing tussen de verantwoordelijkheid voor de werkplek en de verantwoordelijkheid voor applicatie-ontsluiting te voorkomen. De oplossing die de respondenten geven is tweeledig:

- Gebruik het platform bij DXC maar leg het beheer bij de werkplek-leverancier;
- Maak gebruik van Microsoft Virtual Desktop (MVD).

Verder geven de respondenten aan dat een Remote App/Desktop werkt wanneer er geen directe onderlinge afhankelijkheden tussen de applicaties zijn, en geen MS Office integraties. Voor de applicaties waarbij dit wel het geval is, kan er een "Full Remote Desktop" worden gebruikt. Dit heeft niet de voorkeur, omdat er dan sprake is van twee verschillende desktopomgevingen.

6 Netwerk (vraag 32 t/m 35)

6.1 Huidige situatie

Binnen het huidige 'intern trusted' (slotgracht model) netwerk architectuur is een grootschalige overgang naar draadloos netwerk inmiddels ingezet. Laptops 'docken' nog wel op bedraad LAN, maar uit ervaring blijkt dat draadloos werken bijna gelijke kwaliteit biedt, uitgezonderd voor media streaming. UWV zal in de toekomst dus nog meer, waar dat kan, converteren naar WLAN, mits voldaan wordt aan de geldende overheidsrichtlijnen voor veilig WLAN. Voor het ondersteunen van media streaming zijn hogere kwaliteit draadloze netwerken nodig, dus dat stelt ook eisen aan de doorontwikkeling van WLAN diensten. Als gevolg van de conversie naar WLAN neemt het belang van het bekabeld netwerk (BKN) af.
Voor gasten, bezoekers en privé devices van het UWV zal een logisch gescheiden open Hotspot netwerk beschikbaar komen in 2020. Dit draadloos netwerk moet gezien worden als een hospitality dienst. Voor medewerkers van andere overheden die als gast van het Wi-Fi-netwerk gebruik willen maken, is GovRoam als apart geauthentiseerde internet-toegangsdienst beschikbaar. De huidige oplossingen voor netwerk toegangscontrole, remote access toegang, firewalling en werkplek toegangscontrole - alhoewel redelijk werkend zijn op dit moment zeer beperkt geïntegreerd.

6.2 Zero trust (vraag 32 en 33)

Het dominante marktbeeld is dat de beweging naar een zero-trust netwerk wordt gezien als de logische en de te adviseren richting. Een meerderheid van de respondenten noemt zero-trust onvermijdelijk. De huidige 'intern trusted' (slotgracht model) wordt beschouwd als niet langer houdbaar door de veranderingen in het IT landschap: diensten, gebruikers, devices en data bevinden zich steeds vaker buiten het vertrouwde netwerk waardoor applicaties en data minder goed te beschermen zijn.

Alle respondenten geven aan dat een omschakeling naar zero-trust geen gemakkelijke is: een gefaseerde aanpak (en geen 'big bang') zal tijd en inspanning kosten (enkele jaren). De transitie zal veel inspanning en samenwerking vergen over veel domeinen binnen het IT landschap heen. De verkaveling en het aantal betrokken leveranciers hebben invloed op de complexiteit van die transitie. Meer opknippen leidt tot een hogere complexiteit.

Een situatie waarin zowel intern trusted als zero trust naast elkaar functioneren is volgens de respondenten mogelijk. Geen enkele respondent geeft aan dat zero-trust het enige model moet zijn.

6.3 Toegangscontrole (vraag 34)

Bij de keuze voor een zero trust architectuur dient de gebruikers 'identity' als kern van een brede security oplossing voor beveiliging en controle te worden beschouwd. De 'trust' wordt ervan afhankelijk per netwerk-/applicatie onderdeel.

Bij het inrichten van toegangscontrole verdient een Best-of-Suite benadering volgens de respondenten de voorkeur boven een Best-of-Breed benadering vanwege:

1. Betere integratiemogelijkheden en minder overlap van oplossingen;
2. Snellere beschikbaarheid van technische innovaties;
3. Beter, sneller kunnen regelen en sanctioneren van connectiviteit.

6.4 Internet ontsluiting bedrijfsapplicaties (vraag 35)

Er zijn volgens de respondenten weinig/geen risico's in het realiseren van een rechtstreekse internet ontsluiting voor de E-diensten die in het DXC datacenter draaien.

7 Telefonie vast en mobiel (vraag 36 t/m 39)

7.1 Huidige situatie

UWV kent momenteel een strikte scheiding tussen mobiele en zakelijke/vaste telefonie.
UWV maakt gebruik van servicenummer diensten (088/0900/0800), routering van gesprekken voor de kleine interne callcenters zoals de Servicedesk, mobiele abonnementen en het UWV-nummerplan. Daarnaast beschikt UWV nog over een klein aantal enkele- en meervoudige lijnen ten behoeve van onder andere kassa's en intercoms. UWV heeft circa 4.000 'desk phones' (fysieke VoIP telefoontoestellen) in gebruik. De logistiek van deze toestellen wordt verzorgd door KPN. De VoIP oplossing maakt gebruik van het netwerk van UWV dat geleverd wordt door KPN.
Iedere medewerker van UWV, behalve de KCC medewerker, beschikt over een mobiele telefoon met SIM, ongeacht zijn of haar functie. Deze mag privé gebruikt worden. De eerstelijnsondersteuning, van onder andere de mobiele telefoon, wordt verzorgd door de interne UWV IT servicedesk. Voor het beheer en de beveiliging van de mobiele telefoon wordt gebruikgemaakt van een Mobile Device Management oplossing van Citrix in combinatie met Samsung Knox aangevuld met een Mobile Threat Defense oplossing van Checkpoint. Dit alles wordt geleverd en beheerd door KPN.
Het Klant Contact Center (KCC) van UWV maakt gebruik van de UWV generieke telefonie en werkplek oplossing, inclusief een 'softphone'. Deze 'softphones' zijn recent vervangen door 'hardphones' ter verbetering van de spraakkwaliteit. Het 0900 en 088 telefoonverkeer voor het KCC wordt in de datacenters van de leverancier van het callcenter platform afgeleverd.

7.2 Vast- mobiel integratie (vraag 36 en 37)

Dominant zijn twee oplossingen door de respondenten genoemd voor telefonie:

1. Een Hosted Voice oplossing;
2. Een Unified Collaboration & Communication (UC&C) oplossing.

De functionaliteit 'Bereikbaarheid' is volgens de respondenten het beste in te vullen met een hosted voice oplossing terwijl 'Samenwerken' juist dominant is bij een UC&C oplossing.

Bij UC&C ligt de nadruk op interne telefonie; het 1-op-1 bellen tussen collega's onderling. UC&C heeft een naadloze integratie met de werkplek en hoort daarmee ook meer in dat kavel.

Beide oplossingen ontwikkelen volgens de respondenten snel en hebben in functionaliteit al overlap maar de integratie is niet sluitend. Het realiseren van een naadloze vast/mobiel integratie is daarmee lastig. Oplossingen in de markt verschillen en kennen op dit moment nog elk hun eigen risico of uitdaging.

7.3 Smartphone beleid medewerkers (vraag 38)

De mobiele telefoon is onderdeel van de werkplek beleving en daarmee een vanzelfsprekendheid voor alle respondenten. Ze geven aan dat het bieden van een keuze in (smartphone) model goed is (medewerker-tevredenheid en productiviteit) en tegelijk onontkoombaar.

Het 'Choose Your Own Device (CYOD)' beleid (met eventueel nog een stap verder te door een voucher principe te hanteren) wordt dominant als de te preferen regeling beschouwd. Bring Your Own Device (BYOD) is volgens de respondenten een mogelijkheid maar kent risico's op het gebied van security. Zie ook vraag 49.

7.4 Videoconferencing (vraag 39)

Er wordt door de respondenten onderscheid gemaakt tussen persoon-tot-persoon VC en 'VC ruimtes'. Het dominant beeld ten aanzien van beide vormen van videoconferencing is als volgt:

- Persoon-tot-persoon VC is onderdeel van de UC&C oplossing/dienst en moet worden uitgevraagd in het werkplek kavel.
- Een 'VC ruimte' oplossing/dienst dient apart te worden uitgevraagd van een UC&C oplossing/dienst;

Verder wordt een goede integratie van de VC ruimte oplossing met de werkplek UC&C oplossing geadviseerd.

8 Contact Center Dienst (vraag 40 t/m 45)

8.1 Huidige situatie

Telefoontjes komen binnen op centrale nummers (0900 of 088) van het KCC. Het volume en de toeleiding vallen nu niet onder de dienstverlening van het callcenter platform, maar worden onder de generieke telefoniedienst afgenomen (zie ook hoofdstuk 7 'Telefonie'). De telefonie leverancier levert die gesprekken af bij de datacenters van de callcenter platform leverancier. UWV beheert zelf de interfaces op de centrale 0900 en 088 nummers, zodat ze snel voice prompts kan plaatsen in geval van calamiteiten of extreme drukte.
Het transport van de gesprekken naar de klantadviseur vindt nu plaats door de generieke telefonie oplossing. Het transport van digitale berichten (waaronder VDC berichten en chatberichten) loopt via de portalen en een architectuur oplossing van berichtenverkeer tussen portalen, het elektronisch archief (EAED), K3CR, MS KCC en callcenter platform. Dit is nu maatwerk.
Telefonie vormt momenteel verreweg het grootste volume van alle contacten die UWV afhandelt. Ongeveer 4 miljoen per jaar. Daarna vormen de digitale contacten een steeds groter wordende groep met chat, co-browsing, berichtafhandeling via de online portalen (samen ongeveer 2 miljoen).
Momenteel worden alle staande gesprekken opgenomen om ook dreig-gesprekken van begin tot eind te kunnen registreren en voor kwaliteitsdoeleinden (opleiding en kwaliteitsmeting).
De huidige oplossing is matig geïntegreerd. Er is in naam sprake van een suite maar in de praktijk blijken het allemaal verschillende modules te zijn ('puntoplossingen'). Deze oplossingen integreren zeer beperkt met elkaar en met het bestaande ICT-landschap. Dit bemoeilijkt een integrale oplossing en leidt tot instabiliteit en verhoogde complexiteit van de dienst. Daarnaast maakt het gebrek aan integratie de keten inflexibel, duur en tijdrovend om te moderniseren en te innoveren. UWV heeft vanwege de inspanningen en kosten die ermee gemoeid zijn, ook in relatie tot de resterende looptijd, besloten tijdens de looptijd geen upgrade meer uit te laten voeren.

8.2 Integratie Contact Center Diensten (CCD); zero-footprint (vraag 40 t/m 43)

De integratie van CCD met andere toepassingen is volgens de respondenten goed mogelijk met name wanneer CCD als public cloud dienst wordt afgenomen. Integratie vindt volgens de respondenten als volgt plaats:

- Integratie met werkplek: door te kiezen voor een (public) cloud oplossing wordt onafhankelijkheid van het device georganiseerd, waarbij zero-footprint grotendeels mogelijk is. De CCD oplossing is dan web-/browser based en daarmee nagenoeg device onafhankelijk.
- Integratie met telefonie: deze Integratie kan op diverse manieren worden bereikt:
    - Een CCD leverancier met een operator licentie;
    - Een carrier neutraal platform;
    - Via een UC Suite koppelen naar CCD (bijvoorbeeld via Softphone).
    - Standaard koppelingen (bijvoorbeeld API framework)
- Integratie met netwerk: kies een contact center dienst op basis van SaaS (CSaaS) dienst met presentatie via netwerk.
- Integratie met overige toepassingen (gerelateerd aan het primaire proces): integratie met andere diensten zoals CRM, Social kan prima. Bijvoorbeeld o.b.v. API framework. Vaak bestaan er al veel standaard connectoren naar bijvoorbeeld CRM of ERP m.n. in het public cloud domein (die zijn daar immers van afhankelijk). Ook bij API's is het advies om te standaardiseren (ook bij maatwerkoplossingen).

8.3 Kwaliteit, beschikbaarheid, stabiliteit (vraag 44)

Het dominante advies van de respondenten is om een (public) cloud dienst voor CCD te gebruiken. Deze cloud diensten zijn gebouwd op hoge beschikbaarheid en robuustheid. Zaken zoals redundantie op meerdere niveaus (geografisch scheiding, redundant netwerk, telefonie, apparatuur, failover) zijn standaard ingeregeld. Een beschikbaarheid van 5x9 (99,999%) is daarbij geen uitzondering.

8.4 Positie Contact Center Dienst binnen het IT domein (vraag 45)

Het advies van de respondenten is om CCD als apart kavel uit te vragen, waarbij op onderdelen nog keuzes kunnen worden gemaakt waar de knip (en dus integratie) met een telefonie kavel wordt gelegd:

1. CCD met SIP trunk verkeer als 1 kavel;
2. CCD als los kavel en gebruikmakend van verkeer uit het telefonie kavel;
3. CCD als onderdeel van het telefonie kavel.

Verder is het advies van de respondenten om te kiezen voor een cloudoplossing waarbij een aantal respondenten kiest voor public cloud oplossing en een aantal voor een public cloud tenzij oplossing. Een private cloud oplossing wordt door de respondenten gezien als een verkapte vorm van on-premise dienstverlening. Deze variant kost volgens de respondenten snelheid, flexibiliteit en levert hogere kosten op.

9 Security en IAM (vraag 46 t/m 51)

9.1 Huidige situatie

Er is in de inrichting van een Information Security Management System (ISMS) voorzien. Hiermee kan de informatie efficiënt worden verwerkt, ontstaat een basis voor rapportage en sturing en geeft concern-breed inzicht in de mate van compliance. Dankzij de inrichting van een centrale voorziening om log data uit infrastructuur en applicaties op te slaan (log host), kan het UWV adequaat op afwijkingen van standaard patronen reageren en actie ondernemen om problemen te voorkomen, te beperken en op te lossen. De tooling wordt geleverd door de werkplek leverancier en de dienstverlening (SOC) wordt door UWV zelf uitgevoerd. Van contractpartijen op deeloplossingen binnen de IT omgeving wordt verwacht dat zij hun eigen SIEM/SOC en onderliggende log host-dienst hebben ingericht en hiermee koppelen aan het SIEM/SOC van het UWV.
Op het gebied van IB&P zijn maatregelen voor de AVG in het IV-voortbrengingsproces geïmplementeerd. Deze maatregelen betreffen: de verankering van de principes 'privacy by design' en 'privacy by default', inzicht in verwerkingen van persoonsgegevens, implementatie van een model voor het uitvoeren van Gegevensbeschermingseffectbeoordelingen (GEB). Het 'richtinggevend beleidskader privacy' is vastgesteld, waarin staat beschreven wat het voor UWV betekent om aan de vereisten van de AVG te voldoen. De komende jaren werkt UWV aan realisatie van het beleid.
UWV beschikt over een voorziening om via de portalen veilig gegevens met burgers en werkgevers uit te wisselen. De bestaande voorziening biedt onvoldoende bescherming om extra gevoelige gegevens (zoals medische gegevens) uit te kunnen wisselen. Ten aanzien van de verkaveling is het de vraag hoe om te gaan met verschillen in dataclassificatie. UWV investeert in maatregelen die bijdragen aan het verder terugdringen van datalekken, zoals het minimaliseren van de exportfunctie in applicaties met veel persoonsgegevens en het implementeren van een Data Loss Prevention tool.
SOC/SIEM zelf is buiten scope maar de afhankelijkheid is groot. Ten aanzien van Threat en Security Monitoring worden er strikte voorwaarden gesteld aan de KWNTC-dienstverlening

9.2 Positionering IAM (vraag 46)

Het dominante beeld uit de markt is dat respondenten UWV adviseren om de IAM diensten die in scope zijn van het KWNTC domein te beleggen in het kavel waarin ook de werkplek is ondergebracht. De respondenten gebruiken hiervoor argumenten die veelal op elkaar lijken:

- Identiteit en toegang moeten integreren met de werkplek om de beste gebruikerservaring te bewerkstelligen voor de eindgebruiker;
- Identiteiten en werkplekken kunnen zo naadloos op elkaar inhaken;
- identiteit is voorwaarden om O365 te kunnen gebruiken. Voor maximale integratie en het behoud van eenvoud en lage kosten zijn de centrale identiteit, de infrastructuur, de data en de applicaties (onder andere office en mobile apps) belegd in het werkplek kavel;
- Breng IAM onder in het werkplek kavel. Zo wordt toegangscontrole gehouden over data en applicaties afhankelijk van device, locatie, tijdstip en netwerk.

Het dominante beeld van de markt is dat de positionering van het UWV SOC als kavel overstijgend SOC wordt herkend. De markt onderschrijft dat een kavel overstijgend SOC steeds belangrijker wordt in de regievoering op uitbestede dienstverlening zeker als gebruik gemaakt wordt van public cloud dienstverlening.

9.3 Beste practice dataclassificatie beleid (vraag 47)

Het dominante marktbeeld is dat best practices van respondenten met betrekking tot dataclassificatie beleid binnen de publieke sector uitgaan van de BIO (Baseline Informatie Beveiliging Overheid) welke pleit voor een risico gerichte aanpak. De BIO ondersteunt de dataclassificatie als een set met maatregelen waarmee data passend beschermd kan worden. Enkele respondenten verwijzen voor de praktische invulling naar de Handreiking Dataclassificatie van de Informatiebeveiligingsdienst.

Respondenten adviseren veelal een procesmatige aanpak om dataclassificatie in te richten en te gebruiken. Deze aanpak bestaat grofweg uit de onderstaande stappen waarbij respondenten her en der accentverschillen aanbrengen:

1. Inventariseer en classificeer de data. De BIV codering wordt hierbij door meerdere respondenten als hulpmiddel genoemd;
2. Bepaal welke beveiligingseisen en beveiligingsmaatregelen per klasse gelden en implementeer deze (bijvoorbeeld: printen niet toestaan, encryptie toepassen, etc.);
3. Beoordeel de maatregelen op toepasbaarheid door te evalueren en door de effectiviteit te meten. Pas daar waar nodig herstelwerkzaamheden toe.

Naast de procesmatige aanpak wordt ook het gebruik van ondersteunende tooling door veel respondenten als belangrijk genoemd. Er is in de markt veel van dergelijke, ondersteunende tooling beschikbaar die de verschillende stappen van het classificatieproces kunnen automatiseren en ondersteunen. Veel van deze tooling is ook geïntegreerd in de MS365 suite van Microsoft (o.a. Azure Information Protection). Door de processtappen (deels) te automatiseren wordt de eindgebruiker ondersteund en ontlast bij het toepassen van dataclassificatie. Ook kan de tooling ingezet worden om achteraf herstelwerkzaamheden te verrichten.

Tot slot wordt het belang van gebruikers awareness door meerdere respondenten genoemd. Van belang is dat gebruikers worden getraind en stap voor stap worden meegenomen. Ook de continue aandacht voor dataclassificatie is daarbij van belang. Respondenten adviseren hiervoor training en key-user concepten in te zetten.

9.4 Verwerken van categorie 3 informatie (vraag 48)

Het dominante marktbeeld is dat categorie 3 informatie (bijvoorbeeld medische informatie) door eisen vanuit de BIO en AVG om extra beschermingsmaatregelen vraagt. Dit geldt voor zowel data “at rest”, data “in transit” als data “in use”). De beschermingsmaatregelen die daarbij geadviseerd worden zijn onder te verdelen in 4 categorieën:

1. Proces gerelateerde maatregelen: implementeer de bedrijfsprocessen zodanig dat rekening wordt gehouden met zaken als extra toegangsrechten en principes als data-minimalisatie, doelbinding en transparantie;
2. Technische maatregelen: pas digitale bescherming toe op deze gegevens door gebruik te maken van diverse voorhanden zijnde oplossingen zoals encryptie, pseudonimisering, automatische en verplichte dataclassificatie, data loss prevention (DLP), cloud access broker (CAS) en monitoring via SOC/SIEM dienstverlening. Het cloud platform van Microsoft (Office 365) beschikt al over veel oplossingen die hierbij kunnen helpen;
3. Juridische maatregelen: zorg ervoor dat dataverwerking van categorie 3 informatie alleen in Nederland plaatsvindt;
4. Personele maatregelen: zorg voor voldoende bewustzijn en training van de werknemers die met categorie 3 informatie werken.

9.5 Marktontwikkelingen t.a.v. BYOD (vraag 49)

Het dominante beeld van de markt is dat BYOD niet of nauwelijks binnen de publieke sector wordt gebruikt. Enkele respondenten adviseren om het Choose Your Own Device (CYOD) concept te gebruiken als alternatief voor BYOD. Bij COYD kiest een medewerker uit een aantal door de werkgever geselecteerde devices waarvan vooraf is vastgesteld dat deze kunnen voldoen aan het vigerende security- en privacy beleid. De devices worden "company owned" ingericht waarbij privégebruik desgewenst is toegestaan.
Verder geven enkele respondenten aan dat het vandaag de dag wel mogelijk is om binnen de O365 omgeving van Microsoft apparatuur te beheren en te beveiligen waarbij de privéinformatie van het apparaat ongemoeid kan blijven. Wel kan dit voor mogelijke functionele beperkingen zorgen zoals bijvoorbeeld het niet kunnen downloaden van een zakelijk document op het device.

9.6 Vertrouwelijke informatie i.r.t. public cloud diensten (vraag 50 t/m 51)

Het dominante marktbeeld is dat gegevens t/m vertrouwelijkheidsklasse 1 (VK-1 of bedrijfsvertrouwelijk) in de public cloud opgeslagen kunnen worden. Voor hogere vertrouwelijkheidsklassen is er geen dominant marktbeeld. Een enkele leverancier adviseert om deze gegevens on-premise op te slaan. Andere respondenten geven aan dat opslag van deze gegevens in de public cloud mogelijk is indien hier aanvullende maatregelen voor genomen worden (bijvoorbeeld het toepassen van encryptie of het beperken van de verwerking van dergelijke gegevens tot de landsgrenzen van Nederland).

De respondenten gaan niet concreet in op de vraag over de wijze waarop compliance aan EU én NL privacy- en security wet- en regelgeving binnen de door hun voorgestelde verkaveling is geborgd. Wel geven een aantal respondenten een aantal concrete aanbevelingen om compliance aan EU én NL privacy- en security wet- en regelgeving te bevorderen, namelijk:

1. Verwerk niet teveel persoonsgegevens waar dat niet nodig is. Bij voorkeur zijn alle diensten rondom de ondersteuning van de eindgebruiker in één kavel belegd. Dit betekent dat het ook alleen in dat kavel noodzakelijk is om persoonsgegevens van medewerkers van UWV te verwerken.
2. Houdt functioneel beheer van primaire systemen zoveel mogelijk bij UWV zodat leveranciers ook geen toegang (nodig) hebben tot privacy gevoelige informatie op deze systemen.
3. Pas privacy- en security by design toe bij alle kavels en stel een multidisciplinair team van experts aan om privacy- en security compliance verder uit te werken, te testen en te borgen in vervolg trajecten (o.a. aanbestedingen).

10 Maatschappelijk verantwoord ondernemen (vraag 52 t/m 54)

10.1 Huidige situatie

UWV hecht grote waarde aan maatschappelijk verantwoord ondernemen en onderschrijft de internationale normen op dat gebied, onder andere door het verbieden van kinderarbeid een eerlijke beloning en zorg voor het milieu. UWV hecht eveneens grote waarde aan het inzetten van medewerkers met een afstand tot de arbeidsmarkt en stelt hier bij verwervingstrajecten ook eisen aan.

10.2 Impact MVO op verkaveling (vraag 52)

Het dominante marktbeeld is dat MVO geen effect heeft op de verkaveling en/of de sourcing strategie. Alle respondenten geven in meer of mindere mate een eigen invulling aan MVO.

10.3 Inhoud eisen UWV met betrekking tot MVO (vraag 53 en 54)

Alle respondenten zijn bereid afspraken te maken over MVO. Sommigen respondenten geven wel aan dat het te 'rigide' eisen stellen als 'knock-out' criteria kan leiden dat op inhoud van dienstverlening interessante leveranciers worden uitgesloten. Dit omdat ze mogelijk niet letterlijk kunnen voldoen aan de eisen die daarover zou kunnen stellen. Dit terwijl ze wel graag bereid zouden zijn met UWV in overleg te gaan om invulling te geven aan MVO in de geest van de eisen van UWV binnen de redelijke mogelijkheden van de betreffende leverancier.

Meeste respondenten geven verder aan dat zij een verantwoordelijkheid hebben in het recyclen van hardware. Hoe dat wordt ingevuld verschilt veelal per leverancier.

Respondenten hebben geen antwoord gegeven op het effect van MVO eisen op de prijsstelling.

11 Bijlagen

11.1 Bijlage-001: Marktconsultatie KWNTC info doc leveranciers v1.1 20200512.docx

11.2 Bijlage-002: NVI MC KWNTC Totaal v1.0 20200513.pdf