



2.1 Project startarchitectuur

S/4HANA vooronderzoek

Datum: 03-12-2019

Plaats: Den Haag

Auteurs: H.G.A. de Vreede, P.G.J. Gillis, A. Verdoes, H.P. Verkouter, J.V. Aalten, E.P.M. van Putten.

Versie: 1.0

Documentbeheer				
Versie	Status	Auteur(s)	Datum	Opmerking
0.1	Concept	Erik van Putten	16-09-201	Eerste opzet
0.2	Concept	Erik van Putten, H.G.A. de Vreede	29-10-2019	Revisie na SAP sessies
0.3	Concept	Erik van Putten, H.G.A. de Vreede	05-11-2019	Revisie na Architectuur sessies
0.4	Concept	Erik van Putten, H.G.A. de Vreede	11-11-2019	Revisie na Architectuur sessies
0.45	Concept	Erik van Putten, H.G.A. de Vreede, J.V. Aalten, P. Gillis, A. Verdoes	18-11-2019	Revisie na Architectuur sessies
0.47	Concept	Erik van Putten, H.G.A. de Vreede, J.V. Aalten, P.J.G. Gillis, H.P. Verkouter, A. Verdoes	19-11-2019	Pencorrecties
0.60	Concept	Erik van Putten, H.G.A. de Vreede, J.V. Aalten, P.J.G. Gillis, H.P. Verkouter, A. Verdoes	22-11-2019	Oplevering TL & QA
0.62	Concept	Erik van Putten, H.G.A. de Vreede, J.V. Aalten, P.J.G. Gillis, H.P. Verkouter, A. Verdoes	03-12-2019	Verwerking review SAP
0.63	Concept	Erik van Putten, H.G.A. de Vreede, J.V. Aalten, P.J.G. Gillis, H.P. Verkouter, A. Verdoes	03-12-2019	Verwerking collegiale review
0.64	Concept	Erik van Putten, H.G.A. de Vreede, J.V. Aalten, P.J.G. Gillis, H.P. Verkouter, A. Verdoes	12-12-2019	Aanpassing organisatie naar nieuw model
1.0	Finaal		19-12-2019	Finale versie

Deloitte Consulting B.V. is ingeschreven bij de Kamer van Koophandel en Fabrieken te Amsterdam onder nummer 33259541. Deloitte Consulting B.V. is a Netherlands affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited.

Inhoud

1	Introductie	6
1.1	Context PSA	6
1.2	Doel PSA	6
1.3	Structuur van dit document	6
1.4	Doelgroep	6
1.5	Rollen en verantwoordelijkheden PSA	7
2	Project aanleiding	8
2.1	Samenvatting	8
2.2	Doel	9
2.3	Stakeholders	9
2.4	Bedrijfsdrijfveren	9
2.4.1	Inleiding	9
2.4.2	Defensie	10
2.4.3	JIVC	10
2.5	Architectuurdrijfveren	11
2.5.1	Criteria voor selectie van inrichtingsalternatieven	11
3	Bedrijfsarchitectuur	13

3.1 Effect op de Organisatie	13
3.1.1 Afbakening & kaders Organisatie	13
3.1.2 Bedrijfsactoren/-rollen Interne organisatie (binnen Min. V. Defensie)	13
3.1.3 Bedrijfsactoren/-rollen Externe organisatie	13
3.2 Normen, standaarden en principes	14
3.2.1 Architectuur beoordelingscriteria	14
3.2.2 Gebruikt model	14
3.3 Ontwerpbeslissingen Applicatie & technische architectuur	14
3.4 Architectuur punten relevant voor NON-SAP componenten geraakt in migratie	17
3.5 Architectuur open punten applicatie architectuur	17
4 Applicatie architectuur	18
4.1 Dataobjecten (informatiemodel)	19
4.2 Applicaties services	20
4.3 Applicatiefuncties (Logische applicatie)	20
5 Technische Architectuur	23
5.1 Systeemcomponenten	23
5.1.1 Huidige configuratie	23
6 Beveiliging	24
6.1 Informatiebeveiliging	24
6.2 Beveiligingsbesturing	24
7 Informatie governance	26
7.1 Informatie-eigenaarschap en -beheer	26
7.2 Mitigatie op de wettelijk kaders en eisen (compliance)	26
7.3 Privacy	26
7.4 Retentie en verwijdering	26
7.5 Overige kaders	27
8 Beheerketen	28
8.1 Kwalitatieve analyse beheerinspanning in de End State (M&F + GII)	28
8.2 Kwantitatieve analyse beheerinspanning End State (M&F + GII)	29
9 Eisen SAP infrastructuurlandschap S/4HANA	31
10 Architectuur beschouwingen	34
10.1.1 Cloud & Hosting	34
10.1.2 Gebruikersinterface	36
10.1.3 Infrastructuur	38

10.1.4 Dataveiligheid	40
10.1.5 Landschapscomplexiteit, beheer & Ontwikkeling	41
10.1.6 Applicaties & Interoperabiliteit	41
11 Acceptatiecriteria in het kader van het vooronderzoek	43
12 Relatie met andere deelproducten	44
12.1 Input van deelproduct	44
12.2 Input voor deelproduct	44
13 Akkoord	45
14 Bijlage(n)	46
A.1 Architectuurbeslissingen	46
A.2 NON-SAP Add-ons in de migratie	62
A.2.1 Nextlabs	63
A.2.2 Runbook	64
A.2.3 Every Angle	66
A.2.4 B Wise	67
Bijlage 2 Gerelateerde (en BRON) DOCUMENTATIE	68
A.3 Bijlage 4 Lijst Gebruikte afkortingen	69

1 Introductie

Dit stuk vormt het deelproduct "2.1 Project Startarchitectuur" binnen het vooronderzoeksproject S/4HANA migratie. Het document template deels wijkt af van het standaard vooronderzoek template vanwege het feit dat er een standaard Defensie template voor wordt ingezet, welke aansluit bij de projectstandaarden van Project Portfolio Management (PPM) van JIVC.

1.1 Context PSA

Als onderdeel van het "Werken onder Architectuur" wordt de globale oplossingsrichting voor een project vastgelegd in de Project Start Architectuur (PSA). De PSA is de vertaling van de totale (Corporate Defensie) architectuur naar de specifieke situatie omgeving van een project.

1.2 Doel PSA

Het doel van een PSA is om een project een concrete, relevante en praktisch realiseerbare scope mee te geven zodat het projectresultaat past in het grotere geheel van de organisatie. De PSA zorgt er ook voor dat er wordt nagedacht over risico's en dat zo veel mogelijk de huidige kennis en componenten worden hergebruikt. De PSA wordt gemaakt aan het begin van het project of in dit geval als onderdeel van een breder vooronderzoek.

1.3 Structuur van dit document

- H2 Project aanleiding: beschrijft de context en redenen voor het project. Wat voor soort project is het, welke doelen, voor wie, etc.
- H3 Businessarchitectuur: welke processen, organisatieonderdelen en producten/diensten worden geraakt door het project.
- H4 Applicatie (Informatie)architectuur: beschrijft architectuur, welke functionaliteiten zullen gerealiseerd worden en welke informatieobjecten en services worden hierdoor geraakt.
- H5 Technische architectuur: beschrijft de Technische architectuur voor dit project.
- H6 Beveiliging: beschrijft de bestaande beveiligingsarchitectuur en nieuwe beveiligingseisen.
- H7 Informatie Governance: beschrijft wie verantwoordelijk is voor de levenscyclus van de informatieobjecten. En de (wettelijke) kaders, die van toepassing zijn op het informatiedomein waar de informatie-eigenaar verantwoordelijk voor is
- H8 Beheer: beschrijft de componenten die in de operationele situatie beheerd gaan worden.
- H9 Eisen: beschrijft de eisen die SAP stelt aan een S/4 HANA infrastructuurlandschap.
- H10 Acceptatiecriteria: beschrijft de acceptatiecriteria voor dit document in het kader van het vooronderzoek.
- H11 Relatie: beschrijft de relatie van dit product tot andere producten.

1.4 Doelgroep

De doelgroep van de PSA zijn de leverancier, projectleiders en projectmedewerkers van het project, de CIO-office en anderen die deze architectuur inhoudelijk moet kennen om zijn/haar rol goed in te kunnen vullen.

1.5 Rollen en verantwoordelijkheden PSA

In onderstaande modellen worden de rollen en verantwoordelijkheden van de personen die bij het schrijven van een PSA betrokken zijn weergegeven.

Rollen/verantwoording van het document:

ROL	RACI
Opdrachtgever/PE	A
Vooronderzoeksprojectteam/ JIVC	R
Enterprise Architect	C
Portfoliomanager	I

Rollen/verantwoording per hoofdstuk:

ROL	ORG	Project aanleiding	Business architectuur	Applicatie (informatie) architectuur	Technische architectuur	Informatie Governance	Beveiligings architectuur	Beheer	Bijlage 1&2
Opdrachtgever/PE	BV	A	A	A	A	A	A	A	A
"Business Analyst" BV			R	S		S	S		S
IV-Manager BV		S	S			R	R	S	S
Vooronderzoeksprojectteam / JIVC	JIV C	R	S	R	S	S	S	R	R
Projectmanager JIVC		S	S	S	S	S	S	S	S
Applicatie Beheerder				S	S				
Technisch verantwoordelijke				S	R				
Sr. Supplier JIVC		I		I	I	I	I	C	I
Enterprise Architect		C	C	C	C	C	C	C	C
Informatie Beveiliging						S	S		
Informatie Beheer						C			
Solution Architecten				C	C				

2 Project aanleiding

Dit document bevat de Project Start Architectuur voor het *S/4HANA migratie vooronderzoek* en is één van de deelproducten van het gehele vooronderzoek.

2.1 Samenvatting

- Het huidige SAP HANA landschap voldoet nog tot 2021 (regulier vervangingsmoment vanuit LCM), dit is door SAP in de Migration planning Workshop en de Technische Architectuur workshop getoetst. Twee uitersten zijn hier als basis genomen: alle applicaties in decentrale omgevingen (MDG, S/4HANA, EWM, TM) en een scenario waarbij alle applicaties centraal bestaan. Vóór vervanging van het landschap moeten er detailsizing projecten voor de individuele applicaties worden uitgevoerd.
- Voor de componenten welke in de SAP Roadmap (Product Availability Matrix) geen opvolging is aangegeven is door SAP separaat een uitspraak gedaan t.b.v. opvolging van deze producten. (CUA, SLD, PI-AEX, LAMA, Solman);
- De technische monitoring functionaliteit van de Solution Manager wordt vervangen door het Focussed Run product, overige modules CHaRM en ITSM blijven in de Solution Manager welke volgens SAP een opvolging krijgt die nog niet in de roadmaps worden genoemd;
- De complexiteit van het landschap wordt d.m.v. architectuur beoordelingsregels meegenomen in de beoordelingscriteria. Hierdoor wordt in mogelijke keuzes beoogt alternatieven met minder complexiteit te kiezen
- De eisen voor een nieuwe SAP HANA infrastructuur zijn hiervan afgeleid en geven aan in lijn te moeten blijven met de huidige (en toekomstige) datacenter richtlijnen. Afwijkende infrastructuur heeft een kostenverhogend effect op het beheer en de exploitatie. Het SAP TDI model voldoet aan de huidige en toekomstige eisen, voor zover de nu aanwezige kennis.
- SAP HANA V3.0 roadmap onduidelijk en kan van invloed zijn op de vervangingsinvestering in 2021, de HANA versie heeft een directe koppeling met de versie van S/4HANA. SAP kan hier nog geen nadere informatie over verstrekken.
- Impact op beheer is in eerste instantie niet hoog bij migratiescenario "Hergebruik", voor de technische migratie alleen vergelijkbaar met een forse technische release. De optimalisatie & standaardisatie projecten erna in dit scenario zullen de totale druk op de beheer organisatie onder controle moeten houden bij het bepalen van exacte scope en parallelle executie. In het geval van migratiescenario's 'Gefaseerde nieuwe implementatie' en 'Gefaseerde hybride implementatie' ligt dit in de eindsituatie (vanaf 2026) gelijk voor alle scenario's maar is de beheer inspanning gedurende de migratie uitvoering hoog door het langdurig ondersteunen van zowel de oude als de nieuwe omgeving, inclusief de onderlinge koppelingen.
- S/4HANA binnen de Publieke Cloud oplossingen van SAP zijn voor Defensie op dit moment nog niet van toepassing om diverse redenen:
 - De huidige Defensie oplossing DFPS zit niet in de S/4HANA Cloud oplossing op dit moment. Voor de toekomstige D&S oplossing is dit nog niet helder;
 - Niet alle overige Defensie specifieke oplossingen zitten in de S/4HANA Cloud oplossing;
 - Delen zelfbouw zijn lastig tot niet realiseerbaar in de S/4HANA Cloud oplossing;
 - Er is een Defensie Cloud routekaart welke aangeeft wat de Defensie brede richting kan en mag zijn conform Wet en Regelgeving. De huidige Cloud routekaart geeft aan dat DEP-V gegevens niet naar een publieke Cloud omgeving mogen worden verplaatst;
 - De laatste systeem rubricering is hoger (TBB-2) dan de huidige (TBB-4) en beperkt deze gang in nog hogere mate, TBB-2 is namelijk niet benoemd in de Cloudroutekaart maar wordt uitgesloten omdat TBB-4 niet mogelijk is;
- S/4HANA Private Cloud oplossingen, mits voldoende geborgd door partner certificeringen, uitgevoerd met de juiste SAP producten (momenteel de On-Premise versies) kunnen dezelfde oplossing bieden dan de huidige On-Premise oplossing.

- De voorgestelde migratieroutes, via een migratie naar de S/4HANA On-Premise oplossing, middels proces standaardisatie, naar gebruik van SAP Cloud producten wordt volledig ondersteund door SAP. De On-Premise oplossingen zoals voorgesteld door het vooronderzoek bevatten in de eind-architectuur juist allerlei oplossingen van SAP om te kunnen koppelen met Cloud Producten. Dit biedt de mogelijkheid Artificiële Intelligentie, Machine Learning, Analytics, proces integratie, UI ontwikkeling en aanpassingen in een flexibele schil in te zetten waarin toegevoegde waarde wordt gegeven. Randvoorwaardelijk is dan wel dat er voldoende beleidsmatig en vanuit beveiligingsoptiek naar deze oplossingen wordt gekeken. Indien dit niet of te laat door de Defensie organisatie wordt opgepakt worden leveranciers bewegingen naar de Publieke Cloud bedreigend voor de Defensie organisatie. De beweging van de Publieke Cloud oplossing naar de Private Cloud, helpt uiteraard tevens in het realiseren van een werkbare eindoplossing;
- Uiteindelijk kan de Cloud route er voor Defensie dan als volgt uit zien:
 - Nu naar S/4HANA On-Premise;
 - Later naar een hybride situatie met toevoeging van Private Cloud oplossingen;
 - De eindsituatie zou een volledige Private Cloud kunnen zijn, of wellicht een hybride situatie met Private en Publieke Cloud onderdelen, ook voor On-Premise is hier nog steeds ruimte;

2.2 Doel

De behoefte van JIVC is de diverse applicaties in hun lifecycle te kunnen blijven volgen. Door de juiste versie van een applicatie te gebruiken blijft de ondersteuning van de leverancier geborgd. Tevens zal de integraliteit en de afhankelijkheid van applicaties en services beter op elkaar blijven aansluiten. De systemen kunnen dan sneller met nieuwe technologische ontwikkelingen mee en dat past weer binnen de IT strategie van Defensie.

Zie voor het bredere doel van de hele S/4HANA transitie het overkoepelende Plan van Aanpak voor dit vooronderzoek en het uiteindelijke eindrapport. Dit document is slechts een deel van het totale eindrapport "Vooronderzoek S/4HANA migratie".

Afgeleide doelen voor dit PSA:

- Betere ondersteuning in de Front-end applicatie door andere processen en gemoderniseerde webgebaseerde gebruikersinterface voor eindgebruikers & beheerders
- Gegarandeerde ondersteuning door de leverancier
- Gereed voor toekomstige ontwikkelingen binnen het materieellogistieke en financiële domein

2.3 Stakeholders

Zie deelproduct stakeholder analyse.

2.4 Bedrijfsdrijfveren

2.4.1 Inleiding

ERP M&F is de IT-omgeving die Defensie gebruikt als basisadministratie voor de ondersteuning van het materieellogistieke en financiële domein. Deze is gebaseerd op de software van SAP. De leverancier heeft aangekondigd het huidige platform ERP te gaan vervangen door een nieuw platform S/4 HANA. Dit betreft een ingrijpende vernieuwing. De leverancier heeft aangekondigd dat na 2025 de ondersteuning van het huidige platform zal worden beëindigd. Hiermee lijkt de migratie met name IT-gedreven te zijn. Echter het nieuwe S/4HANA platform biedt het fundament om de ambities van Defensie op het gebied van informatievoorziening op termijn mogelijk te maken.

2.4.2 Defensie

Zowel de dreiging waartegen, als de omgeving waarin de krijgsmacht opereert veranderen snel. Goed en modern werkgeverschap vragen eveneens een flexibele voorziening in informatie en middelen om het werk te kunnen doen. Bovenstaande ontwikkelingen vergen dat Defensie gaat handelen vanuit een ander paradigma. Daarbij is informatiegestuurd optreden het uitgangspunt. IT en de beschikbare data worden leidend. Het gaat om effectieve inzet van informatie voor zowel operationele- als ondersteunende processen en het bevorderen van de samenwerking daartussen. Ook in ondersteunende processen is met technologische vernieuwing veel efficiënter te werken. Neem bv. Internet of Things (IoT), sensoren, augmented/virtual reality, robotic process automation (RPA).

Dit nieuwe paradigma vraagt excellente centrale IT-basisvoorzieningen, aangevuld met voorzieningen voor decentraal gebruik. Met betrouwbare data en moderne IT-middelen om te analyseren, krijgt Defensie snel nieuwe inzichten (Fact Based) om sneller (bij) te kunnen sturen en vooruit te kijken.

Inzichten uit data-analyse maken de materiële gereedstelling effectiever en efficiënter. Denk aan analyses voor doorlooptijden en bestelmomenten van reservedelen zodat het onderhoud tijdig valt uit te voeren. Of predictive maintenance, waarbij een voertuigsignaal aangeeft dat een onderdeel moet worden vervangen. Nauwkeurige analyse maakt het mogelijk preventief en dus tijdig onderhoud te plegen. Het opstellen van eenduidige rapportages met cost-to-readiness-modellen vergroot de transparantie en voorspellende waarde van de gereedstelling.

Het IT-fundament neerzetten vergt de ontwikkeling van vijf strategische thema's:

1. IT is robuust. De IT kent een hoge beschikbaarheid, is betrouwbaar en toekomstbestendig;
2. IT is wendbaar. De organisatie speelt in op technologische veranderingen en schaaft snel op- en af in benodigde capaciteit. Ook stelt de IT-organisatie de business in staat van mogelijkheden van (nieuwe) technologie te profiteren;
3. IT is digitaal weerbaar. De IT moet voldoen aan wet- en regelgeving op het gebied van privacy en data-bescherming. De IT moet inherent veilig en compliant zijn ingericht;
4. IT is data gedreven. De organisatie moet deze data, effectief ondersteund door IT, snel verzamelen, analyseren, presenteren en verspreiden;
5. IT is interoperabel. De IT ondersteunt dit door informatie veilig uit te wisselen binnen Defensie, met internationale militaire organisaties en externe partijen. Afstemming op elkaar vergt standaarden, protocollen en procedures. Een tweede vorm van interoperabiliteit is de koppeling van Operationele Technologie (OT) met Informatie Technologie (IT). Veel operationele technologie (apparatuur) heeft eigen informatie verwerkende capaciteiten. Vaak heeft de apparatuur eigen sensoren en werkt alleen optimaal bij een verbinding met achterliggende IT.

2.4.3 JIVC

Het fundament onder de doorontwikkeling van IT als integrale enabler rust, volgens de Defensie Visie op IT, op de volgende drie pijlers:

1. Continuïteit. De betrouwbaarheid van de IT is van wezenlijk belang. Zonder goed functionerende en betrouwbare IT geen inlichtingen, geen missies, geen bedrijfsvoering en dus geen goed functionerende krijgsmacht;
2. Beveiliging. De aard van de krijgsmacht stelt hoge eisen aan de beveiliging. De beveiliging van IT-systemen en de integriteit van data moeten dan ook gegarandeerd zijn;
3. Innovatie. Met de ambitie om goed voorbereid te blijven op een scala aan inzetmogelijkheden is het noodzakelijk om slim gebruik te maken van nieuwe mogelijkheden.

Een belangrijke voorwaarde om de continuïteit te kunnen garanderen is dat JIVC gebruik maakt van producten waarop door de leverancier ondersteuning wordt geleverd. SAP heeft aangekondigd dat per 1-1-2026 de ondersteuning van het huidige SAP R/3 platform wordt beëindigd. Hetgeen dit onderzoek voor de transitie naar het S/4HANA platform noodzakelijk maakt.

Alle nieuwe ontwikkelingen van SAP zullen op het S/4HANA platform worden gebaseerd. De transitie naar dit platform is dan een randvoorwaarde om bij deze innovatieve ontwikkelingen aan kunnen sluiten.

2.5 Architectuurdrijfveren

Vanuit een architectuurperspectief zijn de volgende drijfveren relevant:

- **Complexiteitsreductie:** SAP heeft in de afgelopen jaren verschillende producten op de markt gebracht die apart geïnstalleerd moesten worden. Hierdoor is er een complex SAP landschap met interfaces ontstaan. Met S/4HANA biedt SAP, voor een aantal producten, de mogelijkheid deze in één installatie samen te voegen (de zogenaamde embedded variant). Complexiteitsreductie resulteert o.a. in een effectiever en efficiënter beheer.
- **Best Practices;** de inzet van S/4HANA biedt de mogelijkheid terug te gaan naar de Best Practices van SAP, voor zover hier bij de huidige inrichting van af geweken is. Dit geldt zowel voor de inrichting van processen als de infrastructuur.

2.5.1 Criteria voor selectie van inrichtingsalternatieven

Voor de inrichting van het IT-fundament van het SAP Landschap zijn verschillende alternatieven beschikbaar. Om de verschillende alternatieven te kunnen afwegen zijn selectiecriteria opgesteld. In de selectiecriteria zijn de architectuurdrijfveren meegenomen. De selectiecriteria zijn gekoppeld aan de vijf strategische thema's zoals eerder in dit stuk beschreven.

IT is robuust:

- **Continuïteit:** Continuïteit, ongoing support, van de bedrijfsvoering is een belangrijk gegeven binnen Defensie. Defensie heeft operaties die 7 x 24 actief zijn.
- **Autonomie:** Naast continuïteit is autonomie van de bedrijfsvoering een belangrijk gegeven binnen Defensie. Dit criterium is slechts van toepassing voor eenheden die in staat moeten zijn voor kortere of langere tijd zelfstandig te kunnen opereren.
- **Beheer:** Beheer van de IT moet effectief en efficiënt zijn. De personeelsfactor is een belangrijke kostenpost.
- **Toekomstvastheid:** De oplossing blijft toepasbaar in de toekomst.
- **Best practices:** De IT is ingericht op betrouwbaarheid en efficiency conform best practices. Defensie tracht adapter te zijn van beproefde technologie. Hierdoor kan gebruik worden gemaakt van de best practices en ervaringen in de markt. Daarnaast is dit punt van belang voor het verkrijgen resources ten behoeve van de inrichting, beheer en support van de IT.

IT is wendbaar:

- **Schaalbaarheid:** Schaalbare IT zorgt dat Defensie snel en flexibel kan inspelen op veranderende vraag vanuit de organisatie. Schaalbaarheid reguleert bovendien kosten en baten van IT optimaal. Schaalbaarheid geldt voor zowel dataopslag, rekencapaciteit als ook het aantal gebruikers dat bediend kan worden.
- **Uniformiteit:** Op basis van het train-as-you-fight principe verdient het de voorkeur dat ook de IT zowel op de vredeslocatie als in het inzetgebied een grote mate van uniformiteit kent.
- **Gebruiksgemak/vriendelijkheid:** gebruiksgemak/vriendelijkheid is een voorwaarde om IT snel te kunnen veranderen zonder dat hiervoor uitgebreide opleidingen voor nodig zijn.

IT is digitaal weerbaar:

- **Beveiliging:** De beveiliging bij nieuwe IT is integraal onderdeel van het ontwerp van elke IT-component. In plaats van beveiliging van het hele netwerk wordt in de toekomst elk systeem, elke toepassing en elke dataverzameling individueel beveiligd. IT moet digitaal, procedureel én fysiek beschermd worden. Met betrekking tot beveiliging stelt Defensie betrouwbaarheidseisen bestaande uit beschikbaarheid, exclusiviteit en integriteit.

IT is data gedreven:

- **Performance:** De snelheid van het afhandelen van functies en opleveren van data door het systeem. De performance kan sterk uiteenlopen en bepaalt in hoge mate het al dan niet succesvol functioneren van een systeem.

IT is interoperabel:

- **Gebruik van civiele en militaire (open) standaarden:** Kiezen voor standaarden (infrastructuur, diensten, werkprocessen etc.) draagt bij aan robuuste en kosteneffectieve IT. Het gebruik van marktstandaarden verbetert onder meer interoperabiliteit, verhoogt de flexibiliteit, en biedt meer garantie voor de informatiebeveiliging.
- **Integratie:** integratie van systemen binnen Defensie is een vereiste om data uit te wisselen, soms over smalbandige verbindingen. Integratie van systemen kan complex zijn. Hoe eenvoudiger de integratie hoe hoger de waardering.

Total Cost of Ownership: De totale kosten die een product of dienst gedurende de hele levenscyclus of gebruikscyclus met zich meebrengen. Hoe lager de TCO des te hoger de waardering.

2.5.1.1 Waarderingen per criterium

5 = Voldoet volledig aan of draagt volledig bij aan het gestelde criterium

4 = Voldoet in hoge mate of draagt in hoge mate bij aan het gestelde criterium

3 = Voldoet aan of draagt bij aan het gestelde criterium

2 = Voldoet niet volledig aan of draagt niet volledig bij aan het gestelde criterium

1 = Voldoet in het geheel niet aan of draagt in het geheel niet bij aan het gestelde criterium

2.5.1.2 Wegingsfactoren per criterium

0-5 afhankelijk van zwaarte.

3 Bedrijfsarchitectuur

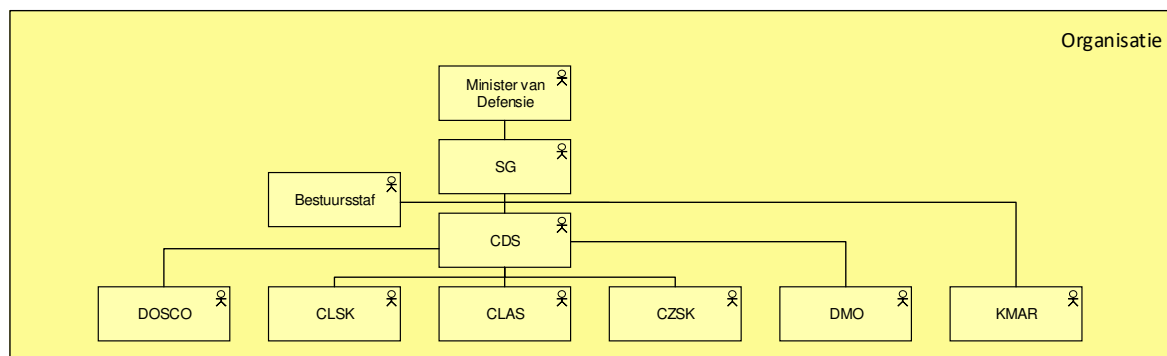
3.1 Effect op de Organisatie

De scope van het vooronderzoek migratie S/4HANA bevat minimaal de ondersteuning van de huidige gebruikers van de ECC applicatie. De huidige organisatie van ERP M&F wordt niet gewijzigd door het project. Als gevolg van dit project zullen er wel wijzigingen kunnen plaatsvinden op de bedrijfsprocessen van ERP M&F.

De beheerorganisatie wordt tevens belicht in het knelpunt over complexiteit.

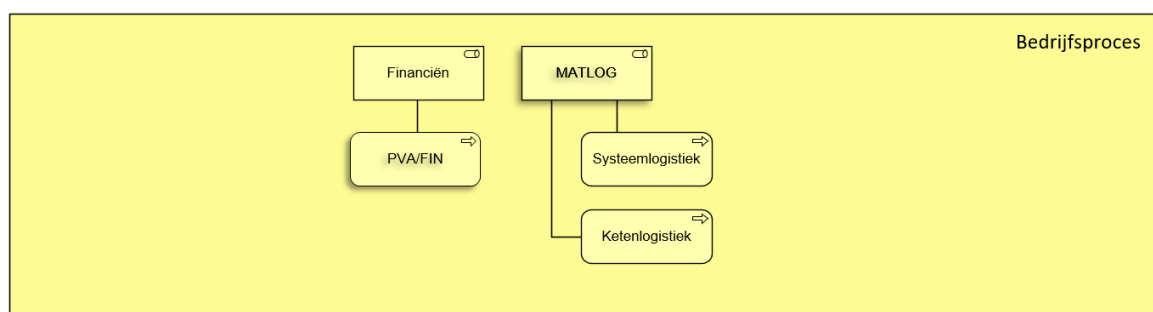
3.1.1 Afbakening & kaders Organisatie

De gehele Materieel Logistieke & financiële Defensieorganisatie wordt geraakt door de uitvoering van een migratie naar S/4HANA.



Figuur 1: Organisatie

3.1.2 Bedrijfsfactoren/-rollen Interne organisatie (binnen Min. V. Defensie)



Figuur 2: Bedrijfsprocessen

3.1.3 Bedrijfsfactoren/-rollen Externe organisatie

Onderstaande afdeling(en) zal (zullen) het resultaat van het project gaan gebruiken:

Organisatie onderdeel	Processen
-----------------------	-----------

CLAS	Financiële en Materieel logistieke processen
CLSK	Financiële en Materieel logistieke processen
CZSK	Financiële en Materieel logistieke processen
KMAR	Financiële en Materieel logistieke processen
DOSCO	Financiële en Materieel logistieke processen
DMO	Financiële en Materieel logistieke processen
Bestuursstaf	Financiële processen

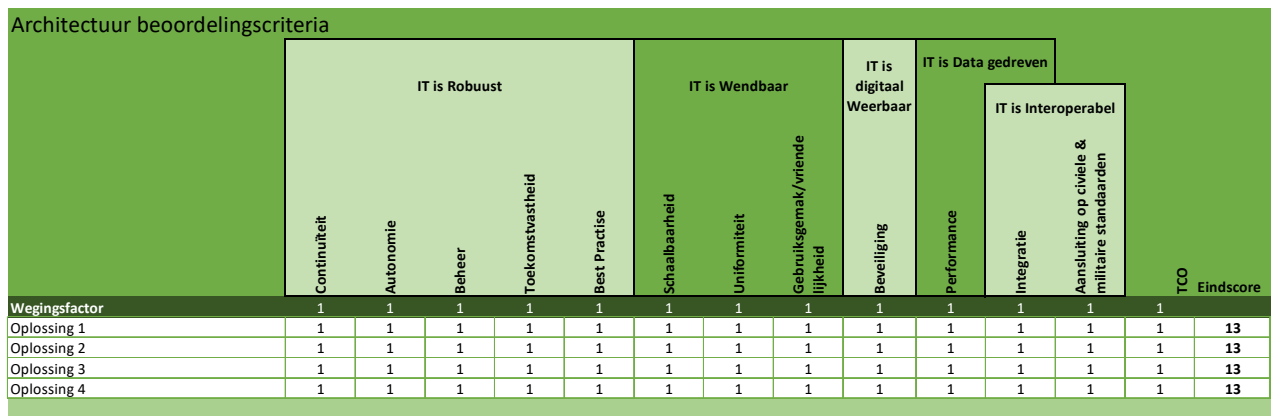
3.2 Normen, standaarden en principes

Bij de dienstverlening, bedrijfsvoering en informatievoorziening heeft ERP M&F qua 'normen' te maken met diverse Wet- en Regelgeving (militair en civiel), NATO standaarden en met professionele richtlijnen en qua 'standaarden' met o.a. protocollen en code systemen. Daarbij spelen v.w.b. de ondersteunende IT de principes en kaders van de defensiearchitectuur ook een belangrijke (sturende en kaderende) rol, deze zijn opgenomen in bijlage 2 van dit document.

3.2.1 Architectuur beoordelingscriteria

Gerelateerd aan de Defensie IT strategie zijn er architectuur beoordelingscriteria opgesteld. Zie tevens in de inleiding van dit stuk.

3.2.2 Gebruikt model



Figuur 3: Architectuur beoordelingscriteria

Wegingsfactoren zijn ingevoegd om criteria t.o.v. elkaar te kunnen positioneren. Omdat de werkgroep dit onderscheid niet kan maken vanuit de diverse beleidsdocumenten is de wegingsfactor voor alle criteria gelijk gehouden (=1).

3.3 Ontwerpbeslissingen Applicatie & technische architectuur

Overzicht ontwerpkeuzes en ontwerppatronen op basis van de geconstateerde knelpunten en afwijkingen t.o.v. de bestaande situatie. In eerste instantie een beknopt overzicht, in de bijlagen de detail uitwerking van ieder individueel knelpunt.

#	Functie gebied	In het vooronderzoek onderkende knelpunten	Reden, consequenties, risico's & mitigatie	Wanneer
1	Architectuur	Netwerkbandbreedte operationele werkplekken is te laag	Mogelijk blokkerend binnen de operationele werkplek, nadere POC test specifiek met deze werkplek noodzakelijk. Tevens testen met Browser Fiori Libs op een lokale fileserver als oplossing van SAP. Andere werkplek mogelijkheden als VDI zouden tevens een werkbare optie kunnen zijn.	Randvoorwaardelijk voor Fiori introductie op de operationele werkplek.
2	Architectuur	Fiori launchpad op IOS apparaten niet in de Defensie Appstore toegestaan	Niet meer van toepassing, SAP heeft de ondersteuning voor deze applicatie beëindigd. Vervangen door URL favoriet in de webbrowser.	N.v.t.
3	Security	Vertrouwelijke data via SAPRouter koppeling tbv S/4 diensten SAP (Readiness Check, BSR Report)	Activiteit frequent noodzakelijk tijdens de projectperiode en in beheer. Architecten bespreken met Security officer en schrijven SAP formeel aan.	Werkbare oplossing randvoorwaardelijk voor: migratie, standaardisatie & optimalisatie, beheer gedurende en na migratie
4	Architectuur	Werkplek voor operationeel optreden loopt achter in OS & browser versies	Momenteel 1 maal per jaar versieaanpassing van deze werkplek, dit vormt een kritische afhankelijkheid met de roll-out en de ondersteuning vanuit SAP (alleen laatste browserversies)	Randvoorwaardelijk dat er borging is tussen de webbrowser (product & versie) en de SAP migratie en beheer
5	Architectuur	SAP Fiori wordt maar op beperkt aantal browsers en versies ondersteund	Advies van SAP (gegeven in Fiori detail workshop) is de inzet de Google Chrome webbrowser. Overige browsers worden tevens ondersteunt, echter allen op de laatst, of voorlaatste beschikbare versie. Microsoft IE support vervalt in 2021.	Zie (4)
6	Beheer	Hoge complexiteit van de te beheren omgeving	Standaardisatie, simplificatie & optimalisatie binnen de projecten. Architectuur beoordelingscriteria op TCO en versimpeling van het landschap.	Randvoorwaardelijk te blijven sturen in architectuurbeleid op TCO
7	Beheer	Perceptie: Hoge hoeveelheid maatwerk	Onderzoek heeft aangetoond dat er een gering deel zou kunnen vervallen. Andere delen kunnen wellicht in overleg met de BV worden omgezet naar de	Randvoorwaardelijk het streven naar verlaging van maatwerk in beleid om te zetten. Goede

			SAP standaard. Daarnaast zijn er maatwerk aanpassingen die door interne standaarden worden afgedwongen (BW extractoren zijn kopieën van origineel, AO/IC heeft maatwerk tbv Wet en Regelgeving).	definities van maatwerk noodzakelijk om hierop te kunnen sturen
8	DataMgt	Materiaalnummer lengte aanpassing & veldinhoud	Oplossing beschreven in het deelproduct "D.14 - Data Plan van Aanpak", tevens escalatie naar SAP noodzakelijk op de niet toegestane speciale tekens in het veld (&*,!)	Zie Data deelproducten (D.14 PvA en 2.8 conversieplan)
9	DataMgt	Zakenpartner conversie nog niet uitgevoerd in ECC	Dit is een verplichting voor Migratie en als zodanig in de voorbereidende activiteiten opgenomen	Zie Data deelproducten (D.14 PvA en 2.8 conversieplan)
10	Architectuur	TM wel of niet in de S4Core	Keuze architectuur: Embedded	Uitgangspunt nieuwe architectuur
11	Architectuur	EWM wel of niet in de S4Core	Keuze architectuur: Embedded	Uitgangspunt nieuwe architectuur
12 a	Architectuur	Fiori Front-end server wel/niet in de S4Core	Keuze architectuur: Embedded	Uitgangspunt nieuwe architectuur
12 b	Architectuur	Fiori Front-end server wel/niet Hybride FLP configuratie	Keuze architectuur: FLP verbinding	Uitgangspunt nieuwe architectuur
13	Architectuur	Einde ondersteuning SAP Portaal 31-12-2024	Keuze architectuur: Uitfaseren en vervangen door FLP	Uitgangspunt nieuwe architectuur
14	Architectuur	Productopvolging SLD	Door SAP bevestigd dat er opvolging komt	Blijvende component
15	Architectuur	Productopvolging PI-AEX	Door SAP bevestigd dat er opvolging komt, echter keuze architectuur uitfasering door overname in GKD als vereenvoudiging van het landschap	Uitgangspunt nieuwe architectuur
16	Architectuur	Opvolging Nextlabs	Door MINDEF aangegeven als inzetbaar in S/4HANA na licentie discussie	Blijvende component
17	Architectuur	Opvolging CUA	Door SAP bevestigd dat deze functionaliteit in de opvolger van het NetWeaver product zit.	Blijvende component
18	Architectuur	Opvolging Solution Manager	Door SAP bevestigd dat de monitoring functie naar het product Focussed Run verplaatst en ChARM en ITSM in een opvolging van de Solution Manager aanwezig blijft.	Blijvende component voor ChARM en ITMS Nieuwe component voor Monitoring
19	Architectuur	Vervanging voor ontbrekende EH&S	Moet in voorbereidende projecten worden opgepakt. Of	Randvoorwaardelijk voor start migratie

functionaliteit in S/4HANA			nieuwe oplossingsrichting in S/4HANA of aanschaf ontbrekende functionaliteit d.m.v. losse SAP licenties	
20	Architectuur	BW operationele rapportages wel/niet naar de S/4core	Dit betreft geen architectuurkeuze, maar een inrichtingsvraagstuk. Derhalve dit punt beleggen in de optimalisatie & standaardisatie projecten waar de Analytics Fiori Apps worden ingezet. Op basis van overgebleven behoefte deze vraag nader beantwoorden.	In het ingeplande blok Analytics meenemen, richting vanuit architectuur is Operationele rapportage bij de bron, dus in S/4HANA
21	Architectuur	MDG wel/niet naar de S/4Core	Keuze architectuur: De-centraal laten bestaan, echter wel migreren naar een S/4HANA stack tbv ondersteuning op langere termijn	Randvoorwaardelijk project MDG-M naar eigen S/4HANA stack decentraal vóór 2025.

3.4 Architectuur punten relevant voor NON-SAP componenten geraakt in migratie

Nr	Functie gebied	In het vooronderzoek onderkende knelpunten	Reden, consequenties, risico's & mitigatie	Actie
1	Architectuur	Opvolging non-sap component Runbook	Runbook opvolging Smart Close bij leverancier Blackline	Randvoorwaardelijk component voor migratie
2	Architectuur	Opvolging non-sap component B Wise	Geen ADR extractie functionaliteit meer gecertificeerd door SAP	Randvoorwaardelijk dit te adresseren bij de ADR
3	Architectuur	Opvolging non-sap component EveryAngle	Nader onderzoek moet concluderen of dit product kan worden uitgefaseerd door Embedded Analytics functionaliteit in S/4HANA	Randvoorwaardelijk onderzoek voor migratie, opnemen in Embedded Analytics blok uit migratieplanning

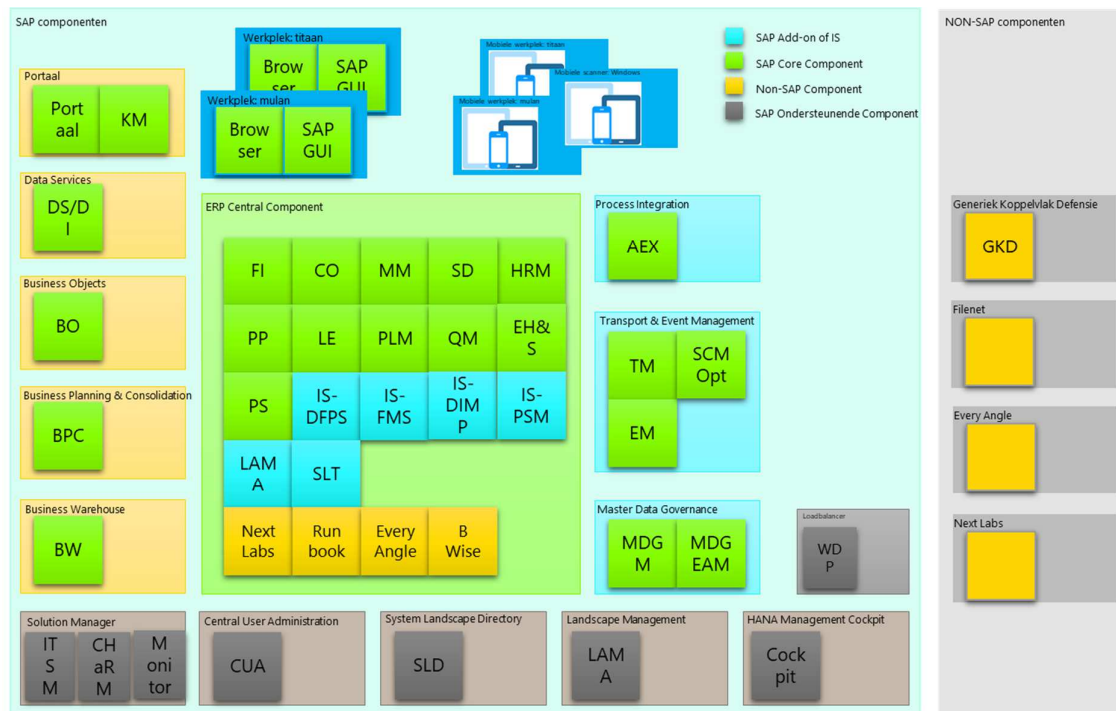
3.5 Architectuur open punten applicatie architectuur

In het project wordt afgeweken van de huidige architectuur. De volgende issues ten aanzien van de architectuur staan nog open:

Nr	Functie gebied	In het vooronderzoek onderkende knelpunten	Reden, consequenties, risico's & mitigatie	Actie
1		Nvt		

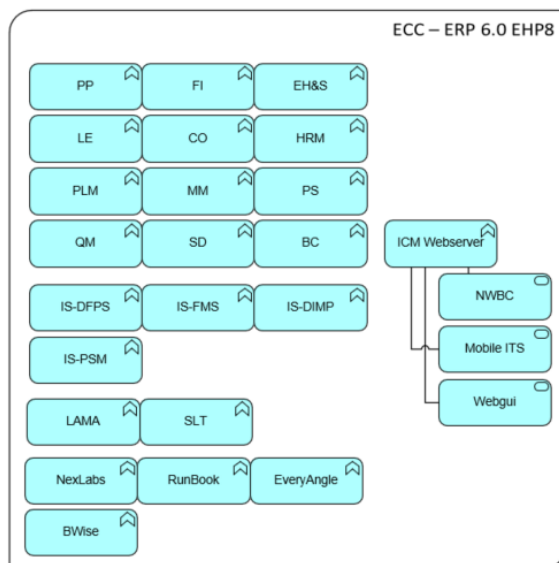
4 Applicatie architectuur

Onderstaande afbeelding toont de huidige situatie voor de totale ERP M&F omgeving.



Figuur 4: Huidige applicatie architectuur, inclusief alle direct aanpalende systemen

T.o.v. deze uitgangssituatie zal deze PSA de ontwikkeling naar de eindarchitectuur voor de totale ERP M&F omgeving schetsen. De scope van de S/4HANA migratie beperkt zich echter in principe tot het SAP ERP Central Component (ECC) deel van de ERP M&F omgeving.



Figuur 5: Huidige ECC Module architectuur

In het plan van aanpak is echter gesteld dat direct aanpalende SAP systemen e.d. worden meegenomen in de impact analyse.

4.1 Dataobjecten (informatiemodel)

Het project heeft impact op het gehele SAP ECC gegevensmodel en alle entiteiten en attributen.

Tijdens de migratie wordt het datamodel van ECC versimpeld naar het S/4HANA model. Binnen de financiële modules vervallen er een aantal tabellen en wordt er gemigreerd naar één nieuwe tabel: ACDOCA en binnen de Logistieke modules vervallen er tabellen welke zijn opgenomen in een nieuwe tabel: MATDOC.

De wijzigingen op het gegevensmodel met de grootste impact zijn:

- BP – Business partner:
 1. Klanten, Leveranciers, gebruikers etc. worden op een andere wijze afgebeeld in het systeem;
- Artikel:
 1. Artikelnummer: Veldlengte van 18 naar 40 posities;
 2. Karakters gebruikt in de nummering (Industriestandaards en NATO Stock nummer zoekfuncties)

Op hoofdlijnen gaat het om functionaliteiten binnen de volgende aandachtsgebieden:

- De BP omzetting is iets wat los staat van de S/4HANA migratie, echter rand voorwaardelijk is, dit is dan ook onderwerp van het deelproduct Voorbereiding. De BP omzetting heeft SAP al lange tijd geadviseerd maar is nog niet gerealiseerd binnen de ERP M&F oplossing. Het nieuwe

dataobject BP vervangt de oude entiteiten door rollen/functies van de BP. Een business partner kan de rol klant hebben maar tevens de rol leverancier. In de oude situatie waren dit twee losse entiteiten in het systeem.

Door deze introductie ontstaan er twee uitdagingen in het systeem:

1. Er wordt een dataobject BP geïntroduceerd, welke moet worden onderhouden in andere transacties met impact op werkwijze (look & feel) (opleiding en systeemdokumentatie)
 2. De oude objecten hebben een eigen nummering en zijn niet aan elkaar gekoppeld, de nieuwe BP objecten hebben eigen nummering en geven een relatie in gekoppelde objecten. Dit werkt door in het aanbrengen van relaties in het systeem en rapportage (analytics) op het systeem, c.q. interfacing met andere systemen als nummering moet worden omgezet.
- Artikelstam nummer
Dit nummer wordt vergroot van 18 posities naar 40 posities.
Het effect van de vergroting is een wijziging van het veld in bestaande programmatuur (std. SAP en zelfbouw) en interfaces.
 - Artikelnummer karakters
In artikelnummers komen karakters voor welke niet door S/4HANA worden ondersteund (";", "*", " ") bijvoorbeeld. Dit is niet iets wat Defensie alleen heeft toegepast maar wat tevens in industriestandaarden en i.c.m. NATO stocknummer zoekfuncties wordt gebruikt. Dit functioneerde in de ECC applicatie, maar niet meer in de S/4HANA applicatie. Hiervoor is een probleemmelding lopende bij SAP. In ticket #463873/2019 wordt een oplossingsrichting gegeven maar dat ligt niet in lijn met de wensen vanuit Defensie.

4.2 Applicaties services

De huidige ECC applicatie is in staat om op twee wijzen de gebruikers interface functionaliteit (Presentatie-integratie service) te bieden:

1. Middels het SAP GUI protocol en de SAP GUI gebruikers interface;
2. Middels de ICM (Internet Communication Manager) en de Webbrowser gebruikers interface.

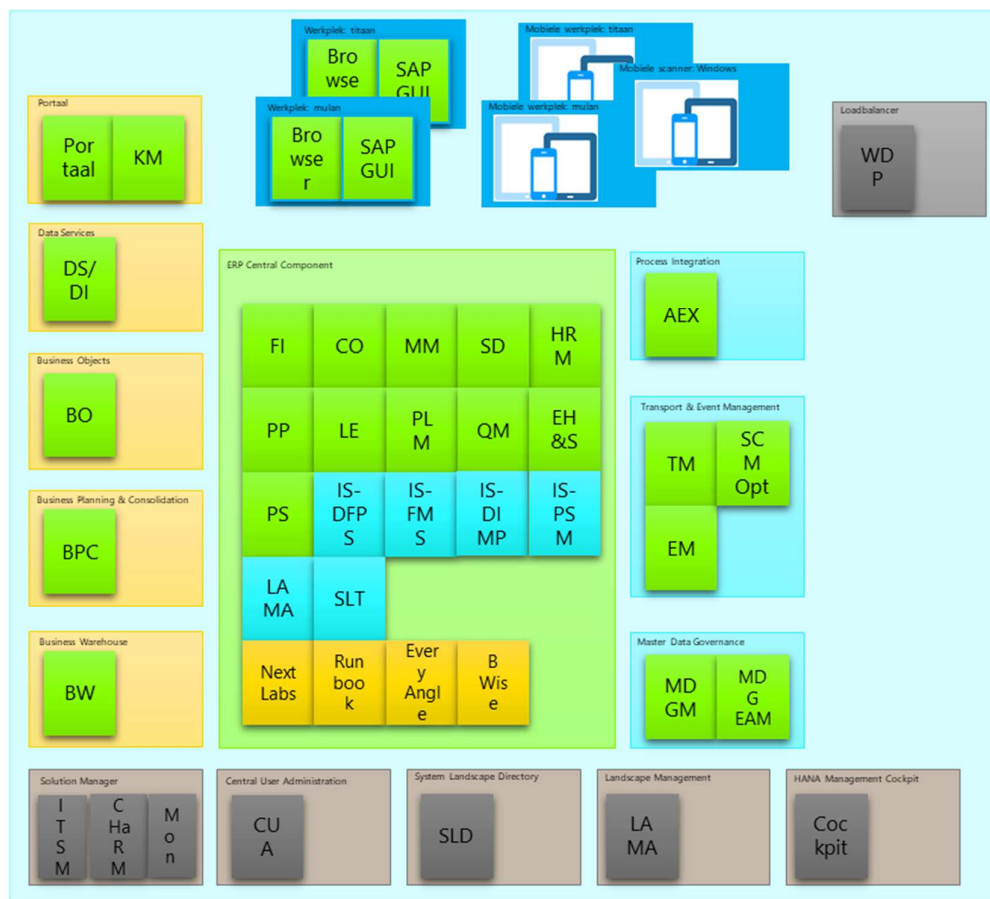
Beiden worden door het Ministerie van Defensie ingezet. De laatste met name voor de op Microsoft Windows Mobile gebaseerde handheld scanners die de MobileITS gebruiken en de NWBC (Netweaver Business Client) functionaliteit voor SAP in het portaal. De vraag is wel in hoeverre de Windows Mobile toekomstvast is. Zeer waarschijnlijk moet er voor deze oplossing op termijn vervanging komen. In principe blijven deze functionaliteiten ongewijzigd. De ICM met Webdynpro gebaseerde schermen worden tevens in Fiori rollen toegepast door SAP evenals de WEBgui gebaseerde standaard transacties via de ICM.

De Fiori Frontend server is een toegevoegde functionaliteit tbv representatie maar maakt gebruik van de ICM webserver t.b.v. de communicatie met webbrowsers.

Vanuit de POC is bovenstaande in de praktijk getoetst.

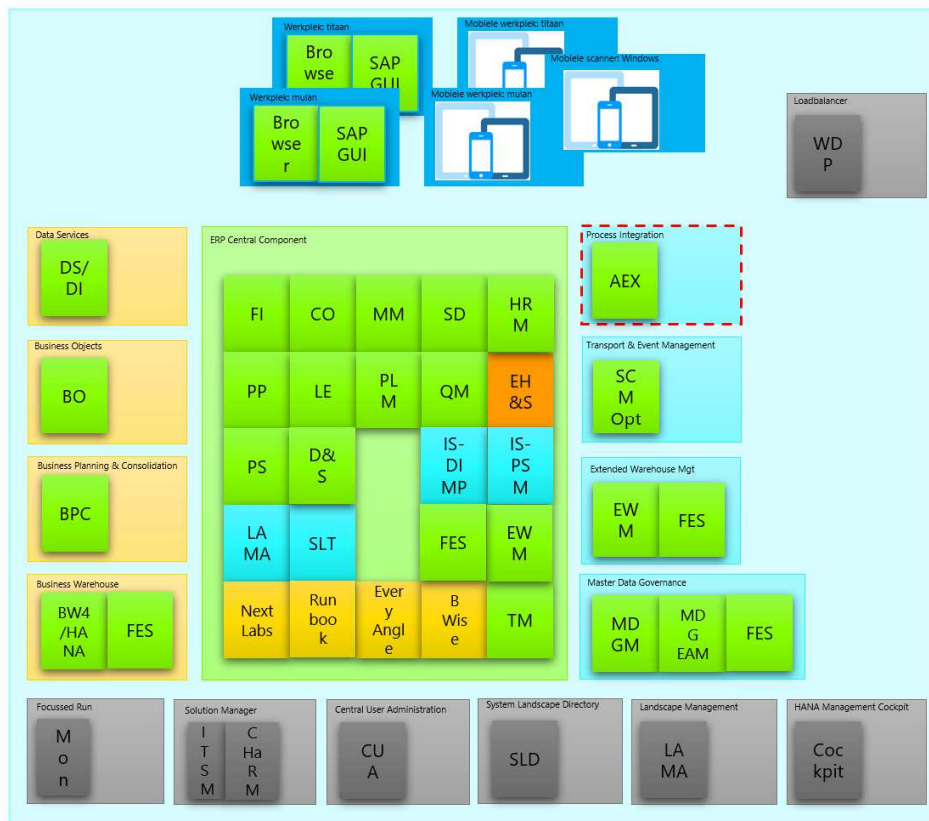
4.3 Applicatiefuncties (Logische applicatie)

Huidige ERP M&F SAP oplossing



Figuur 6: Huidige ERP M&F omgeving, alleen SAP componenten

Conform keuzes in dit document voorgestelde eindsituatie is hiermee bepaald. In de eindsituatie zitten timings afhankelijkheden naar de migratie planningen en scenario's. De eind situatie echter is in alle migratie scenario's gelijk (uitgangspunt).



Figuur 7: Eindarchitectuur

De motivatie om tot deze situatie te komen is gegeven in de individuele oplossing van knelpunten en de omzetting naar beslispunten in de bijlage van dit document.

5 Technische Architectuur

In dit hoofdstuk wordt de scope van het project aangegeven met betrekking tot de technische architectuur.

Deze technische architectuur valt uiteen in de delen:

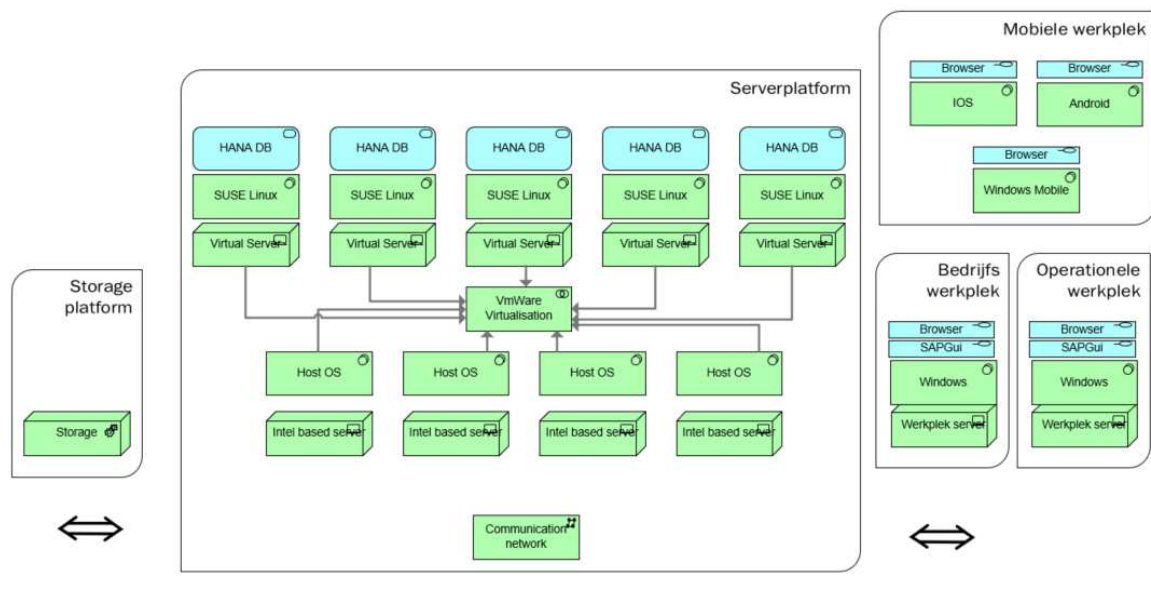
- Systeemcomponenten
- Systeemconfiguratie
- Ontwikkelarchitectuur
- Normen, standaarden en Principes
- Ontwerpbeslissingen Technische architectuur
- Architectuur Issues Technische architectuur

Gezien de sterke verwevenheid tussen deze drie delen, worden ze samen beschreven.

5.1 Systeemcomponenten

5.1.1 Huidige configuratie

Onderstaand diagram geeft de huidige configuratie uit de technische architectuur weer. Hierbij gelden de volgende keuzen, uitgangspunten en aandachtspunten.



6 Beveiliging

In dit hoofdstuk worden de eisen en wensen op het gebied van de beveiliging en de bestaande beveiligingsarchitectuur genoemd die gelden voor het project

6.1 Informatiebeveiliging

De Aanwijzing HDBV 017 Project en programmamanagement (paragraaf 2.6) stelt een aantal kaders met betrekking tot beveiligingseisen in projecten.

De eisen (beveiligingsnormen) met betrekking tot de informatiebeveiliging staan in de D-serie (D/101 t/m D/503) Informatiebeveiliging van het Defensie Beveiligingsbeleid (<http://publicatieportaal.mindef.nl/REG/Forms/BA.aspx>).

De eisen aan de uitvoering van het accreditatieproces zijn opgenomen in D/101 Accreditatie van informatiesystemen.

De eisen met betrekking tot het realiseren van certificering plichtige koppelingen zijn opgenomen in D/401 Koppeling met Defensienetwerken.

6.2 Beveiligingsbesturing

TBB-bepaling

Afhankelijk van het Te Beschermen Belang (TBB) van het informatiesysteem is te bepalen welke sub set aan beveiligingsnormen uit de D-serie van toepassing is op het informatiesysteem. Indien noodzakelijk, volgt later een VIR E&E-analyse, resulterend in een VIR E&E-rapport.

Op te leveren producten:

1. Quick scan TBB-bepaling.
2. Indien noodzakelijk: VIR E&E-analyse in een VIR E&E-rapport.

Accreditatieplicht

Het TBB niveau van het informatiesysteem bepaalt de accreditatieplicht van een informatiesysteem. De accreditatieplicht wordt vastgesteld door Team IBEV.

TBB-1 t/m TBB-3 informatiesystemen dienen geaccrediteerd te worden door de Beveiligingsautoriteit (BA) of door de Beveiliging coördinator (BC); TBB-4 informatiesystemen hebben geen accreditatieplicht, tenzij die door de CIO gekenmerkt zijn als een kritieke IT-systeem voor Defensie. Dit stelt de CIO jaarlijks vast.

Voor de niet-accreditatie plichtige TBB-4 informatiesystemen dienen wel beveiligingsmaatregelen getroffen te worden bij de normen van TBB niveau 4. In plaats van een accreditatie is eerste lijn toezicht conform HDBV Aanwijzing 005 Monitoring & Toezicht van toepassing op het implementeren van beveiligingsmaatregelen.

Verantwoording Beveiligingsnormen uit DBB.

Na de selectie van de van toepassing zijnde normen bij een TBB niveau, dient het project te starten met de verantwoording van de implementatie van deze normen door het nemen van beveiligingsmaatregelen volgens het '*comply or explain*'-principe. Dit betekent het volgende:

- Achter elke van toepassing zijnde norm dient een beveiligingsmaatregel geregistreerd worden in de Maatregelenlijst (opzet).
- De desbetreffende beveiligingsmaatregel dient geïmplementeerd te worden (bestaan en werking).

Hierbij geldt, indien een norm niet of maar deels (door een andere maatregel) afgedekt kan worden door een geïmplementeerde beveiligingsmaatregel dient het restrisico daarbij beargumenteerd te worden door het project. Een risicoanalyse methode, zoals het Risico Reductie Overzicht (RRO) of de Advanced Risk Tool (ART) zijn instrumenten om restrisico's te analyseren en te duiden. De eigenaar van het informatiesysteem dient de aangegeven restrisico's in het informatiesysteem, zoals aangedragen door het project aantoonbaar te accepteren.

In het Statement of Compliance (SoC) IT-dienstverlener dient het project aan de eigenaar en aan de accrediterende instantie per norm aan te geven welke normen wel en welke normen niet afgedekt zijn door middel van (alternatieve) beveiligingsmaatregelen. Idealiter dient de SoC IT-dienstverlener voorzien te zijn van de Bijlage Maatregelenlijst.

Op te leveren producten:

1. Maatregelenlijst.
2. RRO of ART.
3. SoC IT-dienstverlener.

Het project dient hiervoor een gecertificeerde informatiebeveiligingsadviseur in te schakelen.

Certificering plichtige koppelingen

Indien in het informatiesysteem gebruik wordt gemaakt van certificering plichtige koppelingen conform de criteria uit Beslisboom D/401 Koppeling met defensienetwerken, dan dient een Statement of Compliance Koppelingen (SoC-K) opgesteld te worden. Daarin dient per certificering plichtige koppeling verantwoording afgelegd te worden het afdekken van normen voor koppelingen door beveiligingsmaatregelen. Hierbij geldt het "*comply or explain*"-procedure en daarvoor kan een risicoanalyse methode, zoals het Risico Reductie Overzicht (RRO) of de Advanced Risk Tool (ART) gebruikt worden.

Op te leveren product: SoC-K per certificering plichtige koppeling.

Accreditatieverzoek

De eigenaar dient een accreditatieverzoek in voor zijn informatiesystemen van TBB niveau 1 t/m 3 en voor een Defensie kritiek TBB-4 informatiesysteem bij een accrediterende instantie. Hiervoor dient de Eigenaar het accreditatiedossier van het project te krijgen, bestaande uit:

1. Accreditatiedossier
 - 1.1 Quick scan TBB-bepaling en/ of VIRE&E-rapport;
 - 1.2 SoC, inclusief bijlage Maatregelenlijst;
 - 1.3 SoC-K voor certificering plichtige koppelingen.

Op te leveren product: Accreditatiedossier IT-dienst.

7 Informatie governance

Een informatieobject is een eenheid van informatie die relevant is vanuit een bedrijfsperspectief. Een informatieobject heeft betekenis voor de doelstelling en voor het functioneren van een organisatie. Een voorbeeld van een informatieobject is een operatieverslag. Informatieobjecten zijn onafhankelijk van fysieke inrichting of implementatie in een organisatie. Ze kunnen worden vertaald naar een fysiek model en naar fysieke verschijningsvormen van informatie (bijvoorbeeld tabellen in een database, informatie in een datawarehouse-omgeving, informatie in documenten). Dat betekent dat onderscheid moet worden gemaakt tussen de inhoud van een begrip (als concept, iets wat betekenis heeft in de werkelijkheid) en de manifestatie/vorm waarin het wordt opgeslagen of gepresenteerd (papier, digitaal, etiket, ponsplaatje). De manifestatie/vorm blijft buiten beschouwing wanneer gesproken wordt over informatieobjecten.

7.1 Informatie-eigenaarschap en -beheer

Het contentbeheer/gegevensbeheer ligt bij Defensie, namelijk bij de BV.

7.2 Mitigatie op de wettelijk kaders en eisen (compliance)

V.w.b. de (wettelijke) kaders, die van toepassing zijn op het informatiedomein waar de informatie-eigenaar verantwoordelijk voor is, de mitigerende maatregelen dient rekening gehouden te worden met de specifieke applicatie services welke voorzien moeten worden van dataopslag en back-up.

7.3 Privacy

Er dient (vanuit Defensie) in ieder geval voldaan te worden aan de eis, PIA toetsen uit te voeren per informatieobject (Privacy Impact Assessment). AVG is wetgeving en hier dient aan te worden voldaan. Op basis van de resultaten voortkomend uit deze PIA assesment dient te worden bepaald welke additionele maatregelen genomen dienen te worden.

7.4 Retentie en verwijdering

De Generieke Selectielijst Defensie (GSD)¹ waardeert informatieobjecten die ontvangen of opgemaakt zijn tijdens het bedrijfsproces, doormiddel van bewaartermijn. Het is een risicoanalyse instrument voor waarheidsbevinding en afleggen van verantwoording. Aan opgeslagen informatieobjecten worden het GSD proces en de bewaartermijn als metadata toegevoegd. Voor Delight moeten de betrokken processen gerelateerd worden aan de GSD processen. De bewaartermijn start na afdoening van het proces. Na afloop van de bewaartermijn wordt een informatieobject vernietigd en indien van toepassing overgedragen voor bewaring. De vernietiging, migratie of overdracht van informatieobjecten wordt geadministreerd zodat verantwoording mogelijk is. De vernietiging van specifieke categorieën informatieobjecten kan tijdelijk stop gezet worden wanneer de bedrijfsvoering dit vereist.

1
http://www.nationaalarchief.nl/sites/default/files/docs/selectielijsten/gsd_defensie_versie_vastgesteld_stcrt_2014_5937.pdf

Bij bewaartermijnen > 7 jaar wordt is het vereist informatieobjecten formeel te beheren. Hiervoor bestaan twee mogelijkheden:

1. Migratie naar een recordmanagement applicatie die voldoet aan de Moreq 2010 norm. Ondersteuning van de CMIS standaard is hierbij vereist
2. Recordmanagement functionaliteit binnen de applicatie te realiseren

7.5 Overige kaders

1. Informatieobjecten moeten gedurende de volledige bewaartermijn binnen redelijk termijn gevonden en geraadpleegd kunnen worden
2. Informatieobjecten worden beschermd tegen ongeautoriseerde wijziging. Bewerking van afgehandelde informatieobjecten of de daarbij horende meta data wordt vastgelegd
3. Het vastleggen van meta data over informatieobjecten conform een vastgesteld schema (toepassingsprofiel meta data rijksoverheid) moet ondersteund worden. Meta data wordt indien mogelijk automatisch vastgelegd. Meta datavelden zijn voorzien van een beschrijving en worden eenduidig gebruikt. Het gebruik van een gecontroleerd vocabulaire wordt ondersteund. Het is mogelijk versiebeheer op de toe te passen op de gebruikte meta dataschema's. De koppeling tussen de meta data en het informatieobject is onverbrekelijk tot het moment van verwijdering. Door deze maatregelen wordt het beheer en de vindbaarheid van informatie ondersteund
4. Het moet mogelijk zijn informatieobjecten inclusief metadata te migreren in een open formaat. Hierbij vormen de richtlijnen van forum standaardisatie het uitgangspunt
5. Er kan op basis van de toegevoegd meta data een selectie van de beheerde informatie gemaakt worden: vereist voor hotspots, hold verzoeken en partiële export
6. Indien gebruik wordt gemaakt van een digitale ondertekening, dan is deze duurzaam vastgelegd
7. Voor de beheerde informatie moet een "ordeningsplan" opgesteld worden, dit vormt de basis voor de definitieve analyse m.b.t het beheer van de informatie

8 Beheerketen

In dit hoofdstuk worden de kwalitatieve en de kwantitatieve effecten van de implementatie van S/4HANA op de beheerorganisatie en –processen in de End State beschreven. In de bijlage is per migratiescenario het beheer in de tussentijdse periode vergeleken.

De analyse is gebaseerd op de projectproducten [2.1] Project Start Architectuur, [2.6] Migratieaanpak/-planning en [2.12] Toekomstige exploitatiekosten.

De implementatie van S/4HANA wordt benut om de architectuur van de M&F-oplossing zo veel mogelijk te vereenvoudigen. De End State heeft de volgende kenmerken:

- Standaardisatie van de IT-oplossing (en de te ondersteunen bedrijfsprocessen). Bij uitzondering blijft maatwerk gehandhaafd.
- Embedded oplossing voor EWM en TM; MDG-M blijft vooralsnog een hub-oplossing
- ECC on-premise
- Rationalisatie van het aantal omgevingen.

8.1 Kwalitatieve analyse beheerinspanning in de End State (M&F + GII)

Meerwerk

- Business consultancy verhoging binnen de Sectie Plan [overbruggen functionele oplossing met standaard-SAP (beheerproces 'Specification management'); procesbegeleiding op basis van Agile, DevOps en Design Thinking]
- Ontwerpregie: bewaken standaardisatie nieuwe functionele ontwikkelingen (beperken maatwerk)
- UX-architecten/-ontwikkelaars, een nieuwe rol: bewaken van de UX-architectuur en, samen met de gebruikers, de userinterface ontwerpen (voorafgaand aan de technische realisatie van de gebruikersinterface)
- Autorisatiebeheer en Security: complexer en verhoogd risico door toevoeging van FIORI, Best-of-Breed-oplossingen en mobiele randapparatuur.
- Mogelijk verhoogde complexiteit oplossing (combinatie On-premise-SCP-Cloud; meer SAP-componenten - zoals Fiori en de webbrowser - en Best-of-Breed-oplossingen buiten SAP)

Minderwerk

- Verlaagde complexiteit (gereduceerd maatwerk, standaard-oplossing Core/werkplek/user interface, vereenvoudigde architectuur en landschap) leidt tot lagere beheer- en voortbrengingsinspanning (minder incidenten, vereenvoudigde voortbrenging nieuwe functionaliteit en technische release) en een lagere Total Cost of Ownership.
- Het aantal en de complexiteit van de interfaces neemt door de toepassing van de embedded-versie van EWM en TM af.
- Ontwikkeling en beheer van het Fiori-front-end met Javascript is een nieuwe skill voor CrossFunctional; de skill voor het beheer van de back-end met CDS en ABAP blijft ongewijzigd. Na een aanvankelijk investering tijdens de implementatie van S4HANA neemt de beheerlast van het maatwerk af door reductie van het aantal omgevingen (Portal en PI vervallen) en door beschikbaar komen van gebruikersvriendelijkere beheertools (die zelfs de key user in staat stellen een deel van het beheer uit te voeren).
- Het beveiligingsrisico neemt af door de toepassing van de embedded-optie binnen SAP en het Datacenter.
- Verhoogde flexibiliteit M&F-oplossing zonder extra inspanning; de standaard SAP-oplossing verhoogt de toepasbaarheid/aansluitbaarheid Best-of-Breed-oplossingen buiten SAP waardoor snel en goed flexibeliteit aangeboden kan worden.
- De standaardisatie van de IT-oplossing vereenvoudigt het gebruik (en de gebruikerstraining), waardoor de zelfredzaamheid van de eindgebruikers zich zal verhogen en de (beheertaak) gebruikersondersteuning minder wordt.
- De consolidatie van de SAP-oplossingen resulteert in een verlaging van het aantal omgevingen en het beheer daarvan.

Stabiel

- De beheerprocessen blijven ongewijzigd.
 - Het volume werk zal enerzijds toenemen (user-interface, interfacing met Best-of-Breed-oplossingen) en afnemen (keuze embedded staat voor volledige integratie).
 - Technisch beheer: vergelijkbare complexiteit infrastructuur en architectuur.
 - Configuratiemanagement: vereenvoudigde SAP-oplossing (minderwerk) en verhoogde inzet van Best-of-Breed (NON SAP-) oplossingen
- Technisch Beheer verwacht dat de huidige bezetting ook na de migratie volstaat.

8.2 Kwantitatieve analyse beheerinspanning End State (M&F + GII)

Het netto effect van de implementatie van S/4HANA is een verlaging van de Total Cost of Ownership:

- Als gevolg van de standaardisatie van de oplossing kan de inzet van Functioneel/Applicatie-beheer binnen een range van 0% tot 15% afnemen. Voor deze reductie is instemming van de bedrijfsvoering randvoorwaardelijk.
- Business consultants/informatiemanagement binnen de afdeling MLOG&F IT overbruggen dat de diversiteit van de klantwensen worden vertaald naar standaard-SAP; zij bewaken de aanmaak van aanvullend maatwerk. Geschat wordt dat dit team in omvang zal verdubbelen (+ 14 man).
- Verwacht wordt dat het meer- (Fiori) en minderwerk (minder interfaces) per saldo door het huidige CF-team kan worden uitgevoerd.
- Het aantal UX-architecten/-adviseurs is afhankelijk van de ruimte die wordt gegeven aan de customizing van de userinterface.

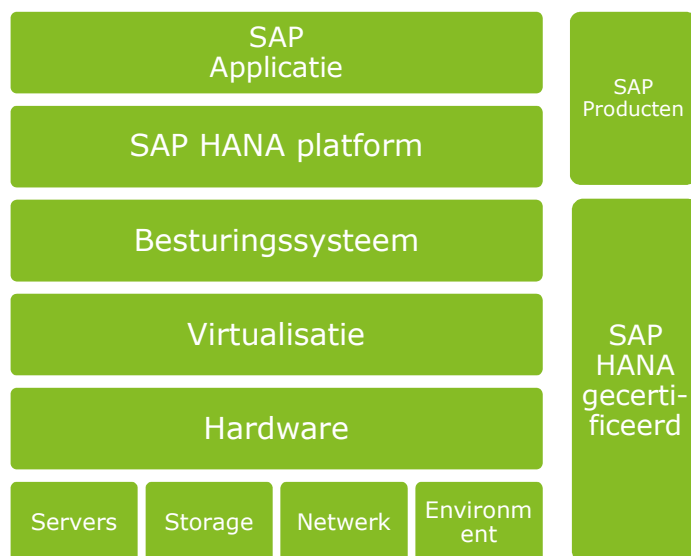
BIJLAGE: KWANTITATIEVE VERGELIJKING MIGRATIESCENARIO'S BEHEERINSPANNING TIJDENS MIGRATIE (M&F + GI&I)

Scenario	Beheerinspanning
Systeemconversie	• Eenduidig landschap wat betreft interfaces en analytics met voordelen voor beheer/technische release en voortbrenging (reguliere CHARM-proces) • Kennis & kunde beheer big bang opbouwen • Kennis & kunde bedrijfsvoering geleidelijk opbouwen
Nieuwe implementatie/Big Bang	• Eenduidig landschap wat betreft interfaces en analytics met voordelen voor beheer/technische release en voortbrenging (reguliere CHARM-proces) • Kennis & kunde beheer en bedrijfsvoering big bang opbouwen • Extra complexiteit als gevolg van onvolwassenheid modules en gebruikerspopulatie
Nieuwe implementatie/Gefaseerd	• Complex tijdelijk landschap (parallel oude en nieuwe oplossing met tijdelijke extra interfaces en analytics o.b.v. diverse bronnen) met gevolgen voor beheer/technische release en voortbrenging (complexe variant van het CHARM-proces over twee ontwikkelstraten heen) • Kennis & kunde beheer big bang opbouwen • Kennis & kunde bedrijfsvoering geleidelijk opbouwen
Hybride/Big Bang	• Eenduidig landschap wat betreft interfaces en analytics met voordelen voor beheer/technische release en voortbrenging (reguliere CHARM-proces) • Kennis & kunde beheer en bedrijfsvoering big bang opbouwen • Extra complexiteit als gevolg van onvolwassenheid modules en gebruikerspopulatie •
Hybride/Gefaseerd	• Complex tijdelijk landschap (parallel oude en nieuwe oplossing met tijdelijke extra interfaces en analytics o.b.v. diverse bronnen) met gevolgen voor beheer/technische release en voortbrenging (complexe variant van het CHARM-proces over twee ontwikkelstraten heen) • Kennis & kunde beheer big bang opbouwen • Kennis & kunde bedrijfsvoering geleidelijk opbouwen

9 Eisen SAP infrastructuurlandschap S/4HANA

Voor de borging van ondersteuning van SAP HANA door de leverancier SAP, dient de hardware, software en personeel gecertificeerd te zijn. Dit geldt zowel voor het bestaande SAP ERP als voor het nieuwe S/4HANA systeem die beide draaien op het SAP HANA platform.

Voor de hardware geldt dat de combinatie van storage, netwerk en server gecertificeerd dient te zijn. Diverse grote leveranciers hebben hun producten door SAP laten certificeren voor SAP HANA. Ook de onderliggende software componenten zoals besturingssystemen en virtualisatie producten dienen gecertificeerd te zijn.



Voor het inrichten van de gecertificeerde SAP HANA ICT infrastructuur in de Defensie datacenters bestaan een aantal SAP HANA gecertificeerde opties:

- Gecertificeerde Appliances
- Tailored Datacenter Integration (TDI)
- IAAS platformen
- Hyper-Converged Infrastructure Solutions (HCI)

Bij de inrichting van de huidige SAP infrastructuur in 2016 waren alleen gecertificeerde appliances en TDI beschikbaar. Aangezien met TDI nagenoeg de bestaande Defensie datacenter architectuur gevolgd kon worden en het beste aansloot op de staande beveiliging en beheer inrichting is toen gekozen voor de inrichting van de SAP HANA infrastructuur op basis van TDI. Voor meer informatie zie Project Start Architectuur (PSA) SAP HANA definitief 1.0 d.d. 10 augustus 2016. Onderstaande tabel geeft de uiteindelijke inrichting aan en of daarmee gebruik werd gemaakt van bestaande in beheer zijnde componenten (Generiek):

ICT laag	ICT component	Generiek
Environment	Datacenter (DC) Maasland & Woensdrecht	Ja

Netwerk	10 Gb Cisco switches (inmiddels met 40Gb ontsloten in DC)	Ja
Storage	NetApp FAS8080	Ja, echter Hosting SAP maakt daarbovenop wel gebruik van specifieke storage functies voor back-up en uitwijk
Servers	HP DL380 Gen9	Ja, voor SAP HANA bij inrichting wel een snellere CPU (snelheid per core) en meer memory (1 TB). Inmiddels is het laatste de nieuwe standaard in het DC
Virtualisatie	VMware	Ja
Besturingssysteem	SuSE Linux	Ja

In dit S/4HANA onderzoek is a.d.h.v. een SAP Technical Architecture and Infrastructure (TAI) Workshop onder leiding van SAP onderzocht of de bestaande SAP HANA ICT inrichting voldoet voor de migratie naar S/4 HANA en voorziet in voldoende capaciteit met een verwachte groei van 10% per jaar, tot de vervanging van de ICT infrastructuur in 2021.

De conclusie is dat de S/4HANA migratie kan worden uitgevoerd en de SAP omgeving tot 2021 kunnen groeien (10% p/j) op de bestaande ICT infrastructuur.

Technical Architecture and Infrastructure @ Ministry of Defense (MoD)

Executive Summary

- We assessed MoD boundary conditions and the technical architecture.
 - Architecture concepts can remain the same for SAP S/4HANA considering current boundary conditions.
 - However if boundary condition change in future an architecture re-design is required.
- Evaluation of existing hardware DL 380 Gen9 for SAP S/4HANA
 - Support is currently validated by HPE hardware partner. SAP information shows certification for SAP S/4HANA.
- Further surrounding SAP systems like TM & EM, BW (operational reporting) will potentially consolidated to SAP S/4HANA, other systems like MDG, Portals, PI have an impact to the future solution (application) landscape and need to be assessed in planning phase.
 - SAP Innovation Strategy Roadmap (ISR) service is recommended.
- A three year sizing projection considering growth rate of 10% for the productive systems has been made.
 - SAP BW on HANA systems shows critical HANA resource consumption, MoD team is following up.
 - The consolidation of SAP TM&EM to SAP S/4HANA ERP seems to be feasible from data volume perspective. SAP HANA servers have maximum of 1TB RAM available. Storage space for S/4HANA conversion is sufficiently available 100TB per Rack.
 - Workload analysis is recommended to validate future workload requirements. Advanced Sizing service recommended.
 - The consolidation of applications needs to be evaluated within an ISR in planning phase.
- Question if SAP HANA 3.0 has impact on hardware requirements, was raised in wrap up, follow up needed.
- A high level architecture template design for SAP S/4HANA systems, based on the current boundary conditions.

© SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL

6

Figuur 8: Executive Summary Slide uit Report-Out SAP TAI Workshop

Vanuit Lifecycle management is 2021 het natuurlijk moment om de ICT infrastructuur voor de SAP systemen te vervangen.

Andere ontwikkelingen bij Defensie hebben direct invloed op de toekomstige keuze van de ICT infrastructuur voor SAP systemen. In juli 2019 is voor de SAP M&F systemen een nieuwe Voorschrift Informatiebeveiliging Rijksdienst Efficiënt & Effectief (VIR E&E) uitgebracht. De nieuwe VIR E&E geeft een hoger betrouwbaarheidsniveau en een hoger te beschermen belangen aan. Een Impact Analyse/Vooronderzoek moet voor JIVC duidelijk gaan maken welke nieuwe eisen de VIR E&E gaat geven, hoe deze ingevuld kunnen worden en wat daarvan de (extra) kosten zijn. Ook het technisch ontwerp van GrIT en de inrichting van datacenters met bijbehorende ICT infrastructuur kunnen gevolgen hebben voor ICT infrastructuur van de SAP systemen.

In 2020 dienen de gevolgen van de VIR E&E en GrIT duidelijk te zijn om een nieuw ontwerp te maken voor de SAP infrastructuur die voldoet aan de SAP HANA certificering en zoveel mogelijk de standaarden van Defensie volgt.

10 Architectuur beschouwingen

10.1.1 Cloud & Hosting

Cloud varianten zijn er in vele smaken momenteel. De meest belangrijke zijn IaaS oplossingen in een Public Cloud, Managed oplossingen tbv SaaS of PaaS of hybride oplossingen waarbij er één van bovenstaande oplossingen wordt toegepast in combinatie met een On-Premise omgeving. Meer en meer beweegt de markt zich naar deze Cloudoplossingen. Deze oplossing hebben bestaansrecht om meerdere redenen:

- Een ander kostenmodel (1), Opex versus Capex, in tegenstelling tot het bezit van hard- en software met een initiële hoge investering, het huren ervan tegen een bepaald termijn bedrag en vooraf bepaalde condities, door de vaak lagere kosten en de grote schaal zijn Cloudleveranciers in staat hogere service niveau's te leveren;
- Een cloudoplossing heeft een ander inzetbaarheidsmodel, waarbij afroep van nieuwe omgevingen of aanpassing op bestaande omgevingen zeer flexibel en vaak direct kunnen worden doorgevoerd, met hogere inzetnelheid (2) en hogere flexibiliteit (3) tot gevolg;
- Universele oplossingen bieden betere koppel mogelijkheden, hierdoor een betere connectiviteit met eco-systemen van de organisatie mogelijk;
- Een laatste voordeel is het kunnen vertrouwen op de kennis in de Cloud, bepaalde eigen kennis of kennisopbouw voor nieuwe technologie, is hierdoor niet specifiek noodzakelijk. Deze specifieke kennis kan in het eigen bedrijf worden geminimaliseerd tot het niveau waarop nog wel kan worden beoordeeld of de Cloud leverancier de gewenste functionaliteit kan leveren (a), d.m.v. van vaststelling van een Cloud SLA en dit in latere instantie ook inhoudelijk kan worden getoetst (b). Universele oplossingen bieden tevens

In bepaalde omstandigheden kan een Cloudoplossing dus een behoorlijke versnelling geven voor nieuwe ontwikkelingen.

Cloudoplossingen maken gebruik van uniforme gebruikersinterfaces door inzet van een generieke internet browser. Door gebruikmaking van gestandaardiseerde internet protocollen wordt de inzet van Cloud tevens voor grote groepen gebruikers bereikbaar (laagdrempelige en toegankelijke interface).

Door gebruikmaking van internationale beveiligingsstandaarden en reguliere toetsing ervan door derden is een cloudoplossing tevens een relatief veilige omgeving. Zolang iedereen de standaarden maar consequent blijft doorvoeren kan dit voor bedrijven zelfs een driver zijn om een Clouddienst af te nemen. Vaak zijn interne bedrijfsprocedures lastig te toetsen en kan men hier voor een bepaald deel van de beveiliging vertrouwen op de leverancier. Dit is wel heel specifiek vastgelegd in de SLA, immers koppelen met de Cloud geeft wederzijdse verplichtingen voor de veiligheid ervan. Zo kunnen bedrijven vaak kiezen voor bepaalde standaarden voor netwerkbeveiliging, data encryptie (in rust en in transport) en zijn er allerlei mogelijkheden voor het implementeren van koppelingen aan de eigen, centrale gebruikersdatabase door inzet van eveneens gestandaardiseerde protocollen. Door gebruikmaking van centrale omgevingen voor de authenticatie wordt voorkomen dat men meerdere keren moet inloggen en wordt het combineren van meerdere gebruikersentiteiten voorkomen. De veiligheid van de integrale omgeving blijft ten allen tijde die van de afnemer, de Defensie organisatie, validatie van security controls bijvoorbeeld.

Met de komst van Cloudoplossingen wijzigen tevens een aantal grote ERP marktspelers hun strategie voor het leveren van diensten. Diensten welke voorheen als on-premise product werden geleverd, worden nu langzaam verplaatst naar Cloud varianten en daarmee wordt tevens het beheermodel aangepast. Daar waar voorheen de leverancier op locatie diende te zijn en het heel duidelijk was wanneer iemand onderhoud deed of ontwikkelde voor een bepaald product, wordt dat nu tevens

vanuit Clouddiensten ingevuld. Zelfs oplossingen welke voorheen werden meegeleverd met de on-premise omgevingen, worden nu al vaak alleen vanuit de Cloud geleverd. In zekere zin wordt de markt voor hard en software oplossingen in de Cloud en het succes ervan gedreven in een richting waarbij on-premise oplossingen achterstand oplopen of zelfs worden uit gefaseerd.

10.1.1.1 Cloudivisie van het ministerie van Defensie

Alle rijksoverheden classificeren de in automatiseringssystemen te verwerken of opgeslagen informatie. Deze classificatie is vastgelegd in de BIO2019 en nader uitgewerkt in overige wet en regelgeving. Voor Defensie specifiek een verbijzondering in de VIR E&E tbv de risico analyse en de D/300. Momenteel bezit de ERP M&F omgeving de rubricering TBB-4 (Te Beschermen Belangen categorie 4) en Departementaal Vertrouwelijk (DEP-V). Er wordt zelfs gewerkt aan een hoger rubriceringsniveau TBB-2: Staatsgeheim Confidentieel (STG-C). Voor dit onderzoek was DEP-V het startpunt dus daar concentreert het onderzoek zich tevens op. Zodra de opdracht wordt verstrekt om de impact nogmaals te toetsen op het niveau STG-C kan deze paragraaf worden herzien.

Het toevoegen van Clouddiensten aan het applicatieve landschap van ERP M&F kan voordelen geven, voor delen die niet gemakkelijk oplosbaar zijn met bestaande on-premise delen. Om dit te kunnen doen zal er een afleiding vanuit wet en regelgeving dienen te worden gemaakt voor Cloud gebruik door het ministerie van Defensie. Het behoeft geen nadere uitleg dat sommige data van Defensie vertrouwelijkheid geniet, maar ook deze delen zijn afhankelijk van de rubricering van de systemen waarin deze data wordt verwerkt of opgeslagen.

Vanwege het feit dat het huidige rubriceringsniveau DEP-V betreft, ligt de focus voor het huidige vooronderzoek op deze classificatie.

Er loopt momenteel een visie onderzoek Cloud vanuit Defensie en op hoofdlijnen zijn dit de eerste richtingen:

Voor DEP-V, Ongerubriceerd en Gemerkte informatie, is het huidige beleid dan wel de bestaande praktijk als volgt:*

- *Ongerubriceerde en Ongemerkte gegevens mogen in een Public Cloud geplaatst worden; dit mag onder huidig beleid.*
- *Ongerubriceerde, Gemerkte gegevens exclusief Personeelsvertrouwelijk** mogen in een Public Cloud geplaatst worden; dit mag onder de huidige praktijk hoewel dat nog niet formeel in beleid is vastgelegd.*
- *Ongerubriceerde, Personeelsvertrouwelijke gegevens kunnen na anonimiseren in een Public Cloud geplaatst worden; dit mag onder de huidige praktijk hoewel dat nog niet formeel in beleid is vastgelegd.*
- *DEP-V gegevens die door 'filtering' (subset van gegevens) of bewerking tot ongerubriceerd worden terug geschaald mogen in een Public Cloud worden geplaatst; dit mag onder de huidige praktijk hoewel dat nog niet formeel in beleid is vastgelegd. Dit kan een optie zijn wanneer een subset van DEP-V gegevens bewerkt worden op een Public Cloud platform terwijl de volledige set van gegevens (DEP-V) in de on-premise Private Cloud blijft. Het komt erop neer dat in de Public Cloud dan alleen nog ongerubriceerde gegevens worden verwerkt.*
- *DEP-V gegevens mogen in een on-premise Private Cloud geplaatst worden. Merk op dat de on-premise Private Cloud geleverd en beheerd mag worden door een externe leverancier wanneer die voldoet aan de ABDO voorwaarden. Dit mag onder huidig beleid.*

**: Merking van gegevens is onafhankelijk van rubricering van gegevens maar voor de besluitvorming wordt merking pas bepalend bij ongerubriceerde gegevens.*

*** : Personeelsvertrouwelijk is de enige merking waaraan op dit moment de extra eis van anonimisering wordt gesteld.*

De ambitie is dat DEP-V gegevens in een Public Cloud geplaatst mogen worden wanneer er voldoende goede maatregelen genomen kunnen worden om de gegevens te beschermen. Op dit moment is er nog geen bekende set van maatregelen die een klein genoeg restrisico opleveren om ze als voldoende goed te beschouwen. Hoewel versleuteling een goede maatregel is voor data in rust en data in transport is versleuteling van data in processing

praktisch nog niet haalbaar. De ontwikkeling in de komende jaren moet uitwijzen welke set van maatregelen als voldoende goed worden beschouwd.

De voorlopige Routekaart Cloud mag met toestemming worden geplaatst in dit document, de oplevering van de Routekaart Cloud is tevens gepland voor november 2019.

Kijkend naar bovenstaande zijn er mogelijkheden om cloudoplossingen toe te staan binnen Defensie en wel op de volgende wijze:

1. Door maskering van DEP-V data op een publieke omgeving waardoor het ongeclassificeerde data betreft of er geen DEP-V data in de uitwisseling met het publieke deel van de oplossing wordt gebruikt;
2. Door ervoor te zorgen dat de oplossing niet publiek kan worden gebruikt maar de oplossing bijvoorbeeld geheel in een private omgeving wordt ingezet;

Van dit eerste deel zijn al voorbeelden in gebruik bij de Rijksoverheid, ook voor SAP delen. Voor de tweede oplossing ligt het iets meer genuanceerd. De oplossing kan dan volledig in eigen datacenters staan, maar ook in specifiek voor dit doel gecertificeerde datacenteroplossingen extern, waarbij er zelfs de mogelijkheid bestaat dat dit externe datacenter, naast private oplossingen tevens publieke oplossingen aanbiedt. Het is in beide gevallen de vraag in hoeverre data voldoende is beveiligd, afhankelijk van het geplaatste rubriceringsniveau van de data.

De data beveiliging wordt hiervoor in drie toestanden beoordeeld: in ruste (opgeslagen op disksystemen), in transport (d.m.v. netwerken door de lucht of door fysieke bekabeling) en in bewerking (door elektrische rekeneenheden (CPU's) bewerkt). Deze laatste categorie is momenteel het meest complex. De rekeneenheden zitten namelijk overal in de keten en kunnen ook overal worden gedeeld met derden. De controle op het beveiligingsniveau van deze laatste categorie faalt momenteel nog, de eerste twee kunnen worden opgelost met behulp van moderne encryptie technologieën. Om bovenstaande redenen wordt het rubriceringsniveau DEP-V momenteel nog niet toegestaan in publiek gedeelde omgevingen.

10.1.2 Gebruikersinterface

Gebruikers interfaces worden intuïtiever, onderzoek naar hoe mensen prettiger werken, productiever zijn en effectiever over informatie beschikken beheersen de applicatiemarkt.

In het verleden probeerden leveranciers elkaar de loef af te steken door inventieve eigen producten als gebruikersinterface in te zetten, momenteel doet men dit nog steeds maar dan binnen een zoveel mogelijk gestandaardiseerd platform. Dit laatste wordt gedreven door onderhoudskundige aspecten in de diversiteit aan gebruikers werkplekoplossingen waar deze interfaces worden ingezet.

Waar Microsoft Windows werkplekken prominent aanwezig waren, komen nu tevens de LINUX varianten op door de leveranciersafhankelijkheid, beveiligingsaspecten en mede gedreven door TCO. Ook mobiele oplossingen hebben een deel van de werkplek markt in handen of zijn er aan toegevoegd. Deze geven niet alleen andere beeldscherm dimensies maar voegen tevens additionele mogelijkheden toe aan de gebruikersinterface. Voorbeelden hiervan zijn Touch, bewegingen met het hoofd of hand, spraak, camera e.d. Dit geeft meer mogelijkheden in de interactie met eindgebruikers.

Door de marktbeveiling naar Cloudproducten worden steeds vaker internetbrowsers ingezet als gebruikersinterface. Waar voorheen deze internetbrowser behoorlijk grafische beperkingen kende is dit met nieuwe internetbrowser technologie (HTML5 & Javascript) verleden tijd. De beweging om daarmee van de "large footprint" en vaak proprietary werkplekapplicatie als front-end af te komen wordt hierdoor versterkt richting de standaard internet browser meegeleverd met het werkplekbesturingssysteem.

In hoeverre is deze internetbrowser nu standaard? Iedere browser heeft weer een eigen specialiteit en dat maakt deze uniek voor een bepaalde leverancier. In een wereld van open standaarden staat dit wel weer haaks op de mogelijke inzet op werkplekken waar veel meer verschillende applicaties ondersteund dienen te worden.

Daarnaast volgen de open standaarden zich in snel tempo op worden en door het zeer hoge gebruik van deze producten regelmatig beveiligingslekken aangetoond welke in patches of nieuwe versies, in een evenzo hoog tempo weer worden gerepareerd. Dit maakt het complex om een standaardiseerde bedrijfswerkplek wel kunnen bijhouden. Ook de applicatie moet dit kunnen volgen, met een gemiddelde lifecycle van bedrijfsapplicaties van 1 jaar op een bepaald patchniveau is dit een uitdaging. De meeste leveranciers geven dan ook "de laatste versie" mee voor de ondersteuning op browser producten.

10.1.2.1 De SAP gebruikersinterface en de werkplek van het Ministerie van Defensie

Er zijn momenteel twee werkplekken in gebruik, de standaard bedrijfswerkplek (MULAN) en de operationele werkplek (TITAAN). Beiden voorzien van een Microsoft Windows oplossing en een Internet Explorer webbrowser. De huidige bedrijfswerkplek heeft daarnaast een Microsoft Edge webbrowser, in het Portfolio Lifecycle Plan (PLP) wordt echter alleen de Microsoft Internet Explorer en Firefox genoemd als officiële applicaties. De versies van webbrowsers op beide werkplekken lopen behoorlijk achter bij de laatst beschikbare versies van de leverancier, waarbij hier niet kan worden gesproken van $n-1^2$ in het versiebeheer, zeker niet voor de operationele werkplek welke momenteel eens per jaar wordt bijgewerkt.

De gebruikers interfaces in gebruik bij ERP M&F zijn de SAP GUI, de web variant van de NWBC, en de Mobile ITS tbv de handscanners. De SAP GUI is een grote, lokaal geïnstalleerde front-end applicatie op de werkplek verantwoordelijk voor snelle grafische informatie en tekstverwerking, waarbij een zeer lage bandbreedte is vereist voor de koppeling met centraal, over LAN en WAN infrastructuur, bereikte servers.

Daarnaast voor specifieke analytische toepassingen wordt er momenteel gebruik gemaakt van een door de internetbrowser ondersteunde portaal functie en separate Business Objects rapportage interfaces.

Al deze gebruikersinterfaces vervangen door één generieke front-end zou de ultieme eindgebruikers en beheer-oplossing geven, waarbij dan tevens de bandbreedte laag kan blijven. Het onderhoud van de werkplek zou zich hiermee beperken tot één standaard applicatie, de internet browser, wat een versimpeling van applicatie beheer voor de werkplek betekent. In de vertaalslag naar FIORI echter is dit nog wel de vraag. Additionele testen moeten uitwijzen of de bandbreedte inderdaad vergelijkbaar is met het huidige SAP GUI gebruik.

Uiteraard biedt de Fiori laag in de applicatie de ontsluiting van verschillende nieuwe functionaliteiten voor SAP. Fiori is ook het middel om innovaties uit te leveren. Het is niet mogelijk volledig de waarde uit S/4HANA te halen zonder inzet van Fiori. Dit is omdat alle innovaties (simulaties, predicties, aanbevelingen) en alle operationele analyses (management by exception) worden uitgeleverd via de Fiori apps.

Beheerders werkplekken

² $N-1$ = De laatste productversie minus 1

De beheeroplossingen zijn tevens nu deels in separate applicaties ondervangen. Het aanpassen van de SAP oplossingen in de code wordt door eclips hulpmiddelen i.c.m. de SAP GUI en de huidige Internet Explorer uitgevoerd. Het vervangen van deze oplossingen door nieuwe on-premise oplossingen is mogelijk, maar geeft in nabije toekomst mogelijk Cloud uitdagingen. De ontwikkelhulpmiddelen worden meer en meer in de Cloud aangeboden en de ontwikkelrichting van de leverancier is tevens toegespitst op die van de Cloud. Hierdoor kunnen on-premise ontwikkelhulpmiddelen achterlopen of zouden deze in de toekomst wellicht verlaten kunnen worden door leveranciers. Buiten de Cloud discussie is er voor de gebruikersinterface inrichting een zeker spanningsveld voor het Ministerie van Defensie bij de ontwikkeling van Fiori applicaties.

Indien we spreken over een gebruikersinterface geheel afgenomen vanuit een Cloud, wat tevens een ontwikkelrichting is van de grote applicatie leveranciers, geeft dit de eerdere standpunten van Cloud toepasbaarheid met de Defensie Cloudvisie als uitgangspunt.

Essentieel is de werkplek, doordat het gebruik van de applicatie verschuift van een dedicated front-end van de applicatie op de werkplek naar een standaard applicatie van de werkplek, de webbrowser, is het van essentieel belang dat die webbrowser in de pas blijft lopen bij de ondersteuning van het applicatieve product. Nieuwe versies, vervanging door alternatieve browserproducten of het achterblijven in opvolging van nieuwere productversies hebben directe implicaties voor de ondersteuning, stabiliteit of zelfs werking van deze applicatie.

Zie tevens de knelpunten 4 & 5.

10.1.3 *Infrastructuur*

In de onderliggende laag van de applicatie bevindt zich in de infrastructuur, deze is opgebouwd uit drie componenten:

1. Een of meerdere netwerken;
2. Een of meerdere opslagsystemen;
3. Een of meerdere rekeneenheden.

Deze componenten zijn allemaal sterk in ontwikkeling en de verwachting is dat deze zich alleen maar sneller zal voortzetten.

De genoemde componenten zijn vrijwel allen goed verkrijgbaar van verschillende leveranciers, uitwisselbaar voor een groot deel en 'commodity' te noemen.

De laatste jaren komen, door de massaproductie van deze componenten en het veelvuldig gebruik ervan, tevens beveiliging aspecten naar boven (Intel's Spectre en Meltdown bijvoorbeeld bij de rekeneenheden). De rekeneenheid zelf bijvoorbeeld heeft vaak al eigen netwerken en opslagsystemen aan boord om opdrachten te versnellen. In opslagsystemen zitten weer rekeneenheden en netwerken om deze systemen te versnellen. Ook netwerkcomponenten bestaan in deze tijd niet meer alleen uit fysieke bekabeling. Er zitten allerlei rekeneenheden en opslagsystemen ingebouwd in netwerkcomponenten t.b.v. besturing, beveiliging en versnelling. Al deze componenten tezamen vormen de infrastructuurlaag van de applicatie.

Door deze complexiteit van de infrastructuur, welke zeker zijn vruchten heeft afgeworpen als we kijken naar de versnelling van verwerking, zit tevens een toegenomen beveiligingsrisico.

Doordat er data wordt verwerkt door deze systemen is het helaas ook mogelijk deze data, ongeautoriseerd te bekijken of zelfs te manipuleren. Het lekken of manipuleren van data kan voor elk bedrijf desastreuze gevolgen hebben en daarom moeten datacenters en leveranciers aantoonbaar

voldoen aan industrie veiligheidsstandaarden en wordt er voortdurend getoetst of gebruikte componenten voldoende veilig zijn.

Daarnaast worden door de leveranciers aanpassingen gedaan in de besturingssoftware van deze componenten om de stabiliteit, de veiligheid en de snelheid te kunnen blijven garanderen. Dit wordt vaak omgezet in patchbeleid door het bedrijf waar de componenten zijn ingezet en conform SLA weer uitgedrukt in een beveiligingsgraad en beschikbaarheid. Ook Cloudleveranciers drukken dit op deze wijze uit, vaak refererend aan industrienormen en wereldwijd erkende certificeringen.

T.b.v. grote applicatieve toepassingen is het gebruikelijk dat er tevens specifieke infrastructurele eisen worden gesteld aan de gebruikte componenten, vaak niet beperkt tot de hoeveelheid van de drie hoofdcomponenten maar tevens de smaak (leverancier), technische architectuur of specifieke versie van de componenten. Dit maakt het complex om een infrastructuur platform aan de ene zijde als veilige publieke omgeving in te zetten en anderzijds alle applicatieve oplossingen te kunnen ondersteunen.

SAP is hier een goed voorbeeld van, SAP ondersteunt alleen gecertificeerde componenten in de gehele infrastructuur. Opslagssystemen (Storage), rekeneenheden (Compute), virtualisatie, operating systeem en netwerk zijn allemaal onderdeel van een certificering. Met name de combinatie van componenten geeft hierin de complexiteit. SAP geeft hier strikte richtlijnen voor af. In het geval van HANA is er een variant welke vrijheidsgraden geeft aan de afnemer van SAP producten. Hier geldt bijvoorbeeld de TDI (Tailored Datacenter Integration) certificering, naast de certificering op specifieke servers of appliances. Deze oplossing wordt door het Ministerie van Defensie momenteel gebruikt.

Cloud leveranciers zoeken om deze reden vaak contact met grote applicatieve spelers om hun naast hun generieke en publieke deel tevens invulling te kunnen geven aan specifieke applicatie-eisen en wensen van grote leveranciers. Soms worden er zelfs specifieke oplossingen gezamenlijk op de markt gebracht. Voor SAP is dit tevens het geval. De HANA Enterprise Cloud (HEC) is hier een goed voorbeeld van.

10.1.3.1 Infrastructuur bij ERP M&F

Het deel binnen de scope van het vooronderzoek bij ERF M&F werkt grotendeels met SAP applicaties. Deze applicaties werken allemaal met de nieuwe in memory database technologie van dezelfde firma, SAP HANA.

SAP HANA kent zeer specifieke eisen naar deze onderliggende infrastructuurlaag. Of het nu een on-premise oplossing betreft of wordt betrokken uit Cloud oplossingen van een derde partij welke SAP applicaties levert, allen dienen een gecertificeerde combinatie (door SAP getoetst) te gebruiken in de geleverde oplossing.

De huidig gebruikte infrastructurele laag bij ERP M&F gebruikt de laatste versie van het HANA product en deze wordt on-premise gebruikt. Deze laag kan tevens de nieuwe vraag voor de bovenliggende S/4HANA ondersteunen. De infrastructuurlaag echter heeft een onderhoudsperiode tot 2021 en dient te worden vervangen conform lifecycle beleid. Dit geeft een mogelijkheid om de S/4HANA implementatie gelijk op te laten lopen met de vervangingen in de infrastructuurlaag. Dit is een kans voor de S/4HANA implementatie om nieuwe componenten met andere applicatieve specificaties te kunnen leveren. Aan de andere kant geeft het een risico omdat de SAP HANA lifecycle niet voldoende houvast geeft op dit moment. De huidige versie blijft voorlopig ondersteund, maar bij de vorige overgang van HANA 1.0 naar 2.0 werden tevens de TDI eisen aangescherpt en verviel de support op specifieke hardware componenten. Versie 3.0 staat nog niet op de roadmap maar uiteraard is er ontwikkeling gaande. De vraag is wat de nieuwe TDI eisen gaan worden en wanneer er verwacht wordt een nieuwe aanscherping van hardware-eisen te gaan doen.

De huidige oplossing heeft beperkingen op de maximale omvang van de HANA database bijvoorbeeld. Deze kent een veel lagere grens (1,5TB) dan nu generiek verkrijgbare en gecertificeerde oplossingen. Met de keuze om bijvoorbeeld naar één S/4HANA platform te gaan en zoveel mogelijk in de huidige core te plaatsen (EWM, TM/EM, MDG-M, MGD-EAM, operationele delen van analytics nu in BW, BPC, etc.), zouden die grenzen mogelijk bereikt kunnen worden en is tijdig voorsorteren op de juiste infrastructuurlaag essentieel.

Het LCM project welke vervanging van het hosting platform ERP M&F in 2021, met geplande projectvoorbereiding in 2020, heeft deze HANA 3.0 informatie nodig om een robuust platform voor de komende jaren te kunnen faciliteren.

10.1.4 *Dataveiligheid*

De beveiliging van data zou het uitgangspunt moeten zijn voor alle databewerkingen. Concessies aan deze stelling dienen te worden afgewogen en eventueel apart te worden gevalideerd in een exceptie maatregel en goedgekeurd door de dataeigenaar, getoetst aan wet en regelgeving.

De algemene richtlijnen hiervoor staan in de BIO2019 en de D300. Defensie heeft invulling gegeven aan deze richtlijnen en deze geïmplementeerd binnen de huidige systemen. Dit wordt tevens periodiek getoetst en bewaakt, deels door de security organisatie van Defensie, deels door de Interne Auditdienst Rijk (ADR).

De Defensie IT strategie, bevat allerlei criteria over de richting welke de Defensie organisatie op zou willen en wellicht moeten gaan. Deze beleidsrichtingen echter moeten wel in de juiste balans met met de beveiligingseisen voor Defensie worden gezien. Naast de beleidsrichting is het tevens noodzakelijk richting te geven aan wet en regelgeving op IT vlak. Om die reden is het goed dat er wordt gewerkt aan een Cloudvisie (Cloud routekaart) zodat er gewogen en getoetst richting kan worden ingezet.

De Cloudvisie richt zich momenteel op de rubricering DEP-V, de hogere rubricering STG-C wordt (nog) niet belicht. De gebruikte Cloudvisie in dit stuk is nog niet gevalideerd en dient nog formeel te worden bekrachtigd en wordt nu alleen gebruikt om te kunnen reflecteren alsof dit de richting zou kunnen zijn.

5 Thema's van de Defensie IT strategie:

1. Robuust
2. Wendbaar
3. Weerbaar
4. Data gedreven
5. Interoperabel

Uitgangspunt voor Defensie is dat ze met moderne applicaties kunnen werken, flexibel zijn in het aanpassen van proces en organisatie en kunnen koppelen met derden, zowel met toeleveranciers als andere Defensie organisaties binnen en buiten NATO verband. Dit alles in een veilige en beschikbare omgeving.

Een ERP systeem kenmerkt zich door de volledige integratie van processen en centrale data. Het beveiligen van specifieke delen binnen zo'n systeem is complex, juist vanwege deze volledige integratie. De flexibiliteit welke Defensie zoekt aan de ene zijde met flexibiliteit en interoperabiliteit wordt beperkt door het rubriceren van data binnen het systeem. Vanwege de eenvoud wordt vaak het gehele systeem gerubriceerd op basis van de hoogste rubriceringsgraad van een enkele dataentiteit. Dit beïnvloedt direct de interoperabiliteit van het systeem. Een systeem mag zonder nadere maatregelen alleen worden gekoppeld met een systeem van gelijkwaardig rubriceringsniveau.

Verhoging van de rubricering van het ERP systeem blokkeert derhalve direct de mogelijkheden voor koppeling en flexibiliteit met systemen van ongelijk rubriceringsniveau.

De keerzijde is uiteraard de veiligheid van bepaalde dataentiteiten. Om deze reden dient voldoende te worden afgewogen of dataentiteiten van hoge rubricering wel in een ERP systeem moeten worden gecombineerd met dataentiteiten van een lager rubriceringsniveau. Wellicht weegt het separaat bedienen van deze dataentiteiten op tegen het plaatsen binnen een volledig geïntegreerde ERP omgeving. TCO calculaties dienen al deze aspecten te belichten.

10.1.5 *Landschapscomplexiteit, beheer & Ontwikkeling*

Complexiteit van het IT landschap kan een bedrijf weerhouden van flexibiliteit en interoperabiliteit. In algemene zin stijgen daarmee tevens de onderhoudskosten.

Waar voorheen de focus lag op het inzetten van een gestandaardiseerde systeem bus i.p.v. point-to-point interface oplossingen en ERP en ketenintegratie speerpunten waren hebben de meeste bedrijven deze punten nu doorgevoerd.

Momenteel zien we voornamelijk trends om schone kernsystemen te hebben en aanpassing in een flexibele schil onder te brengen, dit helpt de kern bij te blijven met de reguliere product lifecycle zonder verdere investeringen in beheer en geeft IT organisaties armslag de flexibiliteit verder te ondersteunen in de schil. Aanpassingen t.b.v. interoperabiliteit of aansluiting op nieuwe technologie wordt nu mogelijk zonder het geheel aan applicaties grondig te hoeven wijzigen. Tevens maakt deze aanpassing inzet van 'best-of-breed' oplossingen mogelijk, zolang koppelvlakken en datentiteiten uitwisselbaar zijn.

De marktbeveging naar Cloudoplossingen geeft niet alleen maar voordelen. Ook de inzet op verschuiving van randvoorwaardelijke systeemcomponenten t.b.v. beheer en ontwikkeling maken deze Cloud transformatie door. Hierdoor wordt de keuze in oplossingen in de on-premise omgeving beperkter. Sommige leveranciers hanteren nog een duidelijk tweesporen beleid, sommigen kiezen duidelijk voor één richting. De grote ERP leveranciers leveren allen Cloudoplossingen, naast on-premise omgevingen. Dit multispoor beleid is goed voor de groei van de markt, de gecontroleerde ontwikkeling van nieuwe diensten en biedt afnemers een brede keuze in oplossingen met een eigen afweging van risico per oplossing, of combinatie van oplossingen in een hybride opstelling van applicaties.

Het vanuit een Cloudomgeving beheerdiensten leveren of de ontwikkeling van applicaties aanbieden is tevens gemeengoed. Het gevolg is dat de ontwikkeling van nieuwe beheer- of ontwikkel-functionaliteit tevens verschuift naar Cloudoplossingen. De Defensie organisatie moet goed kijken naar toekomstige ontwikkelingen op dit vlak om niet, op relatief korte termijn, geblokkeerd te raken in beheer- en-of ontwikkel-functionaliteit voor de on-premise omgeving.

Kijkend naar SAP oplossingen is er uit de workshops naar boven gekomen dat de meeste hulpmiddelen nog on-premise worden ondersteund op dit moment. Voor de Fiori ontwikkeling echter is aangegeven dat Cloud ontwikkeling meer mogelijkheden geeft i.c.m. de (Public Cloud) SAP Cloud Platform functionaliteit voor aanpassingen en om technische koppelingen te kunnen realiseren in vergelijking met de on-premise faciliteiten. Of deze noodzakelijk zijn voor de standaardisatie en optimalisatie projecten in de tweede fase van het 'hergebruik' scenario of vanaf de inrichtingsfase bij scenario's 'nieuwe implementatie' of 'shell conversie' moet duidelijk worden in de fit-to-standard workshops.

10.1.6 *Applicaties & Interoperabiliteit*

Het samenwerken van applicaties is afhankelijk van twee zaken:

1. Het uitwisselen van gelijksoortige informatie;
2. Het kunnen communiceren tussen systemen en/of personen.

Het uitwisselen van gelijksoortige informatie heeft te maken met het doel van de informatie uitwisseling en de afspraken hieromtrent. Het formaat moet hier uitwisselbaar zijn en de mate van detail binnen de uitwisseling van minimaal gelijk niveau (veldlengte, veldtype, validatie etc.) of transformeerbaar op dit niveau.

Informatieveiligheid bepaalt daarnaast dat uitwisseling tussen bron en zender van gelijkwaardig veiligheidsniveau zijn. Tussen systemen van gelijke rubricering of in raakvlak met personen, dient het veiligheidsniveau van persoon en systeem gelijkwaardig te zijn. Bij ongelijkwaardigheid dient er ontkoppeld te worden, of volgen er aanvullende maatregelen.

Het kunnen communiceren heeft te maken met de technische laag. Fysiek bij informatie kunnen of een technische koppeling tussen systemen kunnen realiseren. Systemen moeten dan dezelfde taal (protocol) spreken en elkaar middels een verbinding kunnen bereiken. Personen moeten systemen kunnen raadplegen of onderhouden en systemen moeten personen kunnen bereiken (workflow, mail, TextToSpeech (TTS), etc.).

De mate van samenwerking tussen applicaties (interoperabiliteit) wordt zodoende bepaald door de methode van communicatie en mate van overeenkomst van dataentiteiten. Ook gevolgde processtappen kunnen bepalend zijn, (bijvoorbeeld status sturing, of confirmaties op verstuurd berichten) maar zijn minder relevant dan gestandaardiseerde communicatie methoden en uniforme dataentiteiten.

11 Acceptatiecriteria in het kader van het vooronderzoek

1	PSA omvat de complete scope van het uiteindelijke migratie traject zoals gedefinieerd in het Plan van Aanpak
2	Het minimale level van de gedefinieerde systemen is direct en aanpalend dan wel rand voorwaardelijk
3	Overzicht systeem kenmerken WRICEF & versies, add-on's, externe componenten
4	Acceptatie criteria vanuit architectuur
5	Acceptatie criteria vanuit security (controle met Risk & Security)
6	Acceptatie criteria vanuit data beheer
7	Acceptatie criteria vanuit beheer

12 Relatie met andere deelproducten

12.1 *Input van deelproduct*

- D.09 Huidige Architectuur
Bevat een op knelpunten gebaseerde inventarisatie van de huidige architectuur.
- D.24 Security Controls & Autorisatie

12.2 *Input voor deelproduct*

- D.15 Eind Architectuur
De architectuur eindstatus, de eind situatie van het verander pad welke deze PSA beschrijft.

13 Akkoord

Datum	Naam	Akkoord	Opmerking
12-11-2019	H.G.A. de Vreede		

14 Bijlage(n)

A.1 Architectuurbeslissingen

Beslissing 1	Netwerkbandbreedte operationele werkplekken is mogelijk te laag
Keuze	Randvoorwaardelijk voor Fiori inzet op de operationele werkplek
Rationale	De hedendaagse, maar zeker de toekomstige operaties vragen steeds meer van de beschikbare communicatiemiddelen. Dit geldt voor zowel de commandovoering als de applicaties voor de benodigde bedrijfsvoering. Veel van deze systemen maken gebruik van de schaarse satellietcapaciteit om connectie te maken met de datacentra van Defensie dan wel neven eenheden die niet met andere (operationele) communicatiemiddelen te bereiken zijn. De toe te wijzen bandbreedte is sterk afhankelijk van de behoefte van de desbetreffende eenheid, uiteen lopend van een logistieke basis in het uitzendgebied tot een enkel schip waar ook ter wereld. Echter de toe te wijzen bandbreedte is gelimiteerd. De toegepaste vuistregel vanuit J6 DOPS is 2 Mbps. Dit is dan de bandbreedte voor ALLE operationele en bedrijfvoeringssystemen. De benodigde bandbreedte voor S/4HANA is sterk afhankelijk van het aantal concurrent users en de uit te voeren transacties. Om hierover meer duidelijkheid te krijgen zal een meer diepgaand onderzoek moeten plaats vinden. Toekomst verwachting voor extra satellietcapaciteit is onduidelijk. Ondanks dat de defensienota spreekt over uitbreiding van satellietcapaciteit zijn er bij D-Plannen geen concrete projecten en financiële middelen geïnitieerd/beschikbaar gesteld om de satelliet capaciteit te vergroten.
Risico	Niet of onvoldoende functionerende operationele werkplek op locaties met lage bandbreedte (Missies en schepen)
Beperking	POC starten met specifiek doel het netwerkgebruik van de Fiori apps op de operationele werkplek te meten en hieraan conclusies te verbinden

Beslissing 2	Fiori launchpad op IOS apparaten niet in de Defensie Appstore toegestaan
Keuze	Applicatie niet gebruiken
Rationale	SAP ondersteunt momenteel deze applicatie niet meer en er zijn oplossingen dmv favorieten in de browsers voorhanden die dezelfde functionaliteit bieden
Risico	Geen
Beperking	Geen

Beslissing 3	Vertrouwelijke data via SAPRouter koppeling tbv S/4 diensten SAP (Readiness Check, BSR Report)
Keuze	Dit punt dient te worden besproken met Security vanuit architectuur en gedragen in een Defensie nota naar SAP met de beperkingen welke Defensie ziet in de geboden oplossingen van SAP.
Rationale	Het verwerken en beheren van SAP producten is een complexe activiteit die veel kennis vraagt van Defensie (BV en IT). SAP ontwikkelt voor het beheer van zijn software ook specifieke tooling en services. Denk hierbij aan tooling voor support, beveiliging, lifecycle management, onderhoud van de SAP producten, maar ook workshops voor de goede inrichting, enz. Voor het lifecycle management en onderhoud van de SAP producten is het momenteel al noodzakelijk dat meta gegevens over de SAP systemen van Defensie worden gedeeld met SAP via de geaccrediteerd externe koppeling. Voor het delen van informatie is het Defensie Beveiligingsbeleid (DBB) D/201 van toepassing. Voor de huidige koppeling is zgn. Statement of Compliance Koppeling (SoC-K) opgesteld waarna voor het gebruik van specifieke functies en het delen van specifieke data toestemming is verkregen voor het gebruik van de externe koppeling met SAP. SAP heeft met S/4 HANA de opvolger van het huidige SAP ERP uitgebracht. S/4 HANA is niet een eenvoudige upgrade van SAP ERP, maar een disruptieve ontwikkeling. Dit niet alleen vanwege het beschikbaar komen van nieuwe technologie zoals een nieuwe grafische gebruiker interface, maar ook gewijzigde functionaliteit die kan leiden tot aangepast bedrijfsvoering. Om de impact van de migratie en toekomstig lifecycle management acties te kunnen bepalen heeft SAP tooling ontwikkeld zoals de SAP Early Watch rapporten, de SAP Readiness Check en het SAP Business Scenario Recommendations rapport. Deze check en rapporten zullen de komende jaren noodzakelijk zijn voor de migratie naar S/4 HANA en het onderhoud daarop. Om gebruik te kunnen maken van deze tooling is het delen van informatie uit onze SAP systemen met SAP noodzakelijk. Standaard gaat SAP ervan uit dat door SAP systeem aanwezige rapporten deze informatie wordt verzameld en aan SAP ter beschikking wordt gesteld via een externe koppeling en via de "upload" faciliteit van de SAP support HUB op het internet. Niet altijd is even duidelijk welke gegevens SAP precies verzameld. Zelfs als dit wel wordt omschreven, zoals in SAP note 2758146 voor de SAP Readiness Check, is dit onderhevig aan "spontane" verandering door het aanbrengen van onderhoud op de SAP systemen bij Defensie. Zo is SAP note 2758146 tussen 20-5 en 23-9-2019 22 maal door SAP aangepast (van versie 12 naar versie 34). Dit kunnen kleine tekstuele aanpassingen zijn, maar ook aanpassingen aan programmatuur die andere data vraagt om betere rapporten te kunnen genereren. Het is daardoor ondoenlijk om steeds weer de veranderingen te analyseren en de procedure voor interne goedkeuring te volgen. Ook zijn niet alle services door SAP on- site te leveren. Onduidelijkheid over welke data gebruikt wordt en de hoge frequentie van veranderingen aan de programmatuur, maken het opzetten van een specifieke externe koppeling onmogelijk en daarmee ook het gebruik van deze SAP services. Het niet kunnen gebruiken van deze services geven een grote beperking in het bepalen van de impact bij wijzigingen van de SAP producten bij upgrades en onderhoud en veroorzaken een verhoogd risico voor de continuïteit van de dienstverlening.
Risico	Data uitwisseling zonder helderheid op inhoud
Beperking	
Beslissing 4	Werkplek voor operationeel optreden loopt achter in OS & browser versies
Keuze	Randvoorwaardelijk voor ondersteuning van de leverancier en werking van de Fiori applicaties in de webbrowser

Rationale	Binnen Defensie bestaan meerdere soorten werkplekken. Binnen MULAN bestaan de varianten 'Thin Client', 'Fat Client' en de 'LANTEK' werkplek (technische werkplek). De stand alone en de hoog mobiele werkplek zijn buiten beschouwing gelaten. In het operationele domein is dat de TITAAN werkplek. De versies van zowel de OS'n als de verschillende N20 en N30 applicaties van deze verschillende werkplekken lopen ver uiteen. De versie van Browsers zijn (vaak) gekoppeld aan versies van de OS'n. Fiori is sterk afhankelijk van de juiste versie van de browser. Lifecycle management speelt een steeds dominantere rol voor het ontsluiten van de gewenste functionaliteit. (voor de SAP GUI geldt dit ook echter ihkv S/4HANA is dit buiten beschouwing gelaten) Mulan: De Thin Client is up-to-date met de vigerende versies van Defensie. De updates worden gepushed waardoor deze automatisch met de juiste versies werken. De updates van Fat Client daarentegen wordt voornamelijk tot nu toe geactiveerd door de gebruiker nadat een updatemelding verschijnt. Het is aan de gebruiker om deze update uit te voeren. In de nabije toekomst wordt het beleid dit ook te pushen. Bij de LANTEK werkplek, specifiek ingericht om technische systemen aan te sturen (bv draaibank) is de aanname deze niet voor SAP doeleinden wordt ingezet. TITAAN: De operationele TITAAN werkplek loopt zeer sterk uiteen met de versies. Er wordt gemiddeld 1x per jaar een 'golden image' gemaakt. Dit is een afgeleide van de Mulan werkplek en aantal N20 en N30 applicaties aangevuld met operationele software. Deze image wordt bij nieuw in te zetten werkplekken ingespoeld. De werkplekken die nog niet operationeel ingezet zijn zal een migratie periode worden vastgesteld. Echter de operationele werkplekken die al ingezet zijn zal deze migratie zeer gefaseerd gaan dan wel worden ze pas gemigreerd indien de missie of operatie is afgelopen. De TITAAN werkplek wordt nu gemigreerd van Windows7 naar Windows10. Dit dient 04-2020 te zijn afgerond. De werkplekken in missies zullen voorlopig nog op Windows7 blijven draaien. TITAAN en Mulan zijn 2 verschillende domeinen met elk een eigen DNS. Dit houdt in dat de SAP gerichte URL vanuit TITAAN niet zal werken op Mulan en hiermee de koppeling van Fiori vanuit het operationele domein naar SAP in Mulan niet gemaakt kan worden. Hiervoor zijn meerdere oplossingen denkbaar; o.a. koppelen van de DNS'n of SAP te benaderen via VDI. VDI heeft meerdere voordelen: 1. Het lost de DNS problematiek op en 2. Het lost het versie beheer van de operationele werkplek op. Deze worden dan centraal beheerd. Een nadeel van de VDI oplossing is de bandbreedte. Deze is groter maar kan in aantal worden beperkt door een delicated VDI voor SAP te maken. Deze oplossing dient nader te worden onderzocht.
Risico	Beperkt mogelijk de ondersteuning en de functionaliteit van de SAP UI (Fiori)
Beperking	

Beslissing 5	SAP Fiori wordt op beperkt aantal browsers en versies ondersteund
Keuze	Elke werkplek op een door SAP ondersteunde configuratie laten functioneren en de laatste versies zo frequent mogelijk bijwerken, na het testen van de verschillende SAP webapplicaties. Zo mogelijk de Chrome browser op de werkplek implementeren deze heeft de meeste brede ondersteuning vanuit SAP.
Rationale	Meerdere webbrowsers in gebruik op de verschillende werkplekken daarnaast nog mobiele oplossingen. Door inzet van Fiori wordt de front-end applicatie de webbrowser, niet meer de SAP GUI die op de werkplek staat. Het advies van SAP is te gaan werken met Googles Chrome browser, deze wordt breed ondersteund. Voor de overige browsers is het vaak alleen de laatste of de laatste

	2 versies. De werkplekken lopen hier regelmatig achter op de gevraagde ondersteuning. - MULAN: IE11, Edge in 2020, Mozilla Firefox (Onderhoud 4 maal per jaar) - TITAAN: IE11 (Onderhoud 1 maal per jaar) - Mobiele toepassingen: - IOS -> Safari (laatste 2 versies ondersteund) - Android -> ? - Windows Mobile - Uitdaging voor het onderhoud van de werkplek en zal in randvoorwaarden voor het project moeten worden vastgelegd. Werking van de Fiori lag direct afhankelijk van de interoperabiliteit met de browser.
Risico	Beperkt mogelijk de ondersteuning en de functionaliteit van de SAP UI (Fiori)
Beperking	

Beslissing 6	Hoge complexiteit van de te beheren omgeving
Keuze	Opnemen in beoordelingscriteria in Architectuur criteria en in Eisen SAP tbv Infrastructuur
Rationale	De complexiteit kan niet vanuit Architectuur worden gereduceerd. Echter beïnvloed. Vanuit hosting zowel architectuur kunnen selectiecriteria helpen in het op langere termijn reduceren van complexiteit, door standaardisatie en sturing op TCO.
Risico	
Beperking	

Beslissing 7	Perceptie: Relatief hoge hoeveelheid maatwerk
Keuze	De hoeveelheid maatwerk wordt door SAP als laag gekwantificeerd. Binnen het vooronderzoek is met name gekeken naar de relevantie van het maatwerk tot de migratie en eventuele reductie ervan. Binnen TCO calculaties opnemen van maatwerk opties en bewegen naar standaard SAP oplossingen als uitgangspunt definiëren. Antwoorden zijn gegeven in de werkgroep Proces & Integratie binnen deelproducte As-Is, To-Be, Fit/Gap
Rationale	Het deelproduct As-Is, To-Be, Fit-gap vanuit de Proces & Integratie werkstroom geeft de details op dit vlak
Risico	
Beperking	

Beslissing 8	Materiaalnummer lengte aanpassing & veldinhoud
Keuze	Dit punt is nader toegelicht binnen de deelproducten D.10, D14 en verwerkt in D.08
Rationale	Zie genoemde deelproducten
Risico	
Beperking	

Beslissing 9	Zakenpartner conversie nog niet uitgevoerd in ECC
Keuze	Dit punt is nader toegelicht binnen deelproducten D.10, D.14 en verwerkt in D.08
Rationale	Zie genoemde deelproducten
Risico	
Beperking	

Beslissing 10	TM wel of niet in de S/4Core																																																																																													
Keuze	In de S/4Core opnemen																																																																																													
Rationale	Decentral TM Functionaliteit TM Add-on on S/4HANA S/4HANA ERP Backend Decentral TM Functionaliteit TM Add-on on Netweaver S/4HANA ERP Backend Embedded TM Functionaliteit TM Add-on S/4HANA ERP Backend Architectuur beoordelingscriteria <table><tr><th></th><th colspan="5">IT is Robuust</th><th colspan="3">IT is Wendbaar</th><th>IT is digitaal Weerbaar</th><th colspan="2">IT is Data gedreven</th><th colspan="2">IT is Interoperabel</th><th>TCO</th><th>Eindscore</th></tr><tr><th></th><th>Continuïteit</th><th>Autonomie</th><th>Beheer</th><th>Toekomstvastheid</th><th>Best Practise</th><th>Schaalbaarheid</th><th>Uniformiteit</th><th>Gebruiksgemak/vriendelijkheid</th><th>Beveiliging</th><th>Performance</th><th>Integratie</th><th>Aansluiting op civiele & militaire standaarden</th><th></th><th></th><th></th></tr><tr><td>Wegingsfactor</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr><tr><td>Oplossing 1</td><td>3</td><td>4</td><td>2</td><td>4</td><td>2</td><td>5</td><td>4</td><td>4</td><td>4</td><td>4</td><td>3</td><td>5</td><td>3</td><td>47</td></tr><tr><td>Oplossing 2</td><td>1</td><td>4</td><td>1</td><td>1</td><td>1</td><td>4</td><td>1</td><td>1</td><td>1</td><td>4</td><td>1</td><td>3</td><td>1</td><td>24</td></tr><tr><td>Oplossing 3</td><td>5</td><td>3</td><td>5</td><td>5</td><td>5</td><td>3</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>61</td></tr></table>		IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven		IT is Interoperabel		TCO	Eindscore		Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practise	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriendelijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden				Wegingsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Oplossing 1	3	4	2	4	2	5	4	4	4	4	3	5	3	47	Oplossing 2	1	4	1	1	1	4	1	1	1	4	1	3	1	24	Oplossing 3	5	3	5	5	5	3	5	5	5	5	5	5	5	61
	IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven		IT is Interoperabel		TCO	Eindscore																																																																															
	Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practise	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriendelijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden																																																																																		
Wegingsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1																																																																															
Oplossing 1	3	4	2	4	2	5	4	4	4	4	3	5	3	47																																																																																
Oplossing 2	1	4	1	1	1	4	1	1	1	4	1	3	1	24																																																																																
Oplossing 3	5	3	5	5	5	3	5	5	5	5	5	5	5	61																																																																																
Risico	Beveiliging: Op Netweaver is outdated, is risico. Embedded eenduidiger en eenvoudiger te																																																																																													

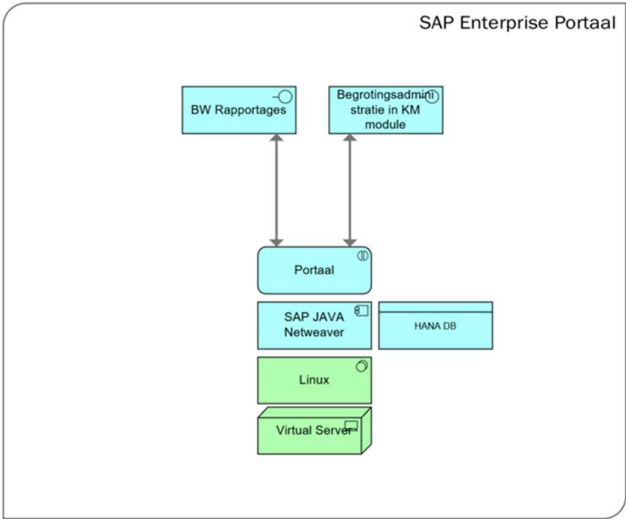
	beveiligen. Geen externe koppeling
Beperking	Continuïteit: TM op Netweaver maar tot 2025, strategie SAP TM embedded Autonomie: Geen 5 vanwege geen volledige disconnected operations ondersteuning Beheer: Beheer outdated product (Netweaver) en extra variant SAP, embedded is meest effectief in beheer Toekomstvastheid: zie continuïteit Best Practise: geen opmerking Schaalbaarheid: Schaalbaarheid binnen de zelfde IT architectuur is voor een HUB makkelijker Uniformiteit: Uniformiteit via Fiori UI (NetWeaver score 1 vanwege afwijkende UI) Eén logisch systeem geeft meer uniformiteit Gebruikersgemak/vriendelijkheid: Fiori moderne UI score 1, GUI verouderde UI score 1 Performance: Mits goed gesized geeft alleen embedded nog een extra voordeel. Minder Netwerk verkeer Integratie: oplossing 3 integratie out-of-the box. Overige oplossing integratie zelf realiseren Aansluiting op Civiele en Mil standaarden: strategie SAP TCO: geen opmerking

Beslissing 11	EWM wel of niet in de S/4Core																																																																																																									
Keuze	Opnemen in de S/4Core. Hybrid oplossing als embedded oplossing niet aan functionele behoefte voldoet.																																																																																																									
Rationale	Decentral EWM Functionaliteit EWM Add-on on S/4HANA S/4HANA ERP Backend Decentral EWM Functionaliteit EWM Add-on on Netweaver S/4HANA ERP Backend Embedded EWM Functionaliteit EWM Add-on S/4HANA ERP Backend Hybrid EWM Functionaliteit EWM Add-on on S/4HANA S/4HANA ERP Backend EWM Functionaliteit EWM Add-on Architectuur beoordelingscriteria <table><tr><th></th><th colspan="5">IT is Robuust</th><th colspan="3">IT is Wendbaar</th><th>IT is digitaal Weerbaar</th><th>IT is Data gedreven</th><th colspan="2">IT is Interoperabel</th><th>TCO</th><th>Eindscore</th></tr><tr><th></th><th>Continuïteit</th><th>Autonomie</th><th>Beheer</th><th>Toekomstvastheid</th><th>Best Practise</th><th>Schaalbaarheid</th><th>Uniformiteit</th><th>Gebruiksgemak/vriendelijkheid</th><th>Beveiliging</th><th>Performance</th><th>Integratie</th><th>Aansluiting op civiele & militaire standaarden</th><th></th><th></th></tr><tr><td>Wegingsfactor</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr><tr><td>Oplossing 1</td><td>4</td><td>4</td><td>3</td><td>4</td><td>4</td><td>4</td><td>4</td><td>5</td><td>4</td><td>4</td><td>3</td><td>5</td><td>2</td><td>50</td></tr><tr><td>Oplossing 2</td><td>1</td><td>4</td><td>1</td><td>1</td><td>1</td><td>4</td><td>1</td><td>1</td><td>1</td><td>3</td><td>1</td><td>3</td><td>1</td><td>23</td></tr><tr><td>Oplossing 3</td><td>5</td><td>3</td><td>5</td><td>5</td><td>5</td><td>3</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>61</td></tr><tr><td>Oplossing 4</td><td>4</td><td>3</td><td>2</td><td>5</td><td>4</td><td>5</td><td>3</td><td>5</td><td>2</td><td>4</td><td>3</td><td>5</td><td>1</td><td>46</td></tr></table>		IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven	IT is Interoperabel		TCO	Eindscore		Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practise	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriendelijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden			Wegingsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Oplossing 1	4	4	3	4	4	4	4	5	4	4	3	5	2	50	Oplossing 2	1	4	1	1	1	4	1	1	1	3	1	3	1	23	Oplossing 3	5	3	5	5	5	3	5	5	5	5	5	5	5	61	Oplossing 4	4	3	2	5	4	5	3	5	2	4	3	5	1	46
	IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven	IT is Interoperabel		TCO	Eindscore																																																																																												
	Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practise	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriendelijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden																																																																																														
Wegingsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1	1																																																																																												
Oplossing 1	4	4	3	4	4	4	4	5	4	4	3	5	2	50																																																																																												
Oplossing 2	1	4	1	1	1	4	1	1	1	3	1	3	1	23																																																																																												
Oplossing 3	5	3	5	5	5	3	5	5	5	5	5	5	5	61																																																																																												
Oplossing 4	4	3	2	5	4	5	3	5	2	4	3	5	1	46																																																																																												
Risico	Beveiliging: Op Netweaver is outdated, is risico. Embedded eenduidiger en eenvoudiger te beveiligen. Geen externe koppeling																																																																																																									
Beperking	Continuïteit: EWM op Netweaver maar tot 2025, strategie SAP EWM embedded Autonomie: Geen 5 vanwege geen volledige disconnected operations ondersteuning. Hybrid score 3 voor continuïteit magazijn Beheer: Beheer outdated product (Netweaver) en extra variant SAP, embedded is meest effectief in beheer Toekomstvastheid: zie continuïteit Best Practise: geen opmerking Schaalbaarheid: Schaalbaarheid in hybride het hoogst vanwege verdelen werklast Uniformiteit: Uniformiteit via Fiori UI (NetWeaver score 1 vanwege afwijkende UI) Eén logisch systeem geeft meer uniformiteit Gebruiksgemak/vriendelijkheid: Fiori moderne UI score 1, GUI verouderde UI score 1 Performance: Mits goed gesized geeft alleen embedded nog een extra voordeel. Minder Netwerk verkeer Integratie: oplossing 3 integratie out-of-the box. Overige oplossing integratie zelf realiseren Aansluiting op Civiele en Mil standaarden: strategie SAP TCO: geen opmerking																																																																																																									

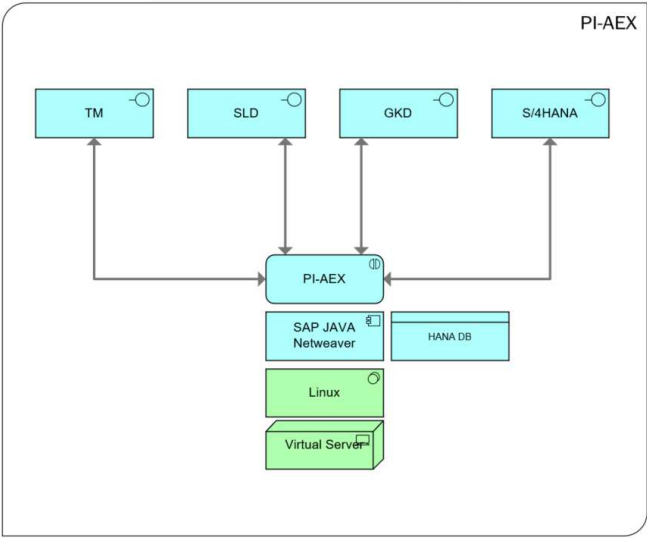
Beslissing 12A	Fiori Front-end server wel/niet in de S/4Core																																																																										
Keuze	Fiori Frond-end server in de Core voor alle producten die op een eigen core blijven (S/4HANA, BW/4HANA, MDG)																																																																										
Rationale	HUB Deployment Fiori Launchpad UI Frontend Odata backend Embedded Deployment Fiori Launchpad UI Frontend Odata backend Architectuur beoordelingscriteria <table><tr><th></th><th colspan="5">IT is Robuust</th><th colspan="3">IT is Wendbaar</th><th>IT is digitaal Weerbaar</th><th>IT is Data gedreven</th><th>IT is Interoperabel</th><th></th><th></th></tr><tr><th></th><th>Continuïteit</th><th>Autonomie</th><th>Beheer</th><th>Toekomstvastheid</th><th>Best Practise</th><th>Schaalbaarheid</th><th>Uniformiteit</th><th>Gebruiksgemak/vriende lijkheid</th><th>Beveiliging</th><th>Performance</th><th>Integratie</th><th>Aansluiting op civiele & militaire standaarden</th><th>TCO</th><th>Eindscore</th></tr><tr><td>Wegingsfactor</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td></td></tr><tr><td>Oplossing 1</td><td>3</td><td>4</td><td>2</td><td>3</td><td>3</td><td>5</td><td>5</td><td>4</td><td>3</td><td>4</td><td>4</td><td>4</td><td>2</td><td>46</td></tr><tr><td>Oplossing 2</td><td>5</td><td>4</td><td>5</td><td>5</td><td>5</td><td>3</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>62</td></tr></table> SAP adviseert en dit is in de Proof-of-concept beproeft, om de Fiori Front-end server in de Core te plaatsen. Hierdoor is het mogelijk rapid-deployment te gebruiken van Fiori gebaseerd op rollen. In de situatie van een HUB dient dit per Fiori App te worden opgezet en verhoogd nodeloos het beheer op alle Apps.		IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven	IT is Interoperabel				Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practise	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriende lijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden	TCO	Eindscore	Wegingsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1		Oplossing 1	3	4	2	3	3	5	5	4	3	4	4	4	2	46	Oplossing 2	5	4	5	5	5	3	5	5	5	5	5	5	5	62
	IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven	IT is Interoperabel																																																																
	Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practise	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriende lijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden	TCO	Eindscore																																																													
Wegingsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1																																																														
Oplossing 1	3	4	2	3	3	5	5	4	3	4	4	4	2	46																																																													
Oplossing 2	5	4	5	5	5	3	5	5	5	5	5	5	5	62																																																													
Risico	De performance van de Fiori Front-End server kan negatief worden beïnvloed door het gebruik van de core en vice versa.																																																																										
Beperking	Fysieke beperkingen in de hardware en de virtuele laag kunnen hier voor beperkingen in het scenario zorgen. Dit is echter in de SAP detail sessies ter voorbereiding van dit deelproduct als risico naar voren gekomen. De sizing is wel op hoog niveau uitgevoerd. Alle componenten bij elkaar in de S/4core passen in de huidige hardware oplossing tot 2021. Continuïteit: Fiori beter dan GUI, strategie Fiori embedded Autonomie: Geen 5 vanwege geen volledige disconnected operations ondersteuning. Beheer: Embedded geeft Fiori Rapid deployment Toekomstvastheid: zie continuïteit Best Practise: geen opmerking Schaalbaarheid: Schaalbaarheid binnen de zelfde IT architectuur is voor een HUB makkelijker Uniformiteit: Uniformiteit via Fiori UI Gebruikersgemak/vriendelijkheid: Fiori embedded score 5, hub score 4 is complex (autorisaties) Beveiliging: Embedded eenduidiger en eenvoudiger te beveiligen. Geen externe koppeling Performance: Mits goed gesized geeft alleen embedded nog een extra voordeel. Minder Netwerk verkeer Integratie: oplossing 2 meest eenvoudig geïntegreerd Aansluiting op Civiele en Mil standaarden: strategie SAP																																																																										

	TCO: geen opmerking
--	---------------------

Beslissing 12B	Fiori Front-end server wel/niet Hybride FLP configuratie																																																																											
Keuze	Fiori front-end sever 1:1 verbinden, geen kruisverbanden																																																																											
Rationale	Hybrid Deployment Hybrid Deployment Architectuur beoordelingscriteria <table><tr><th></th><th colspan="5">IT is Robuust</th><th colspan="3">IT is Wendbaar</th><th>IT is digitaal Weerbaar</th><th>IT is Data gedreven</th><th colspan="2">IT is Interoperabel</th><th>TCO</th><th>Eindscore</th></tr><tr><th></th><th>Continuïteit</th><th>Autonomie</th><th>Beheer</th><th>Toekomstvastheid</th><th>Best Practice</th><th>Schaalbaarheid</th><th>Uniformiteit</th><th>Gebruiksgemak/vriende lijkheid</th><th>Beveiliging</th><th>Performance</th><th>Integratie</th><th>Aansluiting op civiele & militaire standaarden</th><th></th><th></th></tr><tr><td>Wegsfactor</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td></td></tr><tr><td>Oplossing 1</td><td>5</td><td>1</td><td>1</td><td>1</td><td>1</td><td>5</td><td>1</td><td>5</td><td>1</td><td>3</td><td>5</td><td>5</td><td>1</td><td>35</td></tr><tr><td>Oplossing 2</td><td>5</td><td>1</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>1</td><td>5</td><td>5</td><td>3</td><td>5</td><td>5</td><td>55</td></tr></table> Deze oplossing wordt bepaald door de effecten en randvoorwaarden van koppeling. Oplossing 1 geeft een afhankelijkheid van de Fiori laag in de eerste applicatie naar de tweede applicatie. Versies moeten gelijk blijven voor een correcte werking. Een verwijzing binnen de FLP naar een FLP van een andere applicatie werkt onafhankelijk van versies en heeft een sterke voorkeur.		IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven	IT is Interoperabel		TCO	Eindscore		Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practice	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriende lijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden			Wegsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1		Oplossing 1	5	1	1	1	1	5	1	5	1	3	5	5	1	35	Oplossing 2	5	1	5	5	5	5	5	1	5	5	3	5	5	55
	IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven	IT is Interoperabel		TCO	Eindscore																																																														
	Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practice	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriende lijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden																																																																
Wegsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1																																																															
Oplossing 1	5	1	1	1	1	5	1	5	1	3	5	5	1	35																																																														
Oplossing 2	5	1	5	5	5	5	5	1	5	5	3	5	5	55																																																														
Risico																																																																												
Beperking																																																																												

Beslissing 13	Einde ondersteuning SAP Portaal 31-12-2024
Keuze	Het portaal kan worden vervangen als de Grootboekadministratie oplossing in de KM module wordt verplaatst naar BO, deze actie is vastgelegd binnen de Roadmaps Analytics van JIVC. Vervanging van de rolegebaseerde toegang naar de applicatie kan door directe aanroep van de Fiori Frontend server middels de Fiori Launchpad.
Rationale	 The diagram illustrates the SAP Enterprise Portaal architecture. At the top, two boxes represent 'BW Rapportages' and 'Begrotingsadministratie in KM module'. These are connected by double-headed arrows to a central 'Portaal' box. Below the 'Portaal' box is 'SAP JAVA Netweaver', which is connected to 'HANA DB' on the right. The 'Portaal' and 'SAP JAVA Netweaver' boxes are connected by a double-headed arrow. Below 'SAP JAVA Netweaver' is 'Linux', which is connected to 'Virtual Server' at the bottom. The entire architecture is enclosed in a rounded rectangle labeled 'SAP Enterprise Portaal'. Eindegebruikers kunnen in de browser direct de Fiori Launchpad aanroepen ipv de Webgui via het portaal. Zolang de KM functionaliteit is verplaatst naar de BO omgeving. Overigens is het Architectuurbeleid strijdig met het KM gebruik momenteel.
Risico	Geen
Beperking	

Beslissing 14	Productopvolging SLD
Keuze	Volgens SAP wordt deze vervangen door een opvolger binnen het on-premise landschap.
Rationale	Solution Landscape Directory (SLD) <pre>graph TD; PI-AEX <--> SLD; SOLMAN <--> SLD; Portaal <--> SLD; S/4HANA <--> SLD; SLD <--> SAP_JAVA[SAP JAVA Netweaver]; SAP_JAVA <--> HANA_DB[HANA DB]; HANA_DB <--> Linux; Linux <--> Virtual_Server[Virtual Server];</pre>
Risico	
Beperking	

Beslissing 15	Productopvolging PI-AEX
Keuze	Volgens SAP wordt dit product vervangen door een JAVA PO 7.6 opvolger binnen het On-premise landschap.
Rationale	 The diagram illustrates the PI-AEX system architecture. At the top, four SAP modules (TM, SLD, GKD, and S/4HANA) are shown in light blue boxes. Below them is the PI-AEX component, also in a light blue box. Arrows indicate bidirectional communication between each of the four top modules and the PI-AEX component. Below the PI-AEX component is the SAP JAVA Netweaver layer, shown in a light blue box. To the right of the Netweaver is the HANA DB database, shown in a light blue box. Below the Netweaver is the Linux operating system, shown in a green box. At the bottom is the Virtual Server, shown in a green box. The entire system is enclosed in a rounded rectangle labeled 'PI-AEX' in the top right corner.
Risico	Geen
Beperking	Mogelijk is uitfasering van PI mogelijk door overname van deze functionaliteit direct in het GKD.

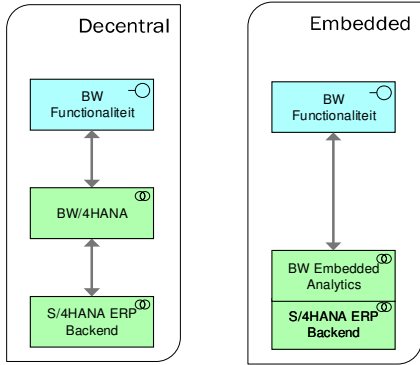
Beslissing 16	Opvolging Nextlabs
Keuze	Volgen van de bestaande oplossing voor S/4HANA
Rationale	Besprekingen gaande met betreffende leverancier. Deze geeft aan dat een deel reeds bestaat in de applicatie en een deel
Risico	
Beperking	

Beslissing 17	Opvolging CUA
Keuze	Volgens SAP blijft dit product onderdeel van de ABAP-stack binnen het on-premise landschap.
Rationale	The diagram illustrates the Central User Administration (CUA) architecture. It is a stack-based system. At the bottom is a 'Virtual Server' (green box). Above it is 'Linux' (green box). Then 'SAP ABAP Netweaver' (blue box) and 'HANA DB' (blue box). Above SAP ABAP Netweaver is the 'CUA' component (blue box). CUA is connected to four application components: 'BW', 'MDG', 'S/4HANA', and 'TM' (all blue boxes). All connections are bidirectional, indicated by arrows with open heads at both ends.
Risico	Opvolging is noodzakelijk voor alle Java gebaseerde applicaties in het landschap
Beperking	

Beslissing 18	Opvolging Solution Manager
Keuze	SAP heeft aangegeven dat er opvolging komt na versie 7.2. De Solution manager wordt nu gebruikt voor ITSM, CHaRM en Technische Monitoring. De eerste twee componenten blijven in het Solution Manager product. De laatste komt in een vervangend product van SAP, Focussed Run.
Rationale	

Risico	
Beperking	

Beslissing 19	Vervanging voor ontbrekende EH&S functionaliteit in S/4HANA
Keuze	Randvoorwaardelijk voor Migratie: Opname in specifiek implementatie project voor vervangende functionaliteit
Rationale	Functionaliteit is momenteel aanwezig in het ECC systeem, maar zal niet meer aanwezig zijn in S/4HANA.
Risico	Ontbrekende functionaliteit bij livegang indien niet vooraf ontworpen
Beperking	

Beslissing 20	BW operationele rapportages wel/niet naar de S/4core
Keuze	N.v.t.
Rationale	 Dit betreft geen architectuurkeuze maar een inrichtingsprincipe op basis van de functionele behoefte. 1 dag oude informatie uit BW eventueel aangevuld met data uit overige bronsystemen en/of historische data of directe rapportage uit Embedded Analytics met S/4HANA data.
Risico	
Beperking	

Beslissing 21	MDG wel/niet naar de S/4Core																																																																																										
Keuze	Niet naar de S/4core																																																																																										
Rationale	Decentral MDG Functionaliteit MDG Add-on on BS S/4HANA ERP Backend Decentral MDG Functionaliteit MDG Add-on on S/4HANA S/4HANA ERP Backend Embedded MDG Functionaliteit MDG Add-on S/4HANA ERP Backend Architectuur beoordelingscriteria <table><tr><th></th><th colspan="5">IT is Robuust</th><th colspan="3">IT is Wendbaar</th><th>IT is digitaal Weerbaar</th><th>IT is Data gedreven</th><th colspan="2">IT is Interoperabel</th><th>TCO</th><th>Eindscore</th></tr><tr><th></th><th>Continuïteit</th><th>Autonomie</th><th>Beheer</th><th>Toekomstvastheid</th><th>Best Practice</th><th>Schaalbaarheid</th><th>Uniformiteit</th><th>Gebruiksgemak/vriendelijkheid</th><th>Beveiliging</th><th>Performance</th><th>Integratie</th><th>Aansluiting op civiele & militaire standaarden</th><th></th><th></th></tr><tr><td>Wegingsfactor</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr><tr><td>Oplossing 1</td><td>1</td><td>5</td><td>1</td><td>1</td><td>1</td><td>5</td><td>1</td><td>1</td><td>1</td><td>4</td><td>1</td><td>2</td><td>1</td><td>25</td></tr><tr><td>Oplossing 2</td><td>5</td><td>5</td><td>2</td><td>5</td><td>5</td><td>5</td><td>4</td><td>5</td><td>4</td><td>4</td><td>3</td><td>5</td><td>3</td><td>55</td></tr><tr><td>Oplossing 3</td><td>3</td><td>3</td><td>5</td><td>3</td><td>2</td><td>3</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>4</td><td>5</td><td>53</td></tr></table> De roadmap van MDG producten laat op dit moment een korte lifecycle zien, door deze korte cycles is plaatsing in de S/4core niet in het belang van continuïteit en stabiliteit. Op het moment dat dit product minder aan veranderingen onderhevig lijkt kan het in de S/4Core worden opgenomen.		IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven	IT is Interoperabel		TCO	Eindscore		Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practice	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriendelijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden			Wegingsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Oplossing 1	1	5	1	1	1	5	1	1	1	4	1	2	1	25	Oplossing 2	5	5	2	5	5	5	4	5	4	4	3	5	3	55	Oplossing 3	3	3	5	3	2	3	5	5	5	5	5	4	5	53
	IT is Robuust					IT is Wendbaar			IT is digitaal Weerbaar	IT is Data gedreven	IT is Interoperabel		TCO	Eindscore																																																																													
	Continuïteit	Autonomie	Beheer	Toekomstvastheid	Best Practice	Schaalbaarheid	Uniformiteit	Gebruiksgemak/vriendelijkheid	Beveiliging	Performance	Integratie	Aansluiting op civiele & militaire standaarden																																																																															
Wegingsfactor	1	1	1	1	1	1	1	1	1	1	1	1	1	1																																																																													
Oplossing 1	1	5	1	1	1	5	1	1	1	4	1	2	1	25																																																																													
Oplossing 2	5	5	2	5	5	5	4	5	4	4	3	5	3	55																																																																													
Oplossing 3	3	3	5	3	2	3	5	5	5	5	5	4	5	53																																																																													
Risico	Beveiliging: Op BS outdated, is risico. Embedded eenduidiger en eenvoudiger te beveiligen. Geen externe koppeling																																																																																										
Beperking	Continuïteit: MDG op Netweaver maar tot 2025, strategie SAP & Utopia is Hub. Autonomie: Geen 5 vanwege geen volledige disconnected operations ondersteuning. Beheer: Beheer Business Suite (BS) per 31-12-2015 outdated product en extra variant SAP, embedded is meest effectief in beheer Toekomstvastheid: zie continuïteit Best Practise: strategie SAP & Utopia is HUB 95% klanten is Hub. Schaalbaarheid: Schaalbaarheid binnen de zelfde IT architectuur is voor een HUB makkelijker Uniformiteit: Uniformiteit via Fiori UI (daarom Netweaver score 1). Eén logisch systeem geeft meer uniformiteit Gebruikersgemak/vriendelijkheid: Fiori score 5, GUI score 1 Performance: Mits goed gesized geeft alleen embedded nog een extra voordeel. Minder Netwerk verkeer Integratie: oplossing 3 meest eenvoudig geïntegreerd Aansluiting op Civiele en Mil standaarden: geen opmerking TCO: geen opmerking																																																																																										

A.2 NON-SAP Add-ons in de migratie

De volgende applicaties zijn relevant voor de werking van SAP vanwege het feit dat ze als Add-on zijn geladen in de huidige ECC omgeving:

1. Nextlabs
2. Runbook
3. Every Angle
4. BWISE

In dit hoofdstuk wordt voor elk van deze vier applicaties beoordeeld of de oplossing kan samenwerken met S/4HANA. In het geval dat een applicatie niet aansluitbaar is, zullen de te treffen mitigerende maatregelen worden voorgesteld.

De inventarisatie omvat de volgende aspecten:

1. *Applicatie-informatie*
 - *Functionaliteit*
 - *ProductLifeCycle*
 - *Beheerder applicatie*
2. *Leverancier*
3. *Informatie door leverancier over de werking van de oplossing met S/4HANA*
4. *Praktische toets van de werking van de applicaties met S/4HANA (facultatief)*
5. *Conclusies over aansluiting op S/4HANA*

A.2.1 Nextlabs

Applicatieinformatie

Functionaliteit

- Datamasking-oplossing buiten SAP
- Defensie heeft de 'advanced solution'-versie van Nextlabs aangeschaft (toekomstvast voor S4HANA, incl. TM en D&S).

ProductLifeCycle

(Roadmap en integratie met S/4HANA)

- De implementatie van de eerste fase van NextLabs geeft aanleiding tot bezinning over de verdere inzet van Nextlabs. Mogelijk is het de oplossing voor de komende 3 a 4 jaar (dus relevant voor de migratie naar S4HANA).
- Defensie overweegt (op termijn) NextLabs te vervangen door de datamasking-oplossing van SAP.

Beheerder applicatie:

rol	deel proces	naam	organisatie	locatie
Eigenaar		KLTZ DGA Bruins	HDBV	Den Haag
Coördinerend beheerder	JIVC/M&F	H. Wichhart	JIVC/IT/M&F	Utrecht
Verantwoordelijke Beheerder	PV	J. v Diest	JIVC/ITT Services	Den Helder
Verantwoordelijke Beheerder	TV	M. Benjamins	JIVC/ITT Services	Den Helder
Uitvoerend beheerder	Applicatie server park	W. Hoedjes	JIVC/ITT Service/unit 2	Den Helder
Uitvoerend beheerder	Functioneel NextLabs	RGW. D. Bruin	JIVC/IT/M&F	Utrecht
Uitvoerend beheerder	SAP Landschap	M. Sassen	JIVC/IT/M&F	Utrecht

Leverancier: Nextlabs

Informatie door leverancier

Nextlabs werkt voor S/4HANA, incl. TM en D&S. Nextlabs bevestigt de werking op S4HANA

Aandachtspunt is de tijdige beschikbaarheid van een werkende oplossing voor BW4HANA.

Praktische toets van de werking van de applicaties met S/4HANA (facultatief): open

Conclusies over aansluiting op S4HANA

Nextlabs is weliswaar geschikt voor S4HANA, maar reeds tijdens de eerste toepassing van Nextlabs (op ECC) rijzen vragen over de bruikbaarheid van de oplossing.

Reactie van de leverancier: Voor Native Fiori Apps heft NextLabs support, de Base + Pack for S/4 dienen hiervoor te worden geïnstalleerd. Maatwerk implementatie objecten dienen te worden aangepast.

Voor Fiori Analytic Apps welke CDS view gebruiken en gebruikmaken van de DPC (Data Provider Class) framework worden ondersteund. Voor de overige Apps wordt nog gewerkt aan ondersteuning voor de meest kritische, in een gefaseerde uitrol.

A.2.2 Runbook

Applicatieinformatie

Functionaliteit

(bron: *Modellenatlas*) Runbook ondersteunt de Interne Controle/het periodeafsluitingsproces binnen de SAP applicatie.

ProductLifeCycle

- (bron: *PLP*) Periodiek technische updates van leverancier Runbook doorvoeren
- Runbook Smart Close biedt een on-premise oplossing die embedded is. Deze oplossing is door SAP gecertificeerd voor S/4HANA. Een Cloud-variant (bruikbaar voor meer applicaties dan SAP) zal tzt beschikbaar komen. Er zijn echter diverse signalen dat Runbook niet S/4-bestendig is:
 - Na 2021 stopt de leverancier Blackline de support van Runbook
 - De beschikbare oplossing werkt via CDS-views (gebruikmakend van de R3-transacties en het ECC- datamodel) en wordt niet verder ontwikkeld voor S/4-transacties.
- Blackline ontwikkelt Runbook Smart close verder onder Blackline smart close (ook een SAP add on), een optie.
- Een alternatief is de SAP S/4HANA Financial Closing Cockpit als opvolger van Runbook. SAP biedt de cockpit zowel voor on-premise als in de cloud (dan met meer functionaliteit). De oplossing is een integraal onderdeel van S/4HANA en ondersteunt de toepassing van Fiori. Er is een aparte licentie vereist.
Er is geen tooling voor de conversie van Runbook naar SAP FCC beschikbaar; een overstap naar de SAP-oplossing vereist ondersteuning door een SAP-consultant. Daarbij moet de behoefte aan archivering en de beschikbaarheid van historie (o.a. audit logging) worden bepaald.

Beheerder Runbook: Asha Oedairadjsingh

Leverancier: Blackline

Informatie door leverancier

- De software van Runbook sluit aan op SAP ERP-software en wordt gebruikt door ondernemingen voor het optimaliseren van financiële verslagleggingsprocedures.
- Runbook is door SAP gecertificeerd voor S/4HANA.

Praktische toets van de werking van de applicaties met S/4HANA (facultatief): open

Conclusies over aansluiting op S/4HANA

- Runbook is niet geschikt voor S/4HANA.
- Alternatieve oplossingen zoals Blackline Smart Close en SAP FCC moeten worden onderzocht.

INTERMEZZO

In de volgende twee paragrafen wordt de toekomstvastheid van Every Angle en B Wise beschreven. Daaraan voorafgaand enkele generieke opmerkingen over Enduser-oplossingen op het gebied van analytics.

M&F heeft een roadmap voor M&F-analytics opgesteld:

- De Selfservice BI betreft M&F-Bedrijfsspecifieke Analytics, niet generiek voor geheel Defensie. Omwille van de voortgang is er voor gekozen niet te wachten op het Defensie (big) data advanced analytics platform.
- Voor de huidige enduser-tools (Every Angle, B Wise) is nog geen – als alternatief - toekomstvaste SAP-oplossing voorhanden. Er is nog geen datum voor de uitfasering van Every Angle en B Wise bepaald.
- De essentie voor analytics is het inrichten van een logisch datamodel voor M&F, minder op de analytics-tooling. Dit datamodel geeft per object een eenduidige definitie van alle gegevens, die zowel door de bedrijfsvoering en de IT wordt gedragen.
- Het logisch datamodel is een degelijke basis voor alle mogelijke analytics-tools, waaronder Every Angle en B Wise. De aanpassing van het datamodel samenhangend met de implementatie van S4HANA zullen de interface (download gegevens vanuit SAP-gegevens) en de rapportages worden heringericht. Dit zal geen showstopper voor de implementatie van S/4HANA blijken.

A.2.3 Every Angle

Applicatieinformatie

- Functionaliteit

Every Angle is een door SAP AG gecertificeerde applicatie waarmee de gebruiker op eenvoudige wijze overzichten kan creëren over gegevens afkomstig uit het Defensie SAP systeem ERP M&F. Deze querytool in gebruik binnen de SAP-omgeving als zogenaamde add-on. EA doet de query binnen het SAP-proces terwijl BW (Business Warehouse) achteraf een rapportage maakt.

- ProductLifeCycle: de Roadmap Analytics voorziet een uiteindelijke uitfasering van Every Angle. De planning van de realisatie van de roadmap is nog niet hard.
- Beheerder applicatie: FB Patrick Obbes, TB Ron de Graaf, AB externe inhuur

Leverancier: Magnitude/Every Angle Software Solutions BV

Informatie door leverancier

Every Angle is compatible met SAP HANA. Bovendien belooft de leverancier snellere en eenvoudigere dataextractie en snellere ontwikkeling van aanvullende angles (leidend tot near real-time analytics). Voor de complexere rapportages kan de Every Angle Model Server nog gebruikt worden.

SAP waarschuwt echter dat Every Angle niet is aangepast op de nieuwe tabellen van S/4HANA en derhalve niet toekomstvast is.

Praktische toets van de werking van de applicaties met S/4HANA (facultatief): open

Conclusies over aansluiting op S/4HANA

De toekomstvastheid van Every Angle is vanwege vermoede ontbrekende aanpassingen van het datamodel (noodzakelijk voor de werking na de migratie naar S/4HANA) twijfelachtig.

De Roadmap Analytics voorziet in de vervanging van Every Angle door alternatieve (SAP-) tooling.

A.2.4 B Wise

Applicatieinformatie

- Functionaliteit:
De ADR zet B Wise als riskmanagement-tool (internal audit/control, compliance, security, governance).
B Wise is een op een lokale PC geïnstalleerde oplossing, die via een verbinding gegevens uit SAP ophaalt. De verbinding is niet geaccrediteerd en mogelijk niet veilig.
- ProductLifeCycle: een opdracht van de ADR aan JIVC (M&F IT) om B Wise door een alternatieve oplossing te vervangen is er vooralsnog niet.
- Beheerder applicatie: belegd bij de ADR (niet JIVC)

Leverancier: SAI Global

Informatie door leverancier: op de website heb ik geen informatie over aansluiting op S/4HANA aangetroffen.

Praktische toets van de werking van de applicaties met S/4HANA (facultatief): open

Conclusies over aansluiting op S/4HANA

Aanpassingen aan het datamodel samenhangend met de migratie naar S/4HANA zullen aanpassingen in de interface vereisen. Het gaat om een enkelvoudige interface; de aanpassing is haalbaar.

De beheeractiviteiten zijn buiten JIVC belegd. Dit betekent dat de end user (ADR) verantwoordelijk is voor de noodzakelijke aanpassingen in de interface en het reportingtool/rapportages.

Bijlage 2 Gerelateerde (en BRON) DOCUMENTATIE

Voor deze PSA zijn de volgende uitgangspunten/-documenten gebruikt:

1. Strategische doelstellingen Defensie
2. Specifieke militaire wetgeving
3. Nederlandse wet- en regelgeving
4. Internationale wet- en regelgeving
5. Nederlandse normering
6. Nationale- en internationale data standaarden t.b.v. optimale ketensamenwerking en certificering

A.3 Bijlage 4 Lijst Gebruikte afkortingen

Afkorting	Omschrijving
POC	Proof of Concept
PSA	Project Start Architectuur
TBB	Te beschermen Belangen
ADR	Audit Dienst Rijk