



## **D.24 & D.25: Security, autorisaties en interne beheersing**

### **S/4HANA onderzoek**

Datum: 20 december 2019

Plaats: Den Haag

Auteurs: Werkstroom RC&C

Versie: 1.0

| <b>Documentbeheer</b> |               |                           |              |                                                                                        |
|-----------------------|---------------|---------------------------|--------------|----------------------------------------------------------------------------------------|
| <b>Versie</b>         | <b>Status</b> | <b>Auteur(s)</b>          | <b>Datum</b> | <b>Opmerking</b>                                                                       |
| <b>0.1</b>            | Concept       | Werkstroom RC&C           | 01-11-2019   |                                                                                        |
| <b>0.5</b>            | Concept       | Werkstroom RC&C           | 23-11-2019   |                                                                                        |
| <b>0.6</b>            | Concept       | Werkstroom RC&C           | 24-11-2019   |                                                                                        |
| <b>0.6.1</b>          | Concept       | Jeroen Kunis              | 27-11-2019   | Review notes                                                                           |
| <b>0.6.1</b>          | Concept       | Guido Thimister           | 27-11-2019   | Review notes                                                                           |
| <b>0.8</b>            | Concept       | Whitney van Steekelenburg | 29-11-2019   | Input project management en SAP verwerkt<br><br>Totaaloverzicht observaties toegevoegd |
| <b>0.9</b>            | Concept       | Frank Hakkennes           | 4-12-2019    | Input QA verwerkt<br><br>Management samenvatting toegevoegd                            |
| <b>1.0</b>            | Definitief    | Stuurgroep                | 20-12-2019   |                                                                                        |

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

|                                               |           |
|-----------------------------------------------|-----------|
| <b>Management samenvatting</b>                | <b>5</b>  |
| <b>1 Introductie</b>                          | <b>7</b>  |
| 1.1 Inleiding                                 | 7         |
| 1.2 Doel van het deelproduct                  | 7         |
| 1.3 Randvoorwaarden                           | 8         |
| 1.4 Uitgangspunten                            | 8         |
| 1.5 Acceptatiecriteria                        | 9         |
| <b>2 Benadering</b>                           | <b>10</b> |
| 2.1 Scope                                     | 10        |
| 2.2 Aanpak                                    | 10        |
| <b>3 Resultaat</b>                            | <b>11</b> |
| 3.1 Autorisaties & Security                   | 11        |
| 3.1.1 Security en autorisatie                 | 11        |
| 3.1.2 Security- & Beheerprocessen             | 19        |
| 3.1.3 GRC and tooling                         | 26        |
| 3.2 Interne beheersing                        | 29        |
| 3.2.1 Applicatiecontroles                     | 29        |
| 3.3 Samenvatting observaties en aanbevelingen | 42        |
| <b>4 Relatie met andere deelproducten</b>     | <b>45</b> |
| 4.1 Input van deelproduct                     | 45        |
| 4.2 Input voor deelproduct                    | 45        |
| <b>5 Akkoord</b>                              | <b>46</b> |
| <b>6 Bijlage(n)</b>                           | <b>47</b> |



## Management samenvatting

Het op effectieve wijze implementeren van autorisaties, security en interne beheersing is randvoorwaardelijk voor de migratie naar S/4HANA. Naast het aanpassen van de technische architectuur, functionaliteiten en processen worden er in S/4HANA diverse nieuwe security concepten geïntroduceerd. Indien dit niet of niet op een effectieve wijze wordt geadresseerd, bestaat het risico dat enerzijds gebruikers in de toekomst taken niet volledig kunnen uitvoeren. Anderzijds bestaat het risico dat kwetsbaarheden worden geïntroduceerd waardoor ongeautoriseerde personen toegang krijgen tot vertrouwelijke informatie, dat onjuiste of frauduleuze handelingen niet worden voorkomen of opgemerkt en dat financiële- en procesmatige informatie onjuist wordt weergegeven. Om de ambities ten aanzien van het verwerken en verschaffen van real-time informatie te kunnen realiseren dient de kwaliteit van processen en data tijdens- en na migratie op de juiste wijze geborgd te worden.

De huidige opzet van zowel autorisaties als interne beheersing blijkt niet goed aangesloten bij het daadwerkelijke gebruik in de huidige SAP omgeving. Beheersmaatregelen werken niet zoals beschreven in het controleraamwerk. Het autorisatiemodel is verouderd en gebruikt meerdere concepten door elkaar wat dit lastig schaalbaar maakt naar S/4HANA.

Het advies is om voorafgaand aan de migratie de uitgangspunten, vereisten en doelarchitectuur uit te werken zodat er voldoende basis is de bovengenoemde risico's af te dekken tijdens en na de migratie. Dit geldt zowel voor het autorisatieconcept, de security inrichting als mede de relevante interne beheersingsmaatregelen.

### *Impact migratie – Simplification*

- Bij hergebruik is de impact beperkt voor autorisaties en security. Er zijn diverse transacties en tabellen die niet meer bestaan en waarvoor rollen inhoudelijk aangepast dienen te worden. Het grootste deel van de autorisatie- en security checks zal bij conversie goed blijven werken;
- Er bestaat nu maatwerk voor uitvoeren van interne beheersingsmaatregelen. Een deel van deze maatregelen zal niet meer werken na conversie door technische aanpassingen. Het advies is daarom om alle relevante maatregelen expliciet mee te nemen in de fit-to-standard analyse, design en test werkzaamheden.

### *Impact migratie - Fiori*

De introductie van Fiori heeft een grote impact op autorisaties, security & interne beheersing.

- Fiori introduceert een additioneel autorisatieconcept voor gebruikerstoegang wat vraagt om aanpassing van het huidige concept en toevoeging van een nieuwe autorisatie laag;
- T.a.v. security zal Fiori additioneel opgenomen dienen te worden in de security configuratie en monitoring procedures;
- Interne beheersmaatregelen zullen opnieuw gedefinieerd en ontworpen moeten worden voor gebruik met Fiori door introductie van nieuwe schermen en processen;
- Daarnaast zullen alle huidige uitgangspunten en tools voor monitoring van zowel autorisaties, security en interne beheersing opnieuw ingericht moeten worden.

### *Architectuur en projecten*

Met S/4HANA en aanverwante technologieën worden diverse nieuwe concepten geïntroduceerd die het toestaan om data makkelijker te ontsluiten. Daarnaast lopen er meerdere projecten die (op termijn) geïntegreerd kunnen worden met S/4HANA om zo een veilig en efficiënt te beheren platform te realiseren. Dit betreft o.a. de implementatie van NextLabs voor data-afscherming, SailPoint voor identity management en CyberArk voor privileged access management. Het verdient aanbeveling om

voorafgaand aan de implementatie deze projecten en nieuwe technologische opties op te nemen in een integrale roadmap voor autorisaties, security en interne beheersing om zo een oplossing te realiseren die klaar is voor de toekomst, op efficiënte wijze beveiliging en beheersing ondersteunen en (toekomstige) additionele kosten door overlap of correcties voorkomt.

#### *Security & Control by design*

Ongeacht het te volgen migratiescenario is het advies om zowel autorisaties en security als ook interne beheersing als integraal onderdeel van de migratieaanpak op te nemen. Daarbij dient ook de huidige set aan maatregelen geëvalueerd te worden om waar mogelijk standaardisatie toe te passen. Het verdient aanbeveling om het huidige controle raamwerk als een integraal onderdeel van het SAP S/4HANA project te vernieuwen zodat optimaal gebruik gemaakt kan worden van standaard S/4HANA functionaliteiten, controles goed aansluiten bij de (vernieuwde) procesgang en vanaf de migratie direct met een goed beheerste omgeving gewerkt kan worden. Daarbij dient ook de noodzaak van de huidige maatregelen op zichzelf beoordeeld te worden zodat alleen relevante maatregelen worden geïmplementeerd in S/4 en geen oude knelpunten worden meegenomen.

## **1 Introductie**

Dit stuk vormt de gecombineerde uitwerking van de individuele deelproducten "D.24 Aanpak informatiebeveiliging" en "D.25 Aanpak interne beheersing".

### **1.1 Inleiding**

De overgang naar S/4HANA maakt het ERP-landschap van Defensie klaar voor de toekomst. Onder andere door het introduceren van nieuwe technieken, nieuwe integratiemogelijkheden, vernieuwde gebruikersinterfaces en mogelijke aanpassingen in functionaliteit en procesgang. Potentieel kunnen al deze aspecten een impact hebben op de maatregelen die zijn vereist en gewenst ten aanzien van beveiliging of beheersing. Voorbeelden hiervan zijn:

- Introductie van de FIORI-gebruikersinterface, welke een nieuw autorisatieconcept introduceert;
- Het aanpassen van processen om standaard SAP te volgen, waardoor procescontroles mogelijk mede aangepast dienen te worden;
- Wijzigingen in de tabelstructuur kunnen ervoor zorgen dat huidige maatregelen en rapportages niet meer werken;
- Het gebruiken van nieuwe mogelijkheden aangeboden in S/4HANA kan huidige controlemaatregelen overbodig maken, zoals het automatisch aansluiten tussen general ledger en sub ledger;
- Het ontsluiten van sensitieve data naar mobile apparaten brengt nieuwe cyber risico's met zich mee.

Dit deelproduct beschrijft de uitwerking van de activiteiten uitgevoerd door de werkstroom Risk, Cyber & Control. Deze werkstroom richt zich op het voorzien van input ter beantwoording van de onderzoeksvragen waar dit relateert aan de relevante risicobeheersingsdomeinen. De focus van deze activiteiten is het bepalen van de impact welke de migratie naar S/4HANA kan hebben ten aanzien van informatiebeveiliging, autorisaties en interne beheersing. Tevens wordt beschreven met welke aspecten rekening gehouden dient te worden voor het plannen en uitvoeren van de migratie en eventuele verschillen tussen de geanalyseerde migratiescenario's.

### **1.2 Doel van het deelproduct**

Het doel van dit gecombineerde deelproduct is te beschrijven wat de impact is op informatiebeveiliging, autorisaties en interne beheersing bij migratie naar S/4HANA. Hierbij wordt inzicht gegeven in de veranderingen, nieuwe mogelijkheden en uitdagingen voor de in het vooronderzoek uitgewerkte migratiescenario's. Deelonderwerpen die zijn onderzocht zijn onder andere:

- Security configuratie
- Gebruikersbeheer
- Authenticatie
- Rollen en rechten
- Compliance aspecten, waaronder privacy
- Interne beheersing en (geautomatiseerde) controles

Naast het inzicht geven in de wijzigingen en mogelijke impact wordt beschreven welke voorbereidende werkzaamheden er uitgevoerd kunnen worden om de startcondities van een eventuele migratie te verbeteren.

### **1.3 Randvoorwaarden**

De volgende randvoorwaarden worden gesteld aan dit gecombineerde deelproduct:

- De op het moment geldende uitgangspunten en richtlijnen zijn gehanteerd als uitgangspunt voor de vereisten ten aanzien van beveiligingsbeleid en interne controle. Zie deelproduct D.23 voor een beschrijving van de relevante normeringen.
- Alleen de relevante migratiescenario's zoals beschreven in deelproduct 2.6 migratieaanpak zijn meegenomen.
- Lessons learned vanuit zowel de markt als Defensie dienen meegenomen te worden als input voor de uitwerking van dit deelproduct;
- De beschrijving van dit deelproduct moet de toetsing van de inhoud ten opzichte van het toetsingskader ondersteunen;
- Het deelproduct dient gericht te zijn op het realiseren van de in PvA beschreven end-state.

### **1.4 Uitgangspunten**

De activiteiten uitgevoerd door de werkstroom RC&C volgen de projectaanpak zoals beschreven in het plan van aanpak. Het belangrijkste uitgangspunt hieruit vormt de fit-for-purpose aanpak. Ter illustratie, bij het bepalen van de impact van S/4HANA op het autorisatiemodel is gefocust op het verkrijgen van een globaal beeld van de mogelijkheden, beperkingen en benodigde aanpassingen voor elk van de gekozen migratiescenario's. Het is bijvoorbeeld niet zo dat alle bestaande SAP-applicatierollen zijn getest op compatibiliteit met S/4HANA. Applicatierollen werden getest in overeenstemming met gekozen POC-processen.

Binnen het onderzoek worden de volgende uitgangspunten gehanteerd (overgenomen uit het plan van aanpak):

- Defensie wil de gedane investering in de huidige omgeving niet verloren laten gaan. Dit betekent dat wordt ingezet op zo min mogelijk (functionele) wijzigingen tijdens de migratie.
- Defensie gaat uit van een implementatie van S/4HANA in een private cloud omgeving op basis van GRIT.
- Elk scenario voor de transformatie moet te allen tijde de continuïteit en integriteit van de Defensie bedrijfsvoering waarborgen.
- De transitie zal resulteren in een volledige overgang waarbij de bestaande SAP-omgevingen op termijn geheel buiten gebruik worden gesteld.
- De aanpak die Defensie zal volgen, b.v. de gefaseerde benadering versus volledige S/4HANA met Fiori moet nog worden besloten.
- De migratie dient in een zo kort mogelijk tijdsbeslag te worden uitgevoerd.
- De impact op de bedrijfsvoering, juist bij operationele inzet dient zo klein mogelijk te zijn. Er zullen daarom tijdens de migratiefase zo min mogelijk ingrijpende functionele wijzigingen in de IV en BV worden uitgevoerd.
- De doorlooptijd migratie dient zo kort mogelijk te zijn.
- Defensie wil maximaal gebruik maken van uitgekristalliseerde standaardoplossingen die door S/4HANA worden geboden. Er wordt zeer terughoudend omgegaan met het implementeren van "oplossingen" die afwijken van deze standaard.
- Ondanks dat er een beperkt aantal wijzigingen in de BV wordt uitgevoerd, wordt wel nadrukkelijk gekeken naar eenvoudig te realiseren verbeteringen waarvan de BV direct toegevoegde waarde ervaart. Denk hierbij bijvoorbeeld aan het verbeteren van de Grafische User Interface en de verbeterde mogelijkheden om real time data uit het systeem te kunnen extraheren.
- De ERP-strategie van defensie wordt nadrukkelijk als uitgangspunt gehanteerd.

## **1.5 Acceptatiecriteria**

De volgende acceptatiecriteria zijn geïdentificeerd voor dit gecombineerde deelproduct:

- Duidelijke afbakening relevante risicodomeinen zoals autorisaties, cyber, interne beheersing, data risico's, privacy, etc.;
- Bepaalde aanpak voor RC&C adresseert in voldoende mate geldende uitgangspunten en richtlijnen voor informatiebeveiliging, privacy en beheersing;
- Bepaalde aanpak voor RC&C wordt gedragen door projectmanagement;
- Afhankelijkheden met andere deelproducten zijn afgestemd met betreffende werkstromen.

## 2 Benadering

### 2.1 Scope

De volgende uitgangspunten worden voor RC&C gehanteerd:

1. Onderzoek is uitgevoerd met inachtneming van verschillende migratiescenario's. Deze scenario's zijn beschreven in deelproduct 2.6 *migratieaanpak*.
2. De doelarchitectuur voor RC&C is gefocust, maar niet beperkt tot enkel de ECC-omgeving. Afhankelijkheden en interfaces met andere systemen, zoals TM, SolMan, BW, MDG, ISDS, Nextlabs en diverse security tools zijn in beschouwing genomen om een effectieve en toekomstbestendige architectuur te kunnen realiseren.
3. De mogelijke impact van gerelateerde projecten is meegenomen in het onderzoek. In deelproduct 2.13 *Afstemming andere projecten* is de algemene relatie met overige projecten beschreven. In dit doorproduct zijn eventuele specifieke aandachtsgebieden benoemd die betrekking hebben op autorisaties, security of interne beheersing.

### 2.2 Aanpak

De aanpak voor dit gecombineerde deelproduct is uitgevoerd in de volgende stappen:

1. Verkrijgen begrip van de AS-IS situatie op basis van beschikbare procesdocumentatie, systeemconfiguratie huidig landschap en ervaring van betrokken teamleden.
2. Analyseren van de impact bij migratie naar S/4HANA zoals beschreven in deelproduct D.23. Voor deze analyse is gebruik gemaakt van de migratiescenario's zoals beschreven in deelproduct 2.6. Naast het inbrengen van eerdere (S/4 gerelateerde) projectervaring is ook gebruik gemaakt van de POC-omgeving voor technische en procesmatige validatie.
3. Uitwerken observaties en aanbevelingen.

De werkstroom RC&C bestaat uit de onderstaande teamleden. Daarnaast zijn diverse validatiewerkzaamheden uitgevoerd in samenwerking met teamleden uit de andere werkstromen en met vertegenwoordigers vanuit IV en BV voor bijvoorbeeld validatie in de POC-omgeving.

- Mark Riem Vis Teamleider Defensie
- Frank Hakkennes Teamleider Deloitte
- Jeen Murk Specialist SAP autorisaties
- Guido Thimister Specialist SAP security
- Jeroen Kunis Specialist interne beheersing
- Lionel Prinsloo Specialist SAP autorisaties & security Deloitte
- Whitney van Steekelenburg Specialist interne beheersing Deloitte

### 3 Resultaat

In dit hoofdstuk worden de resultaten beschreven voor Autorisaties en security (sectie 3.1) en voor interne beheersing (sectie 3.2).

#### 3.1 Autorisaties & Security

Om in de toekomstige S/4HANA omgeving te kunnen voldoen aan de beveiligingsstandaarden zoals vereist is tijdens het vooronderzoek vastgesteld wat de impact is van de verschillende migratie scenario's. Dit betreft de impact op gebruikersbeheer, rollen en autorisaties en de SAP-beveiligingsconfiguratie (sectie 3.1.1), ondersteunende beheerprocessen (3.1.2) en ondersteunende tooling (3.1.3).

##### 3.1.1 Security en autorisatie

De introductie van S/4HANA met Fiori voegt nieuwe dimensies toe aan de SAP-omgeving bij Defensie. Tevens levert het ook nieuwe tools en functionaliteiten op die kunnen worden gebruikt om de toegang tot systeemfuncties en -bronnen te beheren en te beperken. Dit omvat bijvoorbeeld CDS-views, UI Masking en UI Logging en Fiori-apps. De verandering in processen en functionaliteit met ingebedde SAP-modulen vereist een nieuwe kijk op het huidige autorisatieconcept en ontwerp.

##### 3.1.1.1 AS-IS situatie

Het security ontwerp van de bedrijfsprocessen die door SAP M&F worden ondersteund zijn vastgelegd in Business Control Diagrams (BCD's). De door Defensie gehanteerde bedrijfsprocessen zijn in Aris gemodelleerd. Aris is een business process management tool welke binnen Defensie wordt gebruikt voor het inrichten van processen en autorisaties. De security mapping, van transactie tot processtap en transactie tot rol, wordt beschouwd als de norm voor de systeeminrichting van SAP. Het huidige beveiligingsontwerp is als volgt opgezet:

1. Processen zijn gedocumenteerd in Aris;
2. Processtappen worden toegewezen aan transacties in Aris;
3. Transacties worden toegewezen aan master taakrollen in Aris;
4. Master taakrollen worden toegewezen aan samengestelde rollen in Aris;
5. Beperkingsvereisten worden in aparte Excel tabs afgebeeld, bijvoorbeeld bedrijfscodes of bewegingstypen;
6. Master- en afgeleide rolcontext wordt gebruikt voor rolontwerp en rolopbouw;
7. Rollen worden indirect en rechtstreeks aan gebruikers-ID's binnen de applicatie toegewezen. Standaard wordt toegang wordt toegewezen via indirecte toewijzing en extra vereiste specifieke toegang wordt toegewezen via rechtstreekse toewijzing. Toegang via indirect-toewijzingen wordt gewijzigd via HR-acties en gebruikers-ID's via het aanvraagproces.

##### 3.1.1.2 Impact S/4HANA

Door van de huidige SAP ECC-omgeving naar de nieuwe SAP S/4HANA-infrastructuur te migreren, dient Defensie opnieuw kijken naar het SAP-landschap, en het gerelateerde autorisatiemodel- en ontwerp. De nieuwe omgeving brengt nieuwe uitdagingen met zich mee die de huidige opzet omtrent het verlenen en beperken van toegang tot gegevens en functies binnen het SAP-landschap wijzigen. De belangrijkste wijziging is de introductie van de Fiori gebruikersinterface, waarbij de toegangsrechten op zowel de SAP S/4HANA omgeving als de Fiori omgeving dienen te worden gerealiseerd en beheerd.

De impact van S/4HANA omvat, maar is niet beperkt tot, concepten zoals:

- Veranderingen in het datamodel en beschikbare transacties (simplificatie) waardoor bestaande autorisatie- en securityinrichting mogelijk niet meer juist werkt;
- Aanpassingen van functionaliteiten of introductie van nieuwe functies waarvoor nieuwe autorisaties gerealiseerd dienen te worden;
- Fiori-apps en tegels;
- HANA DB en Data Control Language (DCL) die ook CDS-weergaven omvat;
- UI Masking en UI Logging functionaliteiten.

De rest van deze sectie is gewijd aan het gedetailleerder bekijken van de impact van de bovengenoemde concepten op de (tot nu toe) standaard manier om gebruikerstoegang te definiëren binnen Defensie.

### Simplificatie

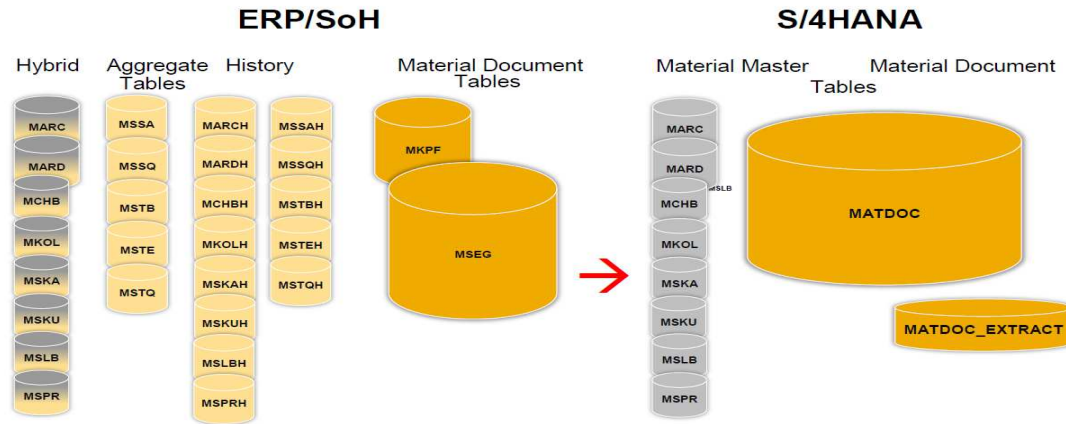
Bij migratie naar S/4HANA wordt zogenoemde simplificatie toegepast om een efficiënter datamodel en geoptimaliseerde gebruikerservaring te bieden. Als onderdeel van de migratie zullen huidige transacties, autorisatieobjecten en tabellen vervallen of worden gewijzigd. Ter illustratie, er zijn ongeveer 100.000 transactie codes in SAP ECC6 beschikbaar en er zijn ongeveer 7600 nieuwe transacties geïntroduceerd in S/4. Voorbeelden waar simplificatie impact heeft zijn geschetst in de onderstaande scenario's.

- Masterdata transacties zijn gecombineerd in één centrale transactie.
  - Transacties FK01, MK01, VD01, XD01 XK01 en 49 andere transacties zijn gecombineerd in transactie "BP".
  - Toegang tot specifieke functionaliteit in transactie BP, b.v. het onderhouden van de klant of leverancier wordt beperkt door het veld "BP-rol".
  - Beperking op lager niveau wordt beheerd door andere velden als voorheen in ECC.
  - Transactie BP is toegankelijk via meerdere Fiori-apps zoals te zien in de onderstaande tabel (dit zijn slechts enkele van de apps) die de verschillende 'views' binnen de masterdata zullen weergeven.  
Functiescheiding wordt verplaatst naar een object- en veldniveau in plaats van een transactieniveau en omvat verschillende objecten, velden en veldwaarden dan in de ECC-instelling.

| Fiori app | Fiori app beschrijving              |
|-----------|-------------------------------------|
| F0850A    | Manage Customer Master Data         |
| F1053A    | Manage Supplier Master Data         |
| F2429     | Business Partner Financial Overview |
| F2505     | Mass Maintenance for Master Data    |
| F3163     | Manage Business Partner Master Data |

- S/4HANA combineert de datastructuren van verschillende componenten (voor FI, AA, CO, CO-PA en ML) in een enkele tabel ACDOCA, genaamd Universal Journal. Het elimineert verschillende aggregatietabellen en indextabellen. Nu hoeven gegevens in slechts één enkele tabel te worden ingevoegd in plaats van meerdere tabellen, waardoor de hoeveelheid data wordt verminderd.
- MATDOC is ook een nieuwe tabel voor voorraadbeheer en elimineert hiermee 26 tabellen (zie hieronder). Materiële documenten worden opgeslagen in MATDOC maar niet in MKPF- of MSEG-

tabellen.



De bovenstaande scenario's illustreren dat de simplificatie en de introductie van nieuwe Fiori apps zal leiden tot een groot aantal benodigde aanpassingen in het autorisatiemodel. Immers, op het moment refereren de rollen naar toegang tot transacties en tabellen die straks niet meer bestaan. Daarnaast dienen de autorisaties aangepast te worden om nieuwe S/4HANA functionaliteiten te ondersteunen, zoals toegang tot nieuwe Fiori applicaties, of nieuwe of toekomstige functies die worden geïntroduceerd met aanpassingen in TM, EWM of D&S.

Als onderdeel van het vooronderzoek is tijdens POC-1 geanalyseerd hoe groot de impact van de simplificatie is bij migratie volgens het scenario 'hergebruik'. Echter dient hierbij te worden vermeld, dat de POC niet alle end-to-end processen heeft behandeld. De simplificatie lijst is geanalyseerd en er zijn diverse validaties uitgevoerd tijdens de POC1 testen. Tevens zijn er testactiviteiten uitgevoerd door IV en BV medewerkers met huidige autorisaties om zo de impact vast te kunnen stellen. De testresultaten tonen aan dat de impact in dit scenario beperkt is. Zoals verwacht zijn er diverse transacties en autorisatieobjecten niet meer beschikbaar. Het aantal dat is geraakt tijdens de POC-1 werkzaamheden is echter beperkt en betreft voornamelijk functionaliteit uit de QM-module, welke niet breed wordt toegepast. Het merendeel van de testscenario's kon goed worden uitgevoerd met de bestaande autorisaties.

### Fiori en toegangspunten

SAP Fiori is een nieuwe gebruikerservaring (UX) voor SAP-software en bijbehorende -applicaties. Fiori biedt een set applicaties die worden gebruikt in reguliere zakelijke functies zoals werkgoedkeuringen, financiële processen, berekeningsprocessen en verschillende self-serviceprocessen. SAP Fiori biedt op het moment meer dan 300 rol gebaseerde applicaties zoals Manufacturing, inkoop, finance, etc. SAP Fiori ondersteunt meerdere gebruiker platforms waarmee gebruikers een proces op hun desktop/laptops kunnen starten en dat proces potentieel kunnen voortzetten op bijvoorbeeld een smartphone of tablet. SAP heeft Fiori Apps ontwikkeld op basis van gebruikersinterface UI5.

## Fiori Apps Overview

A total of 1150+ Fiori apps are available across process areas, 393 of which are Finance apps in the latest 1610 version. Fiori apps can be categorized under the following 4 categories.



Met de introductie van Fiori voor SAP-systemen heeft SAP ook een nieuwe manier geïntroduceerd om toegang te krijgen tot functionaliteit in de SAP-omgeving. Naast het verlenen van toegang op de traditionele manier via transacties en rollen in de backend, wordt Fiori-toegang verleend via Fiori-apps, groepen, catalogi en rollen in de front-end. Hier heeft de gebruiker ook de relevante toegang in de backend nodig. Dit creëert twee toegangslagen die moeten worden ontworpen, geïmplementeerd en onderhouden. Echter hebben niet alle 'transacties' een vervangende Fiori-app, waardoor voor veel S/4 implementatie gebruik via de traditionele GUI nog steeds wordt toegepast. Het is wel mogelijk traditionele transacties via Fiori beschikbaar te stellen door het maken van een UI5-tegel. Dit is eigenlijk een webgui-versie van de transactie waarmee de Fiori look and feel behouden kan blijven.

De impact die de introductie van Fiori heeft is afhankelijk van de manier waarop FIORI wordt geïmplementeerd. Dit kan als centrale hub, waarbij er een aparte FIORI-gateway server wordt toegevoegd aan het landschap, of embedded, waarbij de FIORI-server wordt gedraaid op de S/4HANA instance. Bij de implementatie van S/4HANA en Fiori middels het 'centrale hub' model, dienen de rollen en rechten op twee verschillende servers aangemaakt, beheerd en toegekend te worden aan de gebruiker. Er dient in dit geval een Fiori rol voor het front-end aan de gebruiker toegekend te worden, en daarbij een additionele rol op de backend. Als de toekenning van deze twee rollen niet goed met elkaar is afgestemd kan het zijn dat de gebruiker wel autorisaties heeft in de backend om functionaliteit uit te voeren, maar de beschikbare schermen en knoppen niet kan zien en gebruiken in FIORI.

Indien er gebruik wordt gemaakt van het embedded model, is er de mogelijkheid om ervoor te kiezen één gecombineerde rol aan te maken voor zowel het Fiori front-end als het backend systeem. Op dit moment wordt toegang voor gebruikers in ECC beschikbaar gesteld via directe (gebruikers-ID) en indirecte (HR-positie) toewijzingen. Het beheren van twee autorisatielagen brengt extra complexiteit mee voor deze indirecte toekenning, omdat in geval van een fiori hub-inrichting de HR-masterdata niet noodzakelijkerwijs op de Fiori-server staan.

Daarnaast zal het ontsluiten van Fiori-apps via mobiele apparaten de behoefte aan netwerkbeveiliging en transmissieprotocollen beïnvloeden, aangezien dit betekent dat nieuwe integratiecomponenten worden gebruikt en de SAP-omgeving mogelijk (deels) gekoppeld zal worden aan het Internet. Vanwege de interconnectiviteitsmogelijkheden van S/4HANA en integratie met apparaten die zijn verbonden met internet zal extra beveiliging in overweging moeten worden genomen om vertrouwelijke informatie te beschermen.

Bij het overwegen van Fiori moeten de volgende vragen worden gesteld en beantwoord om het autorisatieontwerp- en model te kunnen heroverwegen:

- Zal de Fiori-frontend worden gebruikt als het enige toegangspunt tot de S/4HANA-functionaliteit?

- b. Zullen transactietegels (UI5-tiles) worden gebouwd om toegang te bieden tot transacties waarvoor geen Fiori-app beschikbaar is?
- c. Wordt er nog steeds GUI-toegang verleend aan bepaalde groepen gebruikers?
- d. Is er behoefte om onderscheid te maken tussen rollen voor Fiori en voor GUI?
- e. Welke installatieconfiguratie wordt gebruikt voor Fiori? Embedded of Hub-server?
- f. Welke Fiori-apps worden gebruikt voor welke mobiele apparaten? Deze moeten worden ingesteld als mobiel om beschikbaar te zijn op draagbare apparaten.
- g. Welke infrastructuur is op dit moment binnen Defensie beschikbaar voor mobiele apps en mobiele gegevensencryptie? Kan dit worden gebruikt voor Fiori-apps die beschikbaar zijn voor mobiele apparaten? Gebruik van mobiele infrastructuur zal meegenomen moeten worden in de totale beveiligingsconfiguratie en beheer van S/4HANA.

Bij het uitvoeren van testactiviteiten POC2 (Fiori) zijn zowel het centrale hub model en het embedded model toegepast. Initieel is het centrale hub model gevolgd, waarbij duidelijk werd dat het identificeren en toekennen van de juiste autorisaties voor de front-end server een erg complexe en tijdrovende activiteit is. Tijdens POC2 is de configuratie gewijzigd naar het embedded model. Hierbij is bevestigd dat het toekennen van een gecombineerde rol voor zowel backend als front-end werkt en op efficiënte wijze is toe te passen. Hierbij dient wel opgemerkt te worden dit hiermee het beheerproces wordt bedoeld. Het daadwerkelijk opzetten van de juiste rolinhoud (autorisaties) bleek een lastige aangelegenheid, mede door beperkte beschikbare documentatie en afhankelijkheden tussen verschillende Fiori apps en de beperkte binnen Defensie aanwezige kennis. Om de functionele (IV en BV) testen te kunnen ondersteunen is daarom getest met een ruime toekenning van Fiori apps voor de testgebruikers. Er kan geconcludeerd worden dat het ontwerpen en inrichten van autorisaties met Fiori een complexe activiteit betreft en veel tijd zal vergen.

Hoewel Fiori een nieuw laag- of autorisatieconcept toevoegt is het tevens de toekomstige richting van SAP om toegang te krijgen tot S/4HANA. Daarom moet een nieuw ontwerp in overeenstemming zijn met roadmap en toekomstige inrichting van het SAP landschap, zodat het nieuwe ontwerp in de toekomst kan worden aangepast aan het nieuwe Fiori-concept en aldus de totale herontwerp inspanning kan worden verminderd.

### **Data toegang**

Traditioneel gezien hebben eindgebruikers geen toegang tot databases vanwege de gevoeligheid van gegevens en het gebrek aan inputcontroles die op procesniveau door de SAP-applicatie worden afgedwongen. De HANA-database maakt het echter mogelijk om als data platform te fungeren, waarbij datamodellen in HANA worden gedefinieerd en ontsloten kunnen worden voor eindgebruikers. Een van de aspecten die bij de migratie naar S/4 overwogen dient te worden is op welke wijze gebruik gemaakt wordt van deze mogelijkheden. Dit betreft zowel de ontsluiting voor procesondersteuning als voor rapportagedoeleinden (zoals met SAC). Een van de mogelijkheden is het gebruik van Data Control Language (DCL) met CDS-weergaven (Core Data Services). CDS zijn gebouwd op bestaande databasetabellen en views om een efficiënte manier van gegevensmodellering te bieden. Hiermee kunnen gegevensmodellen worden gemaakt die door andere bronnen kunnen worden gebruikt, bijv. Fiori-apps of API's. Gebruik van deze technieken stelt Defensie ook in staat om toegang tot algehele datatoegang via de applicatie laag te beperken. Huidige toegang verkregen via databrowsers zoals SE16N kan worden vervangen door gebruik van specifieke CDS-views.

Bij het overwegen van het gebruik van DCL- en CDS-weergaven moet rekening worden gehouden met het volgende.

- a. Wat voor soort toegang hebben gebruikers daadwerkelijk benodigd op dataniveau. Is hiervoor toegang nodig tot de DB?

- b. Hoe kunnen CDS-views worden gebruikt om toegang tot relevante informatie te vergemakkelijken zonder toegang tot de database te krijgen?
- c. Wat is het beslissingscriterium om nieuwe CDS views te maken? Omdat zonder een goede reikwijdte en scope controle, Defensie mogelijk kan eindigen met uiteindelijk grote aantallen CDS-views wat resulteert in kostbare operaties en beheerprocessen.
- d. Hoe past DCL in gegevens- en toegangsbescherming?
- e. Welke autorisatiecontroles moeten in de CDS-views worden ingebouwd? Zijn deze hetzelfde als de beperkingen die we in S/4HANA vereisen?
- f. Hoe worden CDS-weergaven verbruikt? Via Fiori, API of andere bronnen als Odata-service?
- g. Hoe past dit in het autorisatiemodel?

Door de beperkt beschikbare tijd voor POC2 is het opzetten en testen van datatoegang in SAP S/4HANA geen onderdeel geweest van de scope van de POC-validatie. Het niet kunnen testen van deze functionaliteit betekent dat de volledige impact op gegevenstoegang niet kan worden bepaald en dat meer voorbereidende werkzaamheden moeten worden uitgevoerd tijdens het migratieproces.

NextLabs is een add-on tool die wordt geïmplementeerd om de toegang tot gevoelige en kritieke gegevens te beheren. Op basis van informatie ontvangen van SAP is de verwachting dat de migratie naar S/4HANA geen grote impact zal hebben op de integratie van NextLabs met SAP. De enige voorziene verandering voor de migratie is de implementatie van een nieuwe DAM plug-in voor S/4HANA, aangezien alle andere functies zouden moeten werken zoals ingericht in de huidige omgeving. NextLabs is geen onderdeel geweest van de POC-omgeving, en daarmee kon bovenstaande niet in het systeem worden gevalideerd. **UI Masking**

Als additionele beveiliging op datatoegang biedt SAP de mogelijkheid om UI Masking toe te passen. Als reactie op de noodzaak van GDPR-regulering heeft SAP een eigen oplossing geboden: SAP UI Masking & Logging-mechanisme dat de bescherming van de integriteit van de gegevens verwerkt in SAP-applicaties verbetert. SAP UI Masking verbergt specifieke gegevens, zoals waarden in velden en kolommen, tenzij die informatie vereist is voor een specifieke taak. Opgemerkt dient te worden dat UI Masking ook zonder S/4HANA mogelijk is. De huidige UI Masking functionaliteit werkt native met S/4HANA en de Fiori userinterface. UI Masking kan een interessante en efficiënte manier zijn om gevoelige gegevens op dataniveau af te schermen van gebruikersgroepen. Aangezien het verkrijgen van (permanente of on-demand) leestoegang wordt beheerd door middel van autorisaties verdient het aanbeveling deze mogelijkheid mee te nemen in de evaluatie en uitwerking van het vernieuwde S/4HANA autorisatieconcept. UI masking kan worden gebruikt voor gegevensbescherming op het SAP-systeem, maar vervangt niet noodzakelijk andere tools zoals NextLabs. De mate waarin UI-maskering wordt gebruikt, is afhankelijk van de eisen en kan worden gebruikt als aanvulling op andere tools. Het voordeel van UI Masking is dat de toegang tot gevoelige gegevens kan worden beheerd binnen het bestaande autorisatieontwerp en configuratie.

Wanneer het gebruik van de masking wordt overwogen, dient met het volgende rekening te worden gehouden.

- a. Zijn er vereisten voor UI-maskering, zoals afscherming gevoelige dataobjecten of GDPR vereisten?
- b. Welke gegevens te maskeren?
- c. Wordt dit reeds afgedekt, en moet dit worden afgedekt, door de huidige tool voor gegevenstoegang NextLabs?
- d. Wie mag de gemaskeerde gegevens zien?
- e. Is de toegang tot gemaskeerde gegevens gebaseerd op rollen of attributen?
- f. Wordt toegang permanent of on-demand verleend?
- g. Welke rollen moeten worden gekoppeld aan vereiste gemaskeerde objecten?

h. Hoe wordt dit opgenomen in het autorisatieconcept en -ontwerp?

Door de beperkt beschikbare tijd voor POC2 is het opzetten en testen van data masking geen onderdeel geweest van de scope van de POC-validatie.

### **UI Logging**

SAP UI Logging kan helpen om alle activiteiten en acties uitgevoerd op de SAP GUI transactieniveau, te loggen en vast te leggen voor de gebruiker. Het registreert elke invoer of actie die door de gebruiker wordt ingevoerd binnen het systeem. Op basis van de geregistreerde gegevens kunnen er Defensie specifieke regels gedefinieerd worden om overtredingen of ongeautoriseerde activiteiten te melden. Daarbij kunnen gebruikers tevens beperkt of gecontroleerd worden door autorisatieobjecten, op basis van transacties, op basis van de rol, het niveau, de organisatie-eenheid of andere parameters. SAP UI Logging kan inzicht bieden bij het bewaken van de toegang van gevoelige transacties door de gebruikers en bij het identificeren van datalekken.

UI Logging en UI Masking kunnen samen worden gebruikt om de toegang tot bepaalde informatie te beperken en ook om te controleren wie deze gegevens daadwerkelijk bekijkt/ wijzigt. Opgemerkt dient te worden dat UI Logging geen specifieke S/4HANA techniek is. Echter is wel aanbevolen in overweging te nemen of UI Logging op effectieve wijze de security beheer en monitoring processen kan ondersteunen als een nieuwe securityopzet wordt gerealiseerd voor S/4HANA.

Door de beperkt beschikbare tijd voor POC 2 is het opzetten en testen van UI Logging geen onderdeel geweest van de scope van de POC-validatie.

#### **3.1.1.3 Aandachtspunten en aanbevelingen**

Om de veranderingen in architectuur en nieuwe beschikbare functionaliteit te kunnen verwerken, moet het volgende worden overwogen en verwerkt in het autorisatie-concept en het rolontwerp. Hierbij dient de doorlooptijd en omvang van de wijzigingen in overweging te worden genomen tijdens de volgende fases van het project.

#### **1. Migratie naar S/4HANA**

Voor het scenario 'hergebruik' is er minimale impact op het autorisatieconcept en ontwerp. De upgrade naar de nieuwste versie op de S/4HANA-infrastructuur heeft invloed op bepaalde transacties en objecten. Transacties en objecten die op dit ogenblik worden gebruikt, kunnen verouderd zijn of er kunnen nieuwe transacties en objecten zijn die binnen de processen moeten worden gebruikt. Deze kunnen tijdens de upgrade en via de regressietestcyclus worden geïdentificeerd en verwerkt. De resultaten uit POC-1 bevestigen dat merendeel van de gebruikte testscenario's geen impact hebben ondervonden.

#### **2. Migratie naar S/4HANA met Fiori**

De migratie naar Fiori heeft een grote impact op het huidige autorisatieconcept en -ontwerp. De introductie van de S/4HANA-oplossing met Fiori voegt nieuwe dimensies toe aan de SAP-omgeving bij Defensie. Het levert ook nieuwe tools en functionaliteit op die kunnen worden gebruikt om de toegang tot systeemfuncties en -bronnen te beheren en te beperken, zoals CDS-views, UI Masking en UI Logging en Fiori-apps. De verandering in processen en functionaliteit met ingebedde SAP-modulen vereist een nieuwe kijk op het huidige autorisatieconcept en ontwerp.

Nieuwe processen moeten in kaart worden gebracht in Aris of in een vergelijkbare tool. Nieuwe/gewijzigde transacties moeten worden toegewezen aan processtappen. De juiste Fiori-app(s)

moeten worden toegewezen aan de processtappen. Deze transacties moeten worden toegewezen aan de juiste functionele (taak) rol en de Fiori-apps moeten worden toegewezen aan catalogi en groepen. Als UI Masking wordt gebruikt, moeten deze vereisten worden toegewezen aan de juiste rol die toegang geeft tot de gemaskerde velden.

Backend- en front-end-rollen moeten vervolgens worden gemaakt volgens de vereisten en nieuw te gebruiken of aangepaste functionaliteiten. Hierbij dient expliciet rekening gehouden te worden met het deployment model van Fiori (embedded of hub) en de noodzaak om autorisaties nodig voor de front-end te laten aansluiten bij de back-end.

Daarbij is naar voren gekomen dat binnen Fiori het mogelijk is om middels de embedded services, en masse apps te genereren. Daarbij dient er door Defensie nagedacht te worden over een naamgevingsstructuur van de apps zoals de apps worden getoond aan de klant. De naam dient de functionaliteit van de betreffende app te omschrijven.

Het verdient aanbeveling om deze aspecten al vanaf het begin als een integraal onderdeel van het project mee te nemen. Derhalve is de doorlooptijd voor al deze wijzigingen naar verwachting lang en de impact op het autorisatieconcept hoog.

### **3. Datatoegang**

Indien bij de migratie naar S/4HANA de database ontsloten zal worden als dataplatform voor bijvoorbeeld S/4 of SAC dan dient ook de HANA-configuratie en gerelateerde processen onderhanden genomen te worden. De HANA-databaseprocessen dienen in kaart worden gebracht in de Modeling-tool om ervoor te zorgen dat toegangsvereisten worden vastgelegd en onderhouden als onderdeel van de algemene autorisatiestrategie. Met behulp van CDS-weergaven kunnen andere services, zoals Fiori of API's, de Odata-service gebruiken. Er moet een duidelijke strategie worden gedefinieerd voor het gebruik van CDS-views en voor welke bronnen deze service wordt gebruikt.

Hierbij is conform punt 2, migratie naar S/4HANA met Fiori, de aanbeveling om het aspect datatoegang vanaf het begin als een integraal onderdeel van het project mee te nemen zodat de gedefinieerde strategie binnen het project verder geïmplementeerd en meegenomen kan worden. Door de beperkt beschikbare tijd voor POC2 is het opzetten en testen van datatoegang in SAP HANA geen onderdeel geweest van de scope van de POC-validatie. Het niet kunnen testen van deze functionaliteit betekent dat de volledige impact op gegevenstoegang niet kan worden bepaald en dat meer voorbereidende werkzaamheden moeten worden uitgevoerd tijdens het migratieproces. NextLabs is geen onderdeel geweest van de POC-omgeving, en daarmee kon bovenstaande niet in het systeem worden gevalideerd.

Vanwege de interconnectiviteits mogelijkheden van S/4HANA en integratie met apparaten die zijn verbonden met internet moet extra beveiliging in overweging worden genomen zoals mobiele gegevensencryptie, antivirusscanners en firewalls om vertrouwelijke gegevens te beschermen. Huidige infrastructuur binnen MOD beschikbaar voor mobiele apps, moet bekeken worden. Gebruik van mobiele infrastructuur zal meegenomen moeten worden in de totale beveiligingsconfiguratie en beheer.

### **4. Vernieuwing autorisatiemodel**

Het huidige autorisatiemodel gehanteerd voor de SAP-omgeving bij Defensie is al langere tijd in gebruik en niet structureel vernieuwd of up-to-date gehouden. Er worden verschillende rollenconcepten door elkaar toegepast wat de complexiteit van beheer vergroot. Gerelateerd aan de significante impact die S/4HANA zal hebben op het autorisatiemodel is het aanbevolen om voorafgaand aan de migratie een nieuw, voor S/4HANA geoptimaliseerd concept te ontwerpen waarin rekening wordt gehouden met ondersteuning van Fiori toegang, de gekozen wijze van data toegang en de benodigde schaalbaarheid

en wendbaarheid om periodieke updates uit te kunnen voeren wanneer nieuwe functionele componenten worden toegevoegd. Het vernieuwde autorisatiemodel dient rekening te houden met:

- 1) Naamgevingsstructuur voor
  - a. Fiori apps
  - b. Fiori catalogi en groepen
  - c. Rolnamen zoals Netweaver, Fiori, S/4HANA backend, Structural authorization (D&S)
  - d. CDS views
- 2) Beperkingsvereisten voor CDS views die moeten worden gecodeerd
- 3) Beperkingsvereisten voor UI masking en datatoegang (NextLabs)
- 4) Gebruikersbeheer proces (b.v. CUA, direct, indirect, GRC, Sailpoint)
- 5) Nieuwe definitie en kader van functiescheiding
- 6) Toegangsprocedures

Het verdient aanbeveling om vanaf de start van het project, indien mogelijk voordat het project start, rekening te houden met de vernieuwingen in het autorisatiemodel. Voordat het project van start gaat dient Defensie al de basis van het autorisatieconcept vast te stellen zodat deze tijdens het project geïmplementeerd kan worden. Derhalve wordt de impact en doorlooptijd van deze aanbeveling op beide aspecten als hoog ingeschat.

## 5. Security by design

Voor een effectieve migratie naar S/4HANA is het van belang dat autorisaties en security als integraal onderdeel wordt meegenomen binnen de project aanpak. Dit betreft het tijdig definiëren van de benodigde maatregelen op basis van de relevante risico's en de te ondersteunen processen. Naar verwachting zal er als onderdeel van de migratie een fit-to-standaard plaatsvinden voor de functionele processen. Het verdient aanbeveling om de gerelateerde autorisaties als integraal onderdeel van deze activiteiten op te nemen. Op deze wijze kunnen de benodigde rollen als integraal onderdeel van de procesgang worden gerealiseerd. Dit zal zorgen voor:

- Duidelijke betrokkenheid en eigenaarschap van de business
- Kosten efficiënte analyse. Het is niet nodig om autorisaties op een later moment toe te voegen aan bijvoorbeeld procesbeschrijvingen. Optimaal gebruik van standaard S/4HANA functionaliteit. Effectieve beheersing direct vanaf migratie

Het verdient hierbij de aanbeveling om net zoals bij punt 4 dit aspect voordat het project start mee te nemen. Denk hierbij aan het bewust maken van de projectleden en medewerkers van Defensie, maar ook om van te voren vast te stellen hoe security al in het ontwerp kan worden meegenomen. Daarbij kan vervolgens security by design worden overwogen tijdens de verschillende stappen en onderdelen van het project.

### 3.1.2 Security- & Beheerprocessen

Om de SAP-omgeving op gecontroleerde manier te beheersen zijn er een aantal specifieke beheerprocessen van toepassing die toezien op het effectief adresseren van risico's ten aanzien van gebruikerstoegang en systeemwijzigingen. De volgende processen zijn meegenomen als onderdeel van het vooronderzoek:

1. Toegangsbeheer, waaronder:
  - Indiensttreding;
  - Doorstroom;
  - Uitdiensttreding.
2. Standaard accounts
3. Authenticatie
4. Gebruikersreview, functiescheidingsreview en security monitoring

## 5. Wijzigingsbeheer

### 3.1.2.1 AS-IS situatie

De beschikbare Defensie procesbeschrijvingen zijn als basis gehanteerd om een duidelijk beeld van de AS-IS situatie te verkrijgen. Daar waar deze documentatie niet volledig beschikbaar of up-to-date bleek te zijn is gebruik gemaakt van algemene good practice procesbeschrijvingen en de praktijkervaring van de RC&C-teamleden.

#### 1. Toegangsbeheer (Indienst-, doorstroom- en uitdienstproces)

Er is op het moment nog geen formele procedure omschrijving beschikbaar waarin de processen en controles zijn beschreven voor de indienst- doorstroom- en uitdienstprocessen. Echter, op basis van een generieke procesomschrijving is de verwachte impact bepaald voor deze drie sub processen.

Indien een gebruiker in dienst komt bij Defensie, dient er een aanvraag te worden gedaan voor een SAP-account. Vervolgens wordt het account aangemaakt op basis van een entry in Peoplesoft. Door middel van een interface tussen Peoplesoft en SAP, wordt er een gebruiker aangemaakt. Deze aanvraag wordt ingediend door een daartoe geautoriseerd persoon, of de aanvraag dient door een geautoriseerd persoon goedgekeurd te worden. Vervolgens dienen de specifieke rollen- en rechten aan dit gebruikersaccount toegekend te worden, het toekennen van deze rollen en rechten gebeurt bij Defensie via de Central User Administration (CUA). Bij het proces voor de huidige SAP-oplossing worden rollen via het zogenoemde indirecte rollenprincipe toegekend aan gebruikers. De gebruiker wordt als deel van het standaard proces toegewezen aan een HR-positie in SAP. Op basis van deze toekenning ontvangt de gebruiker de toegangsrechten die zijn gekoppeld aan deze positie. Daarnaast kunnen ook rollen direct aan individuele gebruikers worden toegekend, bijvoorbeeld voor specialistische- of plaatsvervangende activiteiten.

Zoals aangegeven wordt CUA gebruikt binnen de gebruikersbeheerprocessen van Defensie. Bij de overgang naar S/4HANA zal CUA gebruikt kunnen worden. Dit past bij de eis die vanuit Defensie gesteld wordt dat alle systemen en mandanten vanuit het CUA-systeem beheerd dienen te worden.

Indien een persoon binnen Defensie wijzigt van functie, dient deze aanvraag te worden ingediend door een daartoe geautoriseerd persoon, of de aanvraag dient door een geautoriseerd persoon goedgekeurd te worden. Vervolgens dienen de specifieke rollen- en rechten aan dit gebruikersaccount toegekend te worden, en de rollen van de oude functie dienen verwijderd te worden. Dit loopt via het CUA-systeem. Aangezien een medewerker doorgaans aan één HR-functie is gekoppeld worden de gerelateerde rollen direct aangepast als de medewerker in SAP van posities wordt veranderd. Indien het nodig is de oude rechten (tijdelijk) beschikbaar te laten, wordt dit met directe roltoekenning opgevangen.

Indien een gebruiker uit dienst treedt, dient het account geblokkeerd te worden en de rechten dienen ingetrokken te worden van het account. Hiervoor geldt hetzelfde principe als beschreven onder in dienst treding.

Daarbij wordt er binnen Defensie onderscheid gemaakt tussen verschillende gebruikerstypen:

- **Dialooggebruikers:** deze accounts mogen alleen door personen gebruikt worden en dienen te alle tijden identificeerbaar te zijn. Toegang tot deze accounts geschiedt voor een beperkte tijdsduur. Dialooggebruikers maken gebruik van interfaces en achtergrondprocessen om transacties juist, volledig en efficiënt uit te voeren. Authenticatie geschiedt door middel van gebruikersnaam en wachtwoord. Daarbij zijn er wachtwoord parameter instellingen gedefinieerd en zijn verboden woorden en lettercombinaties die zijn opgenomen in de USR40.
- **Systeemgebruikers:** Systeembeheer taken worden door enkele achtergrondgebruikers uitgevoerd, welke als systeemgebruiker zijn aangemaakt. Hiervoor geldt dat het wachtwoord

een automatisch gegenereerd wachtwoord dient te zijn. Systeembeheer taken van beheerders worden onder deze achtergrondgebruikers gepland. De totale autorisaties van de beheerders bestaan dus uit een optelsom van autorisaties op zijn functies op persoonlijke gebruikersnaam + autorisaties van alle systeemgebruikers waarvan hij/zij de achtergrondtaken mag inplannen.

- Communicatiegebruikers: mogen niet gebruikt worden, indien wel gebruikt dan dient dit afzonderlijk te worden beoordeeld. Op deze gebruikersaccounts kan niet interactief worden ingelogd.
- Servicegebruikers: Dit type is in staat om meerdere keren aan te loggen. Het gebruik van serviceaccounts is niet toegestaan, echter wordt dit gecontroleerd gedoogd door Defensie wanneer dit noodzakelijk wordt geacht.
- Referentie gebruikers: worden gebruikt voor het toekennen van autorisaties aan andere gebruikers. Het gebruik van gebruikerstype referentie is niet toegestaan binnen Defensie.

Daarbij heeft Defensie als uitgangspunt dat dialoog (generieke) groepsaccounts niet zijn toegestaan omdat het gebruik van deze accounts niet herleidbaar zijn tot een natuurlijk persoon. Dit zullen derhalve met name taak gebonden accounts zijn, waarbij het de aanbeveling is om het accounttype te wijzigen naar een type waar niet interactief mee ingelogd kan worden, het zijnde "B" of "C" type accounts.

## 2. Standaard accounts

Dit betreffen accounts die standaard door SAP worden gecreëerd bij de installatie, deze zijn derhalve initieel aanwezig binnen het SAP-landschap. Hiervoor zijn binnen Defensie op dit moment de volgende normen gedefinieerd:

- DDIC: account dient standaard geblokkeerd te zijn, waarbij het standaard wachtwoord gewijzigd dient te zijn. Het account heeft bij activatie SAP\_ALL benodigd, en mag niet verwijderd worden.
- SAP\*: account dient standaard geblokkeerd te zijn, waarbij het standaard wachtwoord gewijzigd dient te zijn. Daarbij heeft het account standaard geen rechten toegewezen. Om te voorkomen dat de installatie gebruiker automatisch opnieuw wordt gecreëerd (wat gebeurt als deze user uit het systeem wordt verwijderd) met het standaard wachtwoord moet de parameter "login/no\_automatic\_user\_sapstar" op 1 worden gezet.
- SAPCPIC: account dient te zijn verwijderd
- TMSADM: account mag alleen bestaan op 000 mandanten. Het account dient op de overige mandanten te zijn verwijderd.

## 3. Authenticatie

Authenticatie gebeurt door middel van Single Sign-On.

Indien er geen gebruik gemaakt wordt van Single Sign-On (waarbij het de aanbeveling is om SSO te implementeren, omdat SSO de voorkeur heeft om te worden gebruikt voor een strenger authenticatiemechanisme), dienen de security parameters geactiveerd te worden. De wachtwoorden worden binnen Defensie verstrekt conform een vast proces waarbij het accounts en wachtwoord apart worden gedeeld met de gebruiker.

## 4. Gebruiker review, functiescheidingsreview en security monitoring

Binnen Defensie wordt er elke maand een controle uitgevoerd op kritieke autorisaties met de CSI-tool. Daarbij wordt er elke drie maanden een SOD-analyse uitgevoerd. Hierbij zijn er drie area's of control gedefinieerd:

1. Beheer
2. FINAD (financieel)
3. MATLOG (materieel/ logistiek)

Eens in de drie maanden wordt een van de bovengenoemde drie gebieden gecontroleerd door middel van het draaien van de CSI-tool. De CSI-tool geeft een download met de betreffende functiescheidingsconflicten. Deze functiescheidingsconflicten dienen op hun beurt weer als input voor de DART-tool. De DART-tool is een custom build tool van Defensie waarbinnen een functiescheidingsconflict wordt naar een rapport en derhalve met name gefocust is op reporting. Met de komst van S/4HANA is het mogelijk dat de objecten, transacties en tabellen wijzigen, ongeacht het migratiescenario. Derhalve dient geanalyseerd te worden of de filter settings aangepast dienen te worden, bijvoorbeeld wanneer tabellen of transacties wijzigen.

Voor Security monitoring bestaat er in de huidige omgeving een interface naar het security monitoring platform. Hiervoor wordt gebruikt gemaakt van diverse logbestanden die door SAP worden bijgehouden, zoals de security audit log.

#### Wijzigingsbeheer

Binnen het wijzigingsbeheerproces kunnen er verschillende soorten processen worden onderscheiden:

- Transport en releasemanagement, waarbij er transporten middels de OTAP-straat naar productie worden gezet;
- Incidentproces, waarbij transporten en wijzigingen buiten het reguliere wijzigingsbeheerproces om naar productie worden gezet. Dit in verband met de urgentie van de wijziging, hetgeen een kortere doorlooptijd vergt;
- Open- en dichtzetten van de mogelijkheid tot het direct toepassen van wijzigingen in het systeem door middel van system- en client change options (SE06 en SCC4).

De security policy van Defensie beschrijft dat alle wijzigingen volgens het change management procedure dienen te worden afgehandeld. Waarbij na goedkeuring, het wijzigingsverzoek in behandeling kan worden genomen. Waarna de start van het change management wordt voortgezet middels het opstellen van een impact analyse met hierin de volgende punten:

- Mate waarin de functionaliteit wordt gewijzigd;
- De mate waarin ontwerpaanpassing gewenst is;
- De mate waarin de technische onderlaag aangepast dient te worden, waarbij er tevens wordt gekeken welke mate er maatwerk is toegepast en in welke mate deze aangepast dient te worden bij de betreffende wijziging;
- Of het voortbrengen van een bestaande, dan wel in gebruik name van een nieuwe functionaliteit betreft;
- De impact van de wijziging.

Tevens schrijft de security policy van Defensie voor dat alle wijzigingen op een gecontroleerde wijze dienen te worden doorgevoerd. Wijzigingen van productiesystemen dienen hierbij te verlopen via het ontwikkel- test en acceptatietraject. Waarbij transporten alleen uitgevoerd mogen worden vanuit de ontwikkelomgeving en waarbij de coördinatie van transporten belegd is bij transport management. Transporten die automatisch door SAP worden vastgelegd (registrerend) dienen te worden getoetst op nalevering van de afgesproken procedures (controleerende functie). Daarbij dient naast de functioneel verantwoordelijke moet ook een technisch verantwoordelijke (beschikkende/ controleerende functie) goedkeuring verlenen om transporten van acceptatie naar productie omgeving te laten uitvoeren.

De voornaamste eis is dat de processen in het traject van ontwikkeling en productie voldoende waarborgen dat:

- Alleen geautoriseerde, integere en verifieerbare wijzigingen worden doorgevoerd;
- Alleen geautoriseerde en verifieerbare overdracht van componenten tussen de verschillende afdelingen mogelijk is;

- Er geen afbreukrisico is en beschikbaarheidsrisico optreedt tijdens de gegevensverwerking.

Het wijzigingsbeheerproces van Defensie dient daarbij de volgende doelen:

- Het bieden van een efficiënte en effectieve ondersteuning aan de voortbrengingsketen met betrekking tot:
  - Het doorvoeren van wijzigingen naar aanleiding van goedgekeurde wijzigingen.
  - Het doorvoeren van goedgekeurde SAP-software patches.
  - Het reduceren van de doorlooptijden tussen ontwikkeling en productie.
- Het creëren van een stabiele en betrouwbare omgeving, om naast de voortbrengingsketen en beheer tevens grootschalige innovaties door te voeren waarbij de voortbrengingsketen zo min mogelijk wordt onderbroken.

### 3.1.2.2 Impact S/4HANA

#### **FIORI-toegang**

De belangrijkste wijziging voor toegangsbeheer is de introductie van de FIORI-user interface. Om gebruikers toegang te verlenen tot de FIORI-apps dienen specifieke FIORI rollen aan de gebruiker toegekend te worden. De impact die dit heeft op toegangsbeheer is afhankelijk van de manier waarop FIORI wordt geïmplementeerd. Dit kan als centrale hub, waarbij er een aparte FIORI-gateway server wordt toegevoegd aan het landschap, of embedded, waarbij de FIORI-server wordt gedraaid op de S/4HANA instance.

Bij de implementatie van S/4HANA en Fiori middels het 'centrale hub' model, dienen de rollen en rechten op twee verschillende servers aangemaakt, beheerd en toegekend te worden aan de gebruiker. Er dient in dit geval een Fiori rol voor de front-end aan de gebruiker toegekend te worden, en daarbij een additionele rol op de back-end. Als de toekenning van deze twee rollen niet goed met elkaar is afgestemd kan het zijn dat de gebruiker wel autorisaties heeft in de back-end om functionaliteit uit te voeren, maar de beschikbare schermen en knoppen niet kan zien en gebruiken in FIORI.

Indien er gebruik wordt gemaakt van het embedded model, is er de mogelijkheid om ervoor te kiezen één gecombineerde rol aan te maken voor zowel het Fiori front-end als het back-end systeem.

Voor zowel indienst, doorstroom als uitdienst betekent dit dat het rollenmodel en de bijbehorende toekenning in het centrale hub model significant complexer wordt. Er is additioneel werk nodig om beide rollen af te stemmen en toe te kennen en er bestaat een vergroot risico dat niet alle oude rechten worden verwijderd bij doorstroom of uit dienst treding. De impact bij het embedded model is beperkt. De rollen zullen wel inhoudelijk aangepast dienen te worden om de FIORI front-end server te ondersteunen, maar er komen geen additionele rollen bij.

Bij het uitvoeren van testactiviteiten POC2 (Fiori) zijn zowel het centrale hub model en het embedded model toegepast. Initieel is het centrale hub model gevolgd, waarbij duidelijk werd dat het identificeren en toekennen van de juiste autorisaties voor de front-end server een erg complexe en tijdrovende activiteit is. Tijdens POC2 is de configuratie gewijzigd naar het embedded model. Hierbij is bevestigd dat het toekennen van een gecombineerde rol voor zowel back-end als front-end werkt en op efficiënte wijze is toe te passen. Hierbij dient wel opgemerkt te worden dat hiermee het beheerproces wordt bedoeld. Het daadwerkelijk opzetten van de juiste rolinhoud (autorisaties) bleek een lastige aangelegenheid, mede door beperkte beschikbare documentatie en afhankelijkheden tussen verschillende FIORI-apps.

#### **Central User Administration**

De Central User Administration (CUA) is niet getest als onderdeel van POC-1 of POC-2, maar zal naar verwachting goed blijven werken gezien er geen wijzigingen zijn aan de onderliggende techniek. SAP heeft bevestigd dat de CUA ook na 2025 ondersteund zal blijven.

### **Processen - Toegangsbeheer**

De generieke uitgangspunten voor gebruikersbeheer zullen niet veranderen met de komst van S/4HANA. Het aanvragen, goedkeuren en toekennen van toegangsrechten gebeurt middels dezelfde procesgang. Het uitgangspunt van de POC is dat eindgebruikers geen directe toegang nodig hebben tot de HANA Database voor bijvoorbeeld analytics. SAP kent diverse (nieuwe) oplossingen om deze processen efficiënter te kunnen uitvoeren zoals SAP Identity Management, GRC Access Control en diverse oplossingen die SAP's cloud based producten ondersteunen. Deze producten zijn echter geen onderdeel van de S/4HANA standaard functionaliteit.

Bij het uitvoeren van testactiviteiten tijdens POC1 (hergebruik) en POC2 (Fiori) zijn er geen bijzonderheden geconstateerd. De gebruikelijke processen en functionaliteit werkt als verwacht, waaronder het aanmaken van gebruikers en het toekennen van rollen via PFCG.

### **Processen – standaard accounts**

Door middel van de overgang naar S/4HANA zullen de standaard accounts niet veranderen. Echter dienen deze accounts wel opnieuw ingesteld te worden, waarbij het standaard wachtwoord van de accounts gewijzigd dienen te worden alsmede de accounts bij default op geblokkeerd dienen te staan. Daarbij dient Defensie een proces in te regelen, dat wanneer de gebruikersaccounts geactiveerd dienen te worden dit volgens een standaardprocedure verloopt middels aanvraag en goedkeuring door geautoriseerde personen. Daarbij dient het account tijdig geblokkeerd te worden na gebruik en dient er een review uitgevoerd te worden op de activiteiten die zijn uitgevoerd door het betreffende account.

### **Processen – authenticatie**

Er zijn geen significante wijzigingen in het authenticatie principe voor S/4HANA.

Indien er geen gebruik gemaakt wordt van Single Sign-On, dienen de security parameters geactiveerd te worden. De wachtwoorden worden binnen Defensie verstrekt conform een vast proces waarbij het accounts en wachtwoord apart worden gedeeld met de gebruiker. Hierbij dient Defensie de huidige configuratie te valideren voor integratie met Fiori.

### **Processen – gebruikersreview en functiescheidingsreview**

Door de komst van S/4HANA zal er een impact zijn op de rulesets die gebruikt worden voor monitoring, zoals de SOD-matrix. Dit komt door de komst van verwijderde, aangepaste en nieuwe transacties, tabellen en SAP-functionaliteiten. De impact van deze wijzigingen op de SOD-matrix dient door Defensie te worden vastgesteld en er dient een nieuwe ruleset opgesteld te worden die alle relevante S/4HANA functies afdekt, inclusief het gebruik van Fiori.

Ten aanzien van security monitoring, zijn er geen significante wijzigingen geïdentificeerd aan de bronnen die worden gebruikt in de SAP-omgeving. Indien wordt gemigreerd naar Fiori dient de security logging uitgebreid te worden met relevante use cases voor de Fiori front-end server.

Tijdens POC-1 (hergebruik) is gevalideerd dat de gebruikte bronnen beschikbaar zijn en werken. Door de beperkt beschikbare tijd voor POC 2 is het opzetten en testen van additionele security monitoring use cases geen onderdeel geweest van de scope van de POC-validatie

### **Processen – wijzigingsbeheer**

Evenals bij toegangsbeheer, is de verwachting dat de generieke uitgangspunten niet zullen veranderen met de komst van S/4HANA. Het transportmechanisme, proces en uitgangspunten zoals gedefinieerd door Defensie en zoals nu wordt toegepast in ECC, zal tevens in S/4HANA toepasbaar zijn. Dit is ook door SAP bevestigd in een validatiesessie.

### 3.1.2.3 Aandachtspunten en aanbevelingen

Op basis van het vooronderzoek zijn de volgende aandachtspunten en aanbevelingen geïdentificeerd.

#### **1. Beheerprocessen**

De impact op de security configuratie is beperkt. In de compatibility scope van SAP (scenario 'hergebruik') zijn er geen significante wijzigingen geïdentificeerd. Het verdient aanbeveling de reguliere validatie toe te passen als bij generieke systeemupdates of conversies.

De processen an sich vereisen geen significante aanpassing om S/4HANA te ondersteunen. Wel is tijdens de analyse gebleken dat de beschikbare documentatie niet volledig en up-to-date is. Het verdient aanbeveling om voor de implementatie van S/4HANA met Fiori, de nieuwe en geoptimaliseerde processen in een vast format te documenteren en helder te communiceren naar de betrokkenen binnen het proces. Hierdoor kan er vanaf de start van ingebruikname van het systeem een uniforme manier van werken worden toegepast en wordt het risico op fouten beperkt.

#### **2. Fiori**

Vanuit het perspectief voor toegangsbeheer verdient het aanbeveling de FIORI front-end server in te richten volgens het embedded model. Dit zal de toekenning en het beheer van rechten efficiënter maken en zal een relatief kleiner risico vormen voor het toekennen van onvoldoende of ongeautoriseerde rechten. Vanuit beheerproces oogpunt dienen de geldende processen uitgebreid te worden naar Fiori. Dit betreft o.a. het toepassen van security monitoring use cases op de front-end server.

### 3.1.3 GRC and tooling

Dit hoofdstuk beschrijft de impact van migratie naar S/4HANA ten aanzien van de tooling gehanteerd ter ondersteuning van autorisaties en security.

#### 3.1.3.1 AS-IS situatie

De huidige tooling voor de Defensie ter ondersteuning van autorisaties en security voor de SAP-omgeving omvat CSI RBM (role build manager) en CSI AA (SoD-analyse). Monitoring van de SAP-omgeving gebeurt op dit moment via DB-scripts. Het verschaffen van toegang aan gebruikers in ECC gebeurt via directe (gebruikers-ID) en indirecte (positie) toewijzing. De rest van de omgeving gebruikt SAP CUA (centraal gebruikersbeheer) voor gebruikersonderhoud.

Op dit moment lopen projecten voor de implementatie van SailPoint voor IAM (Identity and Access Management) en CyberArk voor PAM (Privileged Access Management). Daarbij maakt Defensie op dit moment gebruik van Aris voor het inrichten van controles en processen, en de CSI-tool en de in-huis ontwikkelde DART-tool voor het inrichten en monitoren van functiescheidingsconflicten.

Daarnaast loopt op het moment een traject voor de implementatie van NextLabs. Deze tool zal voor Defensie gebruikt worden om bepaalde data objecten en gevoelige informatie af te schermen door middel van rights management.

#### 3.1.3.2 Impact S/4HANA

Rekening houdend met het bovenstaande en kijkend naar de impact van de nieuwe infrastructuur (paragraaf 3.1.1 en 3.1.4) is het aanbevolen dat een enkele oplossing voor gebruikersonderhoud en toegangsvoorziening moet worden overwogen. Deze oplossing (eventueel in combinatie met UI Logging en UI Masking) zorgt voor een betere beveiliging voor gevoelige toegang en ook voor onderzoek naar ongeautoriseerde activiteiten. Hieronder wordt de impact beschreven van de migratie naar S/4HANA op huidige tools en tools op dit moment binnen Defensie worden geïmplementeerd.

#### **CUA**

Zoals aangegeven wordt CUA gebruikt binnen de gebruikersbeheerprocessen van Defensie. De Central User Administration (CUA) is niet getest als onderdeel van POC1 of POC2, maar zal naar verwachting goed blijven werken gezien er geen wijzigingen zijn aan de onderliggende techniek of tabellen. SAP heeft bevestigd dat de CUA ook na 2025 ondersteund zal blijven. Bij de overgang naar S/4HANA zal CUA gebruikt kunnen worden. Dit past bij de eis die vanuit Defensie gesteld wordt dat alle systemen en mandanten vanuit het CUA-systeem beheerd dienen te worden.

#### **CSI**

Op dit moment wordt binnen Defensie gebruik gemaakt van de CSI tooling om voornamelijk functiescheidingsconflicten in kaart te brengen, te definiëren en te monitoren. Net zoals Aris, is de CSI tooling beschikbaar voor de verschillende soorten gedefinieerde migratiescenario's. Echter dient er wel opnieuw gekeken te worden naar de inhoud van de gedefinieerde functiescheidingsconflicten, zoals aangegeven in onderdeel 3.1.4 is er afhankelijk van het soort deployment model in combinatie met het migratiescenario, een impact op de gedefinieerde SOD's. Indien er wordt gekeken naar migratiescenario 'hergebruik', met hierbij een centraal systeem dan zal de impact beperkt zijn omdat de autorisaties zich maar op één plek bevinden. Echter, bij de introductie van Fiori dient er tweeledig te worden gekeken naar functiescheidingsconflicten. Enerzijds op functiescheidingsconflicten binnen de rollen op de back-end en daarnaast naar toegang via de Fiori front-end. SoD-ruleset moet ook worden bijgewerkt met de nieuwe functionaliteit, transacties, apps en objecten.

Het onderliggende datamodel voor het uitvoeren van de analyses blijft het vrijwel onveranderd. Tabellen en transacties voor gebruikers- en rolonderhoud blijven hetzelfde waardoor het waarschijnlijk wordt geacht dat de CSI-analyses zonder grote problemen zullen blijven werken op S/4HANA. Rolonderhoud dient echter op de juiste manier te worden geconfigureerd voor de aanpak die wordt gevolgd bij het instellen van de Fiori-server b.v. Hub versus ingebouwd server.

### **NextLabs**

Op basis van informatie ontvangen van SAP is de verwachting dat de migratie naar S/4HANA geen grote impact zal hebben op de integratie van NextLabs met SAP. De enige voorziene verandering voor de migratie is de implementatie van een nieuwe DAM plug-in voor S/4HANA, aangezien alle andere functies zouden moeten werken zoals ingericht in de huidige omgeving. Daarnaast geeft SAP aan dat licenties voor NextLabs mogelijk worden gewijzigd in geavanceerde licenties, maar dit zal ook het geval zijn voor de huidige ECC-omgeving. Deze licentiewijzigingen worden op dit moment besproken tussen Defensie en NextLabs en is niet specifiek gerelateerd aan de migratie naar S/4HANA. NextLabs is geen onderdeel geweest van de POC-omgeving, en daarmee kon bovenstaande helaas niet in het systeem worden gevalideerd.

### **SailPoint**

SailPoint is een IAM-oplossing die de integratie en onboarding van applicaties mogelijk maakt op één centraal identiteits- en toegangsplatform. Op deze manier kunnen alle gebruikers/ apparaten/ API's en bots worden beheerd en hebben ze toegang voor deze applicaties. SailPoint heeft standaard connectoren voor SAP S/4HANA en SAP HANA en deze applicaties kunnen worden ingebouwd op het IAM-platform. Daarnaast heeft SailPoint een specifieke module voor SAP GRC-integratie om SoD-analyse op laag niveau (object- en veldniveau) en SAP-systemen mogelijk te maken. Tijdens de migratie van S/4HANA moet worden overwogen of deze toepassing in de toekomst op SailPoint wordt ingebouwd, omdat dit de instelling en installatie van de S/4HANA-omgeving kan beïnvloeden met betrekking tot configuratie, plug-ins en datastromen. De roldefinitie binnen de S/4HANA-omgeving kan ook van invloed zijn op de algehele businessrol die binnen de SailPoint-omgeving wordt gebruikt. Het verdient daarom aanbeveling om tijdens de migratie naar S/4HANA integraal te kijken in welke mate de omgeving kan worden ondersteund door SailPoint om latere aanpassingen en daarmee onnodige extra kosten te besparen.

### **CyberArk**

CyberArk wordt gebruikt voor het beheren en toestaan van toegang tot verhoogde rechten accounts in applicaties. Verhoogde rechten accounts hebben kritische- en brede toegangsrechten toegewezen. CyberArk zorgt ervoor dat toegang alleen wordt toegestaan tot deze gevoelige accounts onder bepaalde voorwaarden en dat deze gebruikerssessies op de juiste manier worden beheerd en toegekend. SAP S/4HANA kan worden opgenomen in de CyberArk-scope om standaard verhoogde rechten accounts zoals SAP\* en DDIC en SAP HANA DB-accounts te beheren. Als de toekomst is om deze applicaties te integreren met CyberArk, dan moet deze integratie verder te worden onderzocht. Dit omdat voor deze integratie mogelijk extra configuratie en instellingen nodig zijn en deze instellingen kunnen worden gedaan tijdens de eerste fasen van de SAP S/4HANA-migratie. Om op deze manier te voorkomen dat er configuratie wijzigingen uitgevoerd dienen te worden in een later stadium. Als de configuratie en instellingen later gewijzigd moeten worden, kan dit van invloed zijn op de functionaliteit- en werking van de systemen die al zijn geconfigureerd en eerder zijn getest. CyberArk kan daarbij ook worden gekoppeld aan SailPoint om één ecosysteem voor gebruikers- en rechtenbeheer te creëren.

#### **3.1.3.3 Aandachtspunten en aanbevelingen**

##### **1. Huidige tooling**

Op basis van de informatie verkregen tijdens het vooronderzoek lijkt de impact op de huidige tooling beperkt. Het datamodel in S/4HANA wijzigt niet significant voor de dataobjecten die relevant zijn voor autorisaties en security. Daarmee wordt verwacht dat CUA, CSI en NextLabs zullen blijven werken op de S/4HANA omgeving. Wel zullen inhoudelijke aspecten zoals functiescheidingsregels vernieuwd moeten worden om eventuele aanpassingen in processen en de toevoeging van Fiori te kunnen ondersteunen.

## **2. Future proof tooling strategie**

Het verdient aanbeveling om naast de analyse van wijzigingen in toegangsrechten, configuratie en beheerprocessen (zie 3.1.1 en 3.1.2) ook te kijken naar het totaal aan tooling dat deze aspecten op efficiënte en effectieve wijze kan ondersteunen. Er dient daarbij rekening gehouden te worden met de IT-beveiliging en toegangsvereisten, gegevenstoegang en -bescherming, ITGC en applicatiecontroles, monitoring en de roadmap van de Defensie-infrastructuur. Daarbij verdient het aanbeveling om dit op holistisch niveau uit te voeren, om overlap tussen toolfunctionaliteit of ongeadresseerde aspecten te voorkomen.

Nadat de strategie is gedefinieerd, dient Defensie deze vereisten te spiegelen aan de huidige tools die in de omgeving worden gebruikt en geïmplementeerd, evenals aan overige beschikbare tools die momenteel geen deel uitmaken van de geïmplementeerde toolset om te bepalen of aan alle vereisten kan worden voldaan op een manier die aansluit bij de gekozen strategie. Dit zal ervoor zorgen dat Defensie alle aanvragen kan uitvoeren en ook kan omgaan met de toekomstige roadmap. S/4HANA brengt een wijziging in het SAP-landschap, maar is niet de enige applicatie die toegang tot gegevens en informatie mogelijk maakt. Beheer van toegang en controles binnen de S/4HANA-omgeving biedt Defensie de mogelijkheid om een standaard GRC-ecosysteem te definiëren dat potentieel kan worden gebruikt voor de bredere Defensie IT-omgeving, en dat ook schaalbaar is voor de toekomst.

Het verdient aanbeveling om voor de start te kijken naar de functionaliteiten- en aspecten die Defensie in de toekomst benodigd acht. Als onderdeel van het architectuur ontwerp dient kan er al een tooling-keuze gemaakt worden. Op deze manier kan de (nieuwe) tooling op een geïntegreerde wijze met S/4HANA geïmplementeerd worden. Hierdoor kan worden voorkomen dat na implementatie van S/4HANA er een nieuw project- en implementatieplan moet worden omgesteld om de betreffende tooling te implementeren, met bijkomende additionele kosten. Tevens kunnen er al tijdens het project testwerkzaamheden worden uitgevoerd om werking tussen het S/4HANA systeem en de tooling te toetsen en op elkaar af te stemmen.

### **3.2 Interne beheersing**

Om de bedrijfsvoering op een efficiënte wijze uit te voeren en om te borgen dat wordt voldaan aan geldende wet- en regelgeving zijn interne beheersingsmaatregelen ingericht gericht op zowel proces als IT-aspecten. Dit betreft een combinatie van maatregelen die ertoe dienen om procesfouten tijdig te identificeren of te voorkomen, om de mogelijkheden tot het plegen van fraude te beperken en om de juistheid van (financiële) verslaglegging te borgen. Ook tijdens- en na de migratie naar S/4HANA is het noodzakelijk relevante risico's te adresseren door passende maatregelen toe te passen. Waar mogelijk kan hierbij gebruik gemaakt worden van (standaard) systeemfunctionaliteiten om zo maatregelen te automatiseren en daarmee zowel de effectiviteit te vergroten als de last op de bedrijfsvoering te verlagen. Door de introductie van nieuwe technologieën en de aanpassing op de huidige SAP-functionaliteit dient onderzocht te worden in welke mate controles nog steeds werken en of aanpassingen nodig, dan wel gewenst zijn. Bovendien kan met de introductie van S/4HANA op termijn gebruik gemaakt gaan worden van nieuwe technieken zoals machine learning en robotics (RPA) om het uitvoeren en monitoren van de ic-maatregelen verder te optimaliseren.

Het is de wens van Defensie om met het vernieuwde SAP-landschap sneller en betere stuur- en procesinformatie te kunnen delen. Om deze informatie van de juiste kwaliteit te kunnen laten zijn, is de effectieve werking van interne beheersing rand voorwaardelijk.

In de huidige situatie is het ontwerp van maatregelen die door SAP M&F worden ondersteund vastgelegd in Business Control Diagrams (BCD's). Deze BCD's zijn in Aris gemodelleerd. Daarnaast zijn IT general controls (ITGC's) ontworpen om de specifieke IT-risico's die impact kunnen hebben op financiële data en systemen gedefinieerd en vastgelegd in Excel sheets. Deze maatregelen worden beschouwd als de norm voor de systeeminrichting van SAP en daarmee ook S/4HANA.

Het is van belang om de mogelijke impact van de verschillende migratie scenario's mee te nemen in het vooronderzoek voor S/4HANA. De bedrijfsvoering en de ADR/ARK steunen immers op de blijvende effectieve werking van deze maatregelen. In dit hoofdstuk wordt daarbij specifiek ingegaan op de controles die mogelijk beïnvloed worden door de invoering van S/4HANA. Dit betreft met name applicatiecontroles (controles die gebruik maken van systeemfunctionaliteit om een procesrisico af te dekken) en generieke IT-controles. De impact op handmatige controles, zoals het reviewen van bepaalde balansposten, is buiten beschouwing gelaten.

#### **3.2.1 Applicatiecontroles**

##### **3.2.1.1 AS-IS situatie**

Om een goed beeld van de AS-IS situatie te krijgen is het interne controle raamwerk op hoofdlijnen bekeken. Binnen het interne controle raamwerk zijn de controles in opzet uitgewerkt. Met andere woorden, hoe ze ingeregeld zouden moeten zijn. Er wordt door Defensie geen consistente periodieke controles uitgevoerd om vast te stellen dat de controles die omschreven zijn in het interne controle raamwerk ook daadwerkelijk op effectieve wijze zijn ingeregeld en of deze ook op een juiste manier functioneren.

Op basis van het interne controle raamwerk kan worden vastgesteld dat er verschillende soorten processen worden onderscheiden:

- Bedrijfsprocessen: onder deze processen vallen onder andere Finad, hetgeen de financiële administratieprocessen omvat, en Matlog, hetgeen de materieel logistieke processen omvat. Het ontwerp van de betreffende risico's en maatregelen hiervoor zijn opgenomen in Aris in de zogenoemde Business Control Diagrams (BCD's). Deze BCD's richten zich met name op de Application Controls en de Autorisatie Controls. Onder de laatstgenoemde vallen onder andere

functiescheidingsconflicten en toegang tot het uitvoeren van kritieke transacties. Onder deze bedrijfsprocessen zijn tevens enkele User Controls voor Finad beschreven.

- IT-processen: onder deze processen vallen onder andere het wijzigingsbeheer, incident management en gebruikersbeheer. Hiervan staat het ontwerp van deze maatregelen in Toetsingskaders.

Zoals hierboven aangegeven, zijn er verschillende soorten controles en maatregelen ingericht binnen het interne controle raamwerk van Defensie. Op basis van een nadere analyse van het interne controle raamwerk is er geconstateerd dat er in totaal 65 detectieve maatregelen zijn opgenomen in het interne controle raamwerk, 911 preventieve maatregelen en voor 32 maatregelen is dit (nog) niet gedefinieerd.

Naast bovengenoemd onderscheid, wordt er tevens onderscheid gemaakt in maatregelsoorten:

- Application Controls: 409 controles gedefinieerd
- Autorisatie Controls: 445 controles gedefinieerd
- Functiescheiding Controls: 83 controles gedefinieerd. Echter is geconstateerd dat er 10 van de 83 geen goed ingevulde identifier hebben
- User Controls: 69 controles gedefinieerd
- Geen classificatie: 2 controles
- **Totaal: 1.008 controles**

De verschillende maatregelen zijn vervolgens weer onderverdeeld onder verschillende processen:

| Proces                                                                               | Opmerking                                                                         | # maatregelen |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------|
| P.0 Beheersystemen                                                                   | IT-operations zoals interface monitoring en mutaties op business-data door M&F IT | 24            |
| P.1 Projectmatig Werken, Verwerven en Afstoten                                       | MM, SD, PS                                                                        | 149           |
| P.2 Bevoorraden en Administratief Materiaalbeheer + EHS Bev en Admin Materieelbeheer | MM                                                                                | 345           |
| P.3 Financiën                                                                        | FI, CO, PSM, IP                                                                   | 260           |
| P.4 Onderhouden & Wapensysteemmanagement                                             | PM                                                                                | 230           |
| P.5 Transporteren                                                                    | TM                                                                                | 37            |
| P.6 Inzetten militaire capaciteit                                                    |                                                                                   | 0             |
| P.7 Beheren IV-ICT                                                                   | Overlapt met P.0                                                                  | 83            |
| <b>Totaal</b>                                                                        |                                                                                   | <b>1.083</b>  |

Het eerdergenoemde aantal van 1.008 sluit niet aan met de hierboven genoemde 1.083 vanwege een timingsverschil bij het draaien van de rapportages.

### 3.2.1.2 Impact S/4HANA

De impact van de SAP S/4HANA modules op het interne controle raamwerk is in grote mate afhankelijk van de mate waarin de SAP Modules wijzigen in het nieuwe systeem. Bij een migratie naar S/4HANA is het benodigd om een aantal SAP-modules en systemen te vervangen. Daarnaast brengt S/4HANA nieuwe functionaliteit met zich mee. Dit betreft onder andere DF-PS/D&S, FMS, Universal Ledger, Business Partners, House Banks, Foreign Trade, TM, MDG, eWM en de introductie van Fiori apps. Voor meer specificaties omtrent de impact van SAP S/4HANA op de huidige modules die worden gebruikt binnen het MOD, zie hiervoor het deelproduct DED D.09 Beheer & Architectuur inventarisatie (Huidig). De impact op de (mogelijke) migratiescenario's is beschreven in het deelproduct DED D.15 "Finaliseren beheer & Architectuur (Toekomstig)".

Hierbij dient tevens gekeken te worden naar de standaard SAP-functionaliteiten, waarbij geanalyseerd dient te worden of de geïdentificeerde controles, welke maatwerk bevatten, omgezet kunnen worden naar maatregelen die uitgaan van standaard SAP-functionaliteit. Deze gewijzigde SAP-modules en systemen resulteren in nieuwe en gewijzigde processen en functionaliteiten waar het interne controle raamwerk op moet worden aangepast. Het gaat hierbij zowel om een nieuwe risicoanalyse als een gewijzigde opzet en inrichting van maatregelen in S/4HANA. In het kader van het interne controle raamwerk is het van belang dat indien de modules wijzigen, deze wijzigingen opgenomen dienen te worden in de controle omschrijvingen en dat de controle omschrijvingen in opzet aangepast dienen te worden op basis van de nieuwe functionaliteiten en eventueel aangepast processen. Hierbij dient tevens gekeken te worden naar de standaard SAP-functionaliteiten, waarbij geanalyseerd dient te worden of de geïdentificeerde controles, welke maatwerk bevatten, omgezet kunnen worden naar maatregelen die uitgaan van standaard SAP-functionaliteit.

Gezien het hoge aantal maatregelen die zijn opgenomen binnen het huidige interne controle raamwerk, is er een eerste selectie gemaakt op basis van het risico dat met de control gepaard gaat. Op basis van de risicodefinitie 'hoog' is een eerste selectie gemaakt van de meest kritieke controles. Binnen verschillende afdelingen is de lijst met interne controles neergelegd door de AO/IC deskundigen van M&F, en is gevraagd de vijf voor de afdeling meest relevante controles te selecteren om tot een representatief beeld te komen.

Voor het vooronderzoek is er input ontvangen van de afdelingen PVA FIN, BEVO en WSM. Door elk van deze afdeling zijn de vijf meest kritieke controles gedefinieerd. Dit betreffen allen Application Controls. Op basis van de omschrijving van de verschillende controles in het interne controle raamwerk, zijn de betreffende controles eerst in de bestaande SAP ECC omgeving uitgevoerd. Vervolgens zijn dezelfde controles uitgevoerd in het geconverteerde POC-systeem van Defensie om zo de impact vast te kunnen stellen bij migratie naar S/4HANA. Bij alle aangeleverde maatregelen hebben we het bestaan in SAP ECC omgeving en de POC-omgeving gevalideerd.

## **PVA FIN**

In het kader van de geautomatiseerde controles is bij het PVA-FIN-team de vraag neergelegd welke interne controles zij het meest relevant achten in de voor hen relevante processen. Op basis van deze vraag zijn er een vijftal relevante applicatie controles naar voren gekomen. De omschrijving van deze applicatie controles zijn op basis van het interne controle raamwerk van Defensie gevalideerd. De validatie vond plaats op basis van de omschrijving in het interne controle raamwerk op het SAP ECC systeem en het S/4HANA POC-systeem.

De volgende controles zijn gevalideerd:

1. Blokkeerredenen verkoopfactuur
2. FI-boekingsperiodes
3. Betalingsblokkering factuur
4. Controle dubbele leveranciers
5. Vier-ogen principe voor crediteurstamdata

Op basis van de uitgevoerde validatiewerkzaamheden op zowel de SAP ECC omgeving als de POC-1 (hergebruik) omgeving, zijn onderstaande uitkomsten naar voren gekomen:

- Blokkeerredenen verkoopfactuur
  - Vastgesteld dat de inrichting binnen de POC-omgeving nog conform de SAP ECC omgeving is. De transactiecodes (OVR2 en OVV3) die gebruikt worden binnen de control, zijn reeds beschikbaar in de POC-omgeving. Echter is voor tabel TVFK vastgesteld dat factuurdokumentsoorten CFB3 en CFG2 zijn toegevoegd. Additioneel is voor tabel TVFK vastgesteld, dat de creditzijde niet meer aanwezig is. Hiervoor is een eerste risico

inschatting gemaakt, waarbij wordt verwacht dat de impact beperkt is gezien de creditzijde op de SAP ECC omgeving niet gevuld is en derhalve wordt geacht dat deze in de huidige situatie ook niet wordt gebruikt. **De maatregel zal hierdoor blijven werken.**

- FI-boekingsperiodes
  - Hierbij is vastgesteld dat de bevoegdheidsgroep in transactie OB52 is gewijzigd van bevoegdheidsgroep 0005 naar bevoegdheidsgroep 0004. Dit kan potentieel van impact zijn, omdat er binnen Defensie wordt geautoriseerd op bevoegdheidsgroepen binnen rollen op bijvoorbeeld object F\_BKPF\_BUP. Afhankelijk van de autorisatieopzet kan dit betekenen dat gebruikers niet meer aan de juiste bevoegdheidsgroep zijn gekoppeld na de conversie. Dit betekent dat dan wel de bevoegdheidsgroepen, dan wel de autorisaties aangepast dienen te worden.
- Betalingsblokkering factuur
  - Voor deze controle is vastgesteld dat er handmatige, customized, regels voor betalingsblokkades zijn ingericht waarbij er transacties worden gespecificeerd in de customization. Derhalve kan er worden geconcludeerd dat er een risico ligt dat enerzijds transacties die worden gebruikt in de Applicatie Controls niet meer beschikbaar zijn in S/4HANA. Anderzijds dat er in de customizing van de Application Controls, transacties worden gebruikt die in S/4HANA niet meer beschikbaar zijn. Waarbij er tevens gelet dient te worden of de custom (Z-transacties) en validatie regels juist en volledig worden overgezet naar het SAP S/4HANA systeem, en de werking van de controles niet wordt beïnvloed. Derhalve is het in de toekomstige migratie raadzaam om, in gelijksoortige gevallen waarbij transacties zijn gespecificeerd in ABAP scriptin, te controleren of er sprake is van vervallen transacties zodat de betreffende maatregel daarop kan worden aangepast.
- Controle dubbele leveranciers
  - Voor de Application Control is naar voren gekomen dat het Kamer van Koophandel nummer (KvK-vestigingsnummer ) niet bestaat in standaard SAP.. Hiervoor is een modificatie toegepast door Defensie, door het veld STCD4 (belastingnummer 4) aan te passen naar het KvK-vestigingsnummer. Op basis van een vergelijking met de SAP ECC omgeving en de POC-omgeving is naar voren gekomen dat deze customizing omgezet wordt naar standaard SAP, waardoor deze configuratie verloren gaat. Hierdoor kan ontstaan dat een ingebruiker de omschrijving van het betreffende veld niet meer zal herkennen als zijnde het vestigingsnummer waardoor de maatregel niet meer zal werken. Daarnaast wordt de daadwerkelijke controle op dubbele leveranciers, gebaseerd op dubbele vestigingsnummers, uitgevoerd in een maatwerk-functiebouwsteen waarbij wordt geselecteerd op transacties die zijn vervallen in S/4HANA (o.a. FK02). Hierdoor werkt de maatregel niet meer op de POC-omgeving. Deze maatwerk-functiebouwsteen dient te worden aangepast op het gebruik van Business Partners.
- Vier-ogen principe voor crediteurstamdata
  - Op basis van een vergelijking tussen de SAP ECC en de POC-omgeving is naar voren komen dat dat er geen wijzigingen zijn tussen beide omgevingen voor de betreffende tabel (T055F).

## BEVO

In het kader van de geautomatiseerde controles, is bij het BEVO-team de vraag neergelegd welke interne controles zij het meest relevant achten in de voor hen relevante processen. Op basis van deze vraag zijn er een vijftal relevante applicatie controles naar voren gekomen. De omschrijving van deze applicatie controles zijn op basis van het interne controle raamwerk van Defensie gevalideerd. De validatie vond plaats op basis van de omschrijving in het interne controle raamwerk op het SAP ECC systeem en het POC-systeem.

Hiervoor zijn de volgende controles gevalideerd:

1. Aansturing overboeking definiëren

2. Inrichten aansturing rekeningen
3. Inrichten bewegingssoorten
4. Inrichten interne nummerreeksen ten behoeve van basisgegevens artikel
5. Inrichten selectieklassen

Op basis van de uitgevoerde validatiewerkzaamheden op zowel de SAP ECC omgeving als de POC-1 (hergebruik) omgeving, zijn onderstaande uitkomsten naar voren gekomen:

1. Aansturing overboeking definiëren
  - Dit betreft een geautomatiseerde controle binnen SAP voor het definiëren van de aansturing van de overboeking. Deze vindt plaats op basis van bewegingssoort. Hiervoor is vastgesteld dat de werking binnen de SAP ECC omgeving en de POC-omgeving op eenzelfde wijze verloopt, waarbij kan worden geconcludeerd dat de werking en de gebruikte transacties in S/4HANA niet gewijzigd zijn ten opzichte van de SAP ECC omgeving.
2. Inrichten aansturing rekeningen
3. Voor deze controle is vastgesteld dat de inrichting van de juiste bewegingssoorten en daarmee direct de aansturing tussen de FI-rekeningen en indirect de aansturing tussen de juiste FM en CO-elementen juist dient te geschieden. Daarbij wordt tevens in de materiaal master aangegeven per item bij welke materiaal type en valuation class dit hoort. Hiervoor is tevens vastgesteld dat het rekening klasse-referentie overzicht in vergelijking met de SAP ECC omgeving niet is gewijzigd in de POC-omgeving. Echter, is voor het rekeningsklasse-referente/artikelsoort weergeven overzicht vastgesteld dat er twee rekening klasse/referentie/artikelsoort zijn toegevoegd. Inrichten bewegingssoorten
  - Deze controle ziet toe dat de bewegingssoorten zijn ingericht conform het procesdocument dat beschikbaar is op de SharePoint omgeving, hierin is per rol de toegestane bewegingssoort aangegeven. Voor deze controle is vastgesteld dat de transactie die wordt gebruikt, transactie OMJJ, beschikbaar is in de POC-omgeving. Derhalve kan worden geconcludeerd dat er geen wijzigingen zijn in de werking van de applicatie control.
4. Inrichten interne nummerreeksen ten behoeve van basisgegevens artikel
  - Hierbij is het van belang dat in het geval van een interne nummering, door SAP afgedwongen dient te worden dat er geen handmatige invoer kan worden gedaan. Hiervoor hebben de testwerkzaamheden zich voornamelijk gericht op het toetsen van SAP M&F en niet voor MDG. Hiervoor is vastgesteld dat transactie MMNR en nummerreeks 01 beschikbaar is op de POC-omgeving, maar dat in de SAP ECC omgeving de nummerstatus 0 betreft en binnen de SAP S/4HANA omgeving de nummerstatus oploopt. Echter, is in dit geval de impact beperkt omdat er binnen Defensie in principe gebruik wordt gemaakt in de relevante artikelstam 03 (Z0 Defensie Internal numbering), hetgeen juist oploopt. Tevens is vastgesteld dat alle genoemde artikelsoorten aan de juiste nummerreeksen zijn gekoppeld.
5. Inrichten selectieklassen
  - Selectieklassen bepalen de keuze die gemaakt kan worden bij het aanleggen van een charge zoekstrategie, middels deze optie is specifiek de sorteervolgorde te definiëren. Voor deze applicatie control is vastgesteld dat de betreffende configuratie in ECC gelijk is aan die van de POC omgeving, en dat derelevante transactie, transactie CU72, beschikbaar is in zowel de SAP ECC als de POC-omgeving.

## WSM

In het kader van de geautomatiseerde controles is ook bij het WSM-team de vraag neergelegd welke interne controles zij het meest relevant achten in de voor hen relevante processen. Op basis van deze vraag zijn er een zevental relevante applicatie controles naar voren gekomen. Wederom is de

omschrijving van deze applicatie controles zijn op basis van het interne controle raamwerk van Defensie gevalideerd. De validatie vond plaats op basis van de omschrijving in het interne controle raamwerk op het SAP ECC systeem en het POC-systeem.

Hiervoor zijn de volgende controles gevalideerd:

1. Gebruikersstatus – in opdracht geven reparatie
2. Nummerreeks meldingen
3. Veld 'Toestand Systeem'
4. Verplichte velden suborder bij hoofddorder
5. Zetten technische status verplicht
6. Gebruikersstatus ILS-maatregel
7. ABAC NextLabs Munitie maatregel ECC

Op basis van de uitgevoerde validatiewerkzaamheden op zowel de SAP ECC omgeving als de POC-1 (hergebruik) omgeving, zijn onderstaande uitkomsten naar voren gekomen:

1. Gebruikersstatus – in opdracht geven reparatie
  - Deze maatregel ziet toe dat alleen artikelmanagers reparatieorders mogen geven door het gebruik van de betreffende status. Voor deze controle is vastgesteld dat het bevoegdheidscode overzicht IOG via transactie BS52 en OIBS niet is gewijzigd en tevens de gebruikersstatus niet is gewijzigd.
2. Nummerreeks meldingen
  - In het geval van een interne nummering dient door SAP afgedwongen te worden dat er geen handmatige invoer kan worden gedaan. Deze control ziet middels transactie IW20 toe, dat nummerreeksen worden toegepast. Voor deze controle is vastgesteld dat de transactie tevens beschikbaar is in de POC-omgeving en dat deze transactie en de configuratie niet is gewijzigd.
3. Veld 'toestand Systeem'
  - Deze maatregel regelt dat het veld 'Toestand Systeem' altijd gelijk is aan 2. Op basis van de testwerkzaamheden is naar voren gekomen, dat er tevens de mogelijkheid bestaat dat er waarde 1 of 3 wordt ingevuld, en SAP vervolgens blijft functioneren. Voor deze controle is daarbij vastgesteld dat er binnen de huidige SAP ECC omgeving gebruik wordt gemaakt van maatwerk binnen de tabellen. Het blijkt dat de maatwerk tabellen niet juist en volledig worden overgenomen in de SAP S/4HANA omgeving, waarbij zowel in het Nederlands als in het Engels de omschrijvingen en de betekenissen verschillend zijn.
4. Verplichte velden suborder bij hoofddorder
  - Binnen deze control worden de transacties OIAZ, OIPOD en OICMPD gebruikt. Hiervoor is vastgesteld dat in de SAP S/4HANA omgeving er opties binnen de transacties bij zijn gekomen zoals SLASH1 en SLASH2. De verwachte impact van deze toevoeging is beperkt, vanwege het feit dat Defensie hier op dit moment geen gebruik van maakt. De configuratie ten aanzien van de verplichte is gelijk in beide omgevingen. Het is daarbij vastgesteld dat de maatregel niet conform beschrijving werkt in het systeem.
5. Zetten technische status verplicht
  - Voor deze geautomatiseerde controle is vastgesteld dat er maatwerk binnen de control wordt toegepast. In de overgang van SAP ECC naar SAP S/4HANA is de conversie van het maatwerk juist verlopen, waarbij is vastgesteld dat het maatwerk tussen de SAP ECC omgeving en de SAP S/4HANA omgeving overeenkomt. Additioneel is voor deze transacties geanalyseerd of deze naar voren komen op de SAP simplificatie list, hetgeen impliceert dat deze transacties niet meer beschikbaar zijn in SAP S/4HANA. Het is vastgesteld dat deze transacties niet naar voren komen op de simplificatie list. Het is daarbij vastgesteld dat de maatregel niet conform beschrijving werkt in het systeem.
  - Het is daarbij opmerkelijk dat deze maatregel is geïmplementeerd als 'waarschuwing', die kan worden genegeerd, en niet zoals het ontwerp van de maatregel die aangeeft als

'error'. De maatregelen functioneert derhalve niet zoals ontworpen. Het verdient derhalve de aanbeveling om dit te corrigeren.

6. Gebruikersstatus ILS Maatregel

- Deze maatregel betreft Gebruiker statussen in het onderhoudsproces. Hierbij is vastgesteld dat de betreffende configuratie ten aanzien van verplichte velden in ECC-gelijk is aan die van de POC-omgeving en derhalve de conversie naar het POC systeem is geslaagd. Het is daarbij vastgesteld dat de maatregel niet conform beschrijving werkt in het systeem.

7. ABAC NextLabs Munitie maatregel ECC

- Deze maatregel betreft 138 transactiecodes waarbij NextLabs actief is voor het beveiligen van munitiedata. Omdat NextLabs, inclusief deze maatregel, nog niet is geïmplementeerd kan de configuratie nog niet worden onderzocht. Op basis van een steekproef hebben wij twee transactiecodes van deze geïdentificeerd die relevant zijn voor NextLabs, maar in S/4 zijn vervallen. De maatregel dient op dit punt te worden aangepast. Het verdient aanbeveling om vervallen transactiecodes op dit punt te onderzoeken.

### 3.2.1.3 Impact S/4HANA met FIORI

Naast het toetsen van de werking van de applicatie controles in SAP ECC en de vergelijking van de werking van de applicatie controles in de SAP S/4 HANA POC-1 (hergebruik) omgeving, is een volgende stap het toetsen van de werking van de applicatie controles in Fiori Apps. De verwachting is dat de Fiori apps van invloed kunnen zijn op de werking van de applicatie controles, omdat autorisaties en toegangsrechten mede bedield zijn aan gebruikers via apps alsmede via transacties.

Hierbij zijn tijdens het testen de volgende drie soorten Fiori apps naar voren gekomen:

1. Native SAPUI5/ HTML5 Fiori apps

Dit zijn de meest innovatieve vorm van Fiori apps waarbij gebruik gemaakt wordt van BADI's en OData koppelingen.

2. Fiori apps gebaseerd op Dynpro

Dit betreffen tegels die gebruik maken van Dynpro's op S/4HANA en kan worden gezien als tussenvorm van het omzetten van transacties naar Fiori apps.

3. Vertegelde transacties

Hierbij vormt de Fiori app een link naar de WebUI waarin de ECC-transactie wordt gebruikt. Hierbij wordt gebruik gemaakt van de reguliere transacties.

## PVA FIN

Voor de 5 PVA FIN geselecteerde controles hebben wij op 18.11.2019 testwerkzaamheden uitgevoerd op de impact van de Fiori apps op de applicatie controles. Hiervoor is vastgesteld dat er een invloed is van de verplichte velden op de Fiori apps. Hierbij is naar voren gekomen dat de verplichte velden die vanuit de configuratie zijn ingeregeld (transactie SPRO), tevens verplichte velden blijven binnen de SAP S/4HANA omgeving met het gebruik van Fiori tegels. Echter, indien er gebruik wordt gemaakt van een transactievariant die zelf specifiek is ingeregeld door Defensie, dan zal deze niet automatisch aangepast worden in de SAP S/4HANA Fiori omgeving. Vastgesteld middels transactie SHD0 is dat er in totaal 90 transactievarianten geconfigureerd zijn binnen de huidige SAP-omgeving. De impact van deze transactievarianten op de interne controlemaatregelen dient verder te worden geanalyseerd voor de daadwerkelijke migratie.

Daarbij is het voor PVA FIN vastgesteld dat er tevens gebruik wordt gemaakt van de 'FIORI-persona' transacties (originele SAP-transactie weergegeven via de Fiori front-end) welke kunnen worden gezien als vertegelde transacties, echter kwam de Dynpro tussenversie niet naar voren tijdens de testwerkzaamheden. Tevens werd tijdens het toetsen hiervan de impact duidelijk van het verdwijnen van transacties/tabellen door de komst van business partners. Zo is vastgesteld dat de FK\* transacties

niet meer worden gebruikt, maar dat de BP (business partner) transactie hiervoor in de plaats zal komen. Hierdoor dienen de specifieke controles tevens in business partner te worden ingeregeld. Voor muteren in financiële gegevens van de leverancier (tabel T055F) is specifiek vastgesteld dat de data wordt geschreven van de business partner naar de debiteuren/crediteuren. Verder is vastgesteld dat er theoretisch een mogelijkheid is dat een persoon bankdata of adres data van een leverancier aanpast, welke pas later effectief wordt gemaakt. Dit is de tijdsafhankelijke instelling die ingeregeld kan worden. De wijziging wordt pas effectief na de gespecificeerde datum, middels een batch account. In dit geval zorgt het batch account dan voor de goedkeuring en niet een onafhankelijke tweede persoon. Of dit issue praktisch kan plaatsvinden, dient verder te worden geanalyseerd voor de daadwerkelijke migratie.

## **BEVO**

Voor de 5 BEVO applicatie controles is op 11.11.2019 getoetst wat de impact zal zijn van de Fiori apps op de werking van de applicatie controles. Hierop is vastgesteld dat de hiervoor relevante apps op het moment van testen nog niet in werking zijn, derhalve kan niet middels testen en walkthroughs worden vastgesteld wat de daadwerkelijke impact is van de Fiori tegels op de werking van de applicatie control. Echter kan voor de control omtrent het inrichten van bewegingssoorten wel worden vastgesteld dat de control op dit moment toeziet op de koppeling tussen toegestane transacties en bewegingssoort. Echter, door de komst van Fiori apps dient er naast de transacties hoogstwaarschijnlijk ook rekening gehouden te worden met de koppeling tussen de toegestane bewegingssoort en de Fiori apps die dit zullen ondersteunen.

## **WSM**

Voor de 7 geselecteerde WSM-controles zijn op 11.11.2019 tevens testwerkzaamheden uitgevoerd op de impact van Fiori apps op de applicatie controles. Hierop is vastgesteld dat de relevante Fiori apps nog niet waren geïnstalleerd. Daar waar bij BEVO naar voren komt dat SAP een transactie 'vertegeld' komt naar voren dat er binnen de WSM-omgeving, een derde versie van een Fiori tegels beschikbaar is namelijk de Dynpro versie. Deze Dynpro versie van de tegel kan worden gezien als een tussenvariant.

Additioneel is tijdens de testwerkzaamheden naar voren gekomen, dat niet alle controles zijn ingeregeld zoals gedefinieerd in het controle raamwerk. Daarbij is additioneel vastgesteld, dat indien er maatwerk wordt toegepast binnen de controle, dit maatwerk tevens aangepast dient te worden om dit in Fiori app werkzaam te krijgen. Tenslotte is er vastgesteld dat niet altijd de verplichte velden vanuit SAP S/4HANA worden overgenomen in de Fiori apps. Hierdoor zullen de 'schermvarianten' van Fiori apart ingericht moeten worden om invoercontroles die voor de traditionele transacties gelden ook van toepassing te laten zijn voor de native Fiori apps.

## **Simplificatie**

Bij de overgang naar S/4HANA zullen bestaande transacties komen te vervallen. SAP heeft hiervoor een simplificatie lijst gepubliceerd waarbij wordt aangegeven welke transacties dit betreft. Hiervoor is een analyse uitgevoerd op het interne controle raamwerk van Defensie. Het is op het moment niet duidelijk te bepalen hoeveel van de bestaande maatregelen worden geraakt, omdat de referentie naar BCD identifiers incompleet is. Dit komt omdat veel van de BCD's niet de transactiecode zelf bevatten maar een omschrijving hoe via het SAP-menu de controle uitgevoerd kan worden. Derhalve, is de algehele impact van de wijziging van transactiecodes op dit moment nog lastig vast te stellen.

Om toch een beeld te kunnen schetsen, is een lijst opgesteld op basis van een vergelijking van de SAP simplificatie lijst met de tabel AGR\_TCODES van de SAP ECC omgeving. Hiervoor is vastgesteld dat dit tenminste 41 verschillende transactiecodes betreffen. Vervolgens is gecontroleerd welke transactiecodes er te herleiden zijn naar de controles die gedefinieerd zijn in het interne controle raamwerk van Defensie. Hiervoor is vastgesteld dat 23 van de 41 transactiecodes worden gebruikt binnen het interne controle raamwerk. Zoals eerder aangegeven, is de verwachting dat de impact groter is omdat in veel van de

interne controles de gebruikte transactiecodes niet zijn gespecificeerd. Additioneel is vastgesteld tijdens de testwerkzaamheden dat de omschrijving van de control binnen het interne controle raamwerk, niet altijd overeenkomt met de control zoals configureert binnen het systeem.

Zie voor de (huidige) simplificatielijst:

[https://help.sap.com/doc/0080a18cdc1045638d31c87b839011e7/1909.000/en-US/SIMPL\\_OP1909.pdf](https://help.sap.com/doc/0080a18cdc1045638d31c87b839011e7/1909.000/en-US/SIMPL_OP1909.pdf)

## **Tabellen**

Naast simplificaties van transactiefunctionaliteit wordt ook het datamodel aangepast in S/4HANA. Tijdens de validatie in de POC-omgeving is ook vastgesteld dat er tabellen worden geraakt door de komst van SAP S/4HANA die relevant zijn voor bepaalde controles. Dit omdat naast transacties, ook tabellen obsoleete raken. Denk hierbij aan de business partner tabel, die de customer- en vendor masterdata tabellen vervangt. Voor de T\* tabellen (T000 etc.) is vastgesteld dat er in totaal 4.112 tabellen zijn op de SAP ECC omgeving, die niet meer beschikbaar zijn in S/4HANA. Andersom, kan worden gesteld dat er 1.274 T\* tabellen op de SAP S/4HANA omgeving zijn, die niet meer beschikbaar zijn op de SAP ECC omgeving.

## **Maatwerk**

Dat transacties en tabellen obsoleete raken, raakt niet alleen de standaard SAP-functionaliteit van de applicatie controles. Tijdens de testwerkzaamheden is naar voren gekomen dat er binnen de applicatie controles welke Defensie heeft gedefinieerd, tevens gebruik wordt gemaakt van maatwerk. Binnen het maatwerk is vastgesteld dat er referenties worden gebruikt naar standaard SAP-transactiecodes en tabellen. Echter, door de overgang naar S/4HANA is het mogelijk dat de betreffende transactiecodes binnen het maatwerk obsoleete raken en dat tabelverwijzingen niet meer kloppen. Daarbij is vastgesteld dat in principe de standaard customizing op basis van de SPRO is vastgesteld, dat de data wordt overgenomen als er wordt gekeken naar zowel de SAP ECC als de POC-omgeving. Echter is wel vastgesteld, dat wanneer bijvoorbeeld de namen van tabel items worden gewijzigd, deze niet worden overgenomen. Daarbij is vastgesteld dat indien er maatwerk wordt toegepast binnen de control dit maatwerk tevens aangepast dient te worden om dit in Fiori app werkzaam te krijgen. Tenslotte is er vastgesteld dat niet altijd de verplichte velden vanuit SAP S/4HANA worden overgenomen in de Fiori native tegels omdat er sprake is van aparte gebruikersschermen. Hierbij is tevens vastgesteld dat er een invloed is van de verplichte velden op de Fiori apps. Hierbij is naar voren gekomen dat de verplichte velden die vanuit de configuratie zijn ingeregeld (transactie SPRO), tevens verplichte velden blijven binnen de SAP S/4HANA omgeving met het gebruik van Fiori tegels. Echter, indien er gebruik wordt gemaakt van een transactievariant die zelf specifiek is ingeregeld door Defensie, dan zal deze niet automatisch aangepast worden in de SAP S/4HANA Fiori omgeving. Vastgesteld middels transactie SHD0, dat er in totaal 90 transactievarianten geconfigureerd zijn binnen de huidige SAP-omgeving.

## **Documentatie**

Tijdens het vooronderzoek is naar voren gekomen dat controles in de praktijk niet op dezelfde manier werken zoals beschreven in het raamwerk. Daarnaast is het op basis van het controleraamwerk niet altijd duidelijk welke specifieke SAP-transacties of tabellen worden gebruikt. Dit maakt het lastig om te bepalen welke controles na de migratie nog zullen werken.

### **3.2.1.4 Aandachtspunten en aanbevelingen**

Op basis van de uitgevoerde validatiewerkzaamheden, waarbij er een vergelijking is gemaakt van (applicatie) controles in de SAP ECC omgeving versus de POC-omgeving, is naar voren gekomen dat er door de overgang van SAP ECC naar SAP S/4HANA verschillende aandachtsgebieden zijn waarbij voorafgaand of tijdens de migratie actie benodigd is.

### **3. Bepaling en documentatie van de relevante controles**

Het huidige controle raamwerk is niet volledig en up-to-date gedocumenteerd. Controles blijken in de praktijk niet altijd te zijn ingericht zoals beschreven, waardoor het valideren van de inrichting in S/4HANA niet goed mogelijk is. Hierdoor is het ook niet altijd goed mogelijk om de maatregelen in het huidige controle raamwerk op efficiënte wijze te monitoren (zowel in de huidige inrichting, als na migratie).

In het kader van het SAP S/4HANA project is een van de doelstellingen om in de toekomst betere managementinformatie te hebben. Echter, om juiste en volledige managementinformatie te rapporteren dient een focus gelegd te worden op de juistheid en volledigheid van de data waarover gerapporteerd dient te worden. Dit kan onder andere door interne beheersingsmaatregelen te implementeren. In het verlengde van het interne controle raamwerk kan er op die manier tevens een focus gelegd worden op het efficiënter maken van de interne processen, door middel van control automatisering en het gebruik van standaard S/4HANA functionaliteiten.

Een eerste stap die kan worden uitgevoerd voorafgaand aan de migratie is derhalve het analyseren van het huidige controle raamwerk, en daarbij de controlemaatregelen te evalueren op relevantie en prioriteit, te toetsen en aan te passen waar nodig. Hierbij kan Defensie in eerste instantie focussen op de 'low hanging fruits'. Waarbij men kan denken aan het opschonen en aanpassen van de huidige controles binnen het controle raamwerk. Echter, in de toekomst is het van belang dat er structureel wordt gekeken naar de opzet, bestaan en werking van het huidige controle raamwerk.

Het verdient aanbeveling om het huidige controle raamwerk als een integraal onderdeel van het SAP S/4HANA project te vernieuwen zodat optimaal gebruik gemaakt kan worden van standaard S/4HANA functionaliteiten, controles goed aansluiten bij de (vernieuwde) procesgang en vanaf de migratie direct met een goed beheerste omgeving gewerkt kan worden.

Derhalve dient dit aspect al voor de start van het project in behandeling te worden genomen. Zodat er voor de start van het project een interne controle raamwerk staat die is gevalueerd en getoetst. Bij de implementatie kunnen vervolgens de relevante interne controle maatregelen in opzet en werking worden meegenomen. Derhalve is de impact en de doorlooptijd van deze aanbeveling hoog. Indien dit aspect niet al voor het project in overweging wordt genomen, ontstaat het risico dat er gedurende de implementatie van S/4HANA wijzigingen doorgevoerd dienen te worden welke initieel niet waren ingeschat, hetgeen op hun beurt weer impact kunnen hebben op andere aspecten binnen het project zoals het autorisatieconcept, implementatie van verschillende modules, etc.

### **4. Evaluatie maatwerk**

Uit de maatwerkanalyse blijkt dat in de huidige SAP-oplossing een groot aantal maatwerk componenten en user exits zijn geïmplementeerd voor interne controle doeleinden. Dit betreft bijvoorbeeld het uitvoeren van validaties en aansluitingen.

Het verdient aanbeveling om als onderdeel van de migratie per maatwerkitem gerelateerd aan interne beheersing vast te stellen of deze functionaliteit nog steeds noodzakelijk is. Daarbij dient geëvalueerd te worden of de functionaliteit reeds bestaat in standaard SAP-functionaliteit in de nieuwe omgeving. Daarbij dient ook kritisch gekeken te worden naar de noodzaak van de maatregel zelf. Mogelijk is de maatregel niet meer actueel, of kan deze komen te vervallen door aanpassingen op regelgeving-, beleid- of procesniveau om zo de bedrijfsvoering efficiënter en effectiever te kunnen laten opereren.

Indien de maatregel noodzakelijk blijkt, dient er beoordeeld te worden of er naast het huidige maatwerk alternatieve maatregelen mogelijk zijn. Dit zouden alternatieve standaard SAP-functionaliteiten kunnen zijn, maar ook organisatorische of procesmatige aanpassingen. Het kan bijvoorbeeld mogelijk zijn om een maatwerk data validatie te vervangen door een standaard SAP-analyse of rapportage.

## **5. Simplificatie en technische migratie**

Tijdens de testwerkzaamheden is naar voren gekomen dat er transacties en tabellen verdwijnen door de komst van SAP S/4HANA. Defensie heeft een lijst van kritische transacties opgesteld. Een eerste stap is om deze kritische transacties te vertalen naar het huidige interne controle raamwerk, en vast te stellen binnen welke controles kritische- en gewijzigde transacties worden gebruikt. Een volgende stap in het kader van SAP S/4HANA Fiori app is om vast te stellen welke native Fiori apps er gebruik maken van de als kritiek geïdentificeerde transacties. Er dient derhalve een mapping gemaakt te worden tussen transacties en de native Fiori apps om vervolgens te bepalen of de gewenst maatregelen in de nieuwe Fiori apps op de juiste wijzen kunnen worden geïmplementeerd.

Tevens komt in de conclusies naar voren dat transactievarianten niet juist en volledig worden overgezet naar native SAP S/4HANA Fiori tegels. Hierbij is vastgesteld dat er 90 transactievarianten aanwezig zijn binnen Defensie. Eerst dient er nagedacht te worden over het huidige proces, om vast te stellen of de transactievarianten nog benodigd zijn. Indien het proces aangepast kan worden om naar standaard SAP over te gaan, dient dit in overweging genomen te worden. Indien het niet mogelijk is om de transactievariant, en derhalve het maatwerk, om te zetten naar standaard SAP, dient er te worden vastgesteld of de transactievariant met hierin onder andere de configuratie omtrent verplichte velden geïmplementeerd kan worden (zie ook onder maatwerk).

## **6. In control by design**

Voor een effectieve migratie naar S/4HANA is het van belang dat interne beheersing als integraal onderdeel wordt meegenomen binnen de project aanpak. Dit betreft het tijdig definiëren van de benodigde maatregelen op basis van de relevante risico's (zoals opgenomen in aanbeveling 1). Naar verwachting zal er als onderdeel van de migratie een fit-to-standaard plaatsvinden voor de functionele processen. Het verdient aanbeveling om de gerelateerde interne beheersingsaspecten als integraal onderdeel van deze activiteiten op te nemen. Op deze wijze kunnen de beheersmaatregelen als integraal onderdeel van de procesgang worden gerealiseerd. Dit zal zorgen voor:

- Duidelijke betrokkenheid en eigenaarschap van de business
- Kosten efficiënte analyse. Het is niet nodig om interne beheersing op een later moment toe te voegen aan procesbeschrijvingen
- Optimaal gebruik van standaard S/4HANA functionaliteit
- Effectieve beheersmaatregelen direct vanaf migratie

### **Relatie tot migratiescenario's**

De beschreven impact en aanbevelingen zijn relevant voor alle migratiescenario's. Voor het scenario hergebruik zal de optimalisatie naar Fiori op een later moment worden uitgevoerd. De impact t.a.v. simplificatie en maatwerk zullen direct als onderdeel van de technische conversie geadresseerd dienen te worden. Dit geldt ook voor het hybride scenario.

Voor het scenario 'nieuwe omgeving' geldt dat het adresseren van simplificatie en de maatwerkanalyse gefaseerd uitgevoerd kunnen worden. Namelijk alleen voor de deelfunctionaliteiten die onderdeel zijn van de onder handen zijnde gefaseerde migratiestappen. Dit zal op termijn dezelfde werkzaamheden betreffen, echter over een langere periode verdeeld. Generieke IT-controles

#### 3.2.1.5 AS-IS situatie

De generieke IT-maatregelen volgen dezelfde beschrijving zoals vermeld in sectie 3.2.1.2. Onder deze controles vallen onder andere de onderwerpen wijzigingsbeheer, incident management en gebruikersbeheer. Hiervan staat het ontwerp van deze maatregelen in Toetsingskaders.

#### 3.2.1.6 Impact S/4HANA

##### **Fiori security**

De belangrijkste wijziging voor de generieke IT-controles is de introductie van de FIORI-user interface. Om gebruikers toegang te verlenen tot de FIORI-apps dienen specifieke FIORI rollen aan de gebruiker toegekend te worden. De impact die dit heeft op de IT-controles heeft is afhankelijk van de manier waarop FIORI wordt geïmplementeerd. Dit kan als centrale hub, waarbij er een aparte FIORI-gateway server wordt toegevoegd aan het landschap, of embedded, waarbij de FIORI-server wordt gedraaid op de S/4HANA instance.

Wordt het embedded model gebruikt, dan is de impact beperkt en zullen slechts enkele specifieke configuraties aan de reeds bestaande controles toegevoegd moeten worden. Bij de implementatie van S/4HANA en Fiori middels het 'centrale hub' model wordt er een aparte front-end server aan het landschap toegevoegd waarvoor de general IT controls ingericht en gemonitord dienen te worden. Hierbij zullen de volgende aspecten meegenomen moeten worden:

- **Authenticatie:** Wachtwoordverificatie voor Fiori wordt geconfigureerd via SAP Fiori Gateway of Single Sign On. Als authenticatie is geconfigureerd via SAP Fiori Gateway, dient naast de SAP-authenticatie, ook de authenticatiecontrole in de SAP Fiori Gateway opgenomen te worden.
- **Standaard SAP Accounts:** De standaardwachtwoorden voor standaard SAP-accounts dienen in alle mandanten gewijzigd te zijn, en op de juiste manier beveiligd te zijn. Indien toegang tot een van deze krachtige gebruikersaccounts vereist wordt geacht, dient het verzoek te zijn gedocumenteerd en goedgekeurd door het management. Waarbij vervolgens de toegang wordt verwijderd na voltooiing van de werkzaamheden en de activiteiten op basis van de logging worden gereviewd.
- **Standaard profielen:** toegang tot SAP\_ALL/SAP\_NEW en andere standaard profielen dient voldoende beveiligd te zijn door ervoor te zorgen dat geen enkele dialoog of servicegebruiker toegang heeft tot deze profielen. Indien toegang vereist is, dient het profiel te worden aangevraagd en voor toekenning dient de aanvraag goedgekeurd te worden door management. Na voltooiing van de werkzaamheden dienen de autorisaties verwijderd te worden bij het account en de activiteiten van het account te worden gereviewd.

##### **Overige IT-controles**

- **Gebruikersrechtenreview:** Bij een gebruikersreview wordt er gekeken naar de actieve gebruikers in het SAP-systeem en de daarbij toegekende rollen en rechten. Bij het gebruik van S/4HANA en Fiori dient er naast de toegang op de back-end tevens geanalyseerd te worden welke Fiori objecten onderdeel zijn van de review. Hierbij dient zowel de front-end als de back-end toegang binnen Fiori overwogen te worden voor de review.
- **Functiescheidingsreview:** De komst van SAP S/4HANA en Fiori zal beperkte impact hebben op de functiescheidingsconflicten binnen het systeem. Echter zal er wel een impact zijn op de inhoudelijke autorisaties, objecten en tabellen ten opzichte van het huidige autorisatiemodel. De gebruikte ruleset zal daarom moeten worden aangepast om S/4HANA goed te ondersteunen. Dit betreft onder andere het aanpassen van items die geraakt worden door simplificatie (obsolete transacties, objecten en tabellen) en het kunnen reviewen van toegang via Fiori apps.
- **Authenticatie**
  - Indien er geen gebruik wordt gemaakt van Single Sign-On, maar er wel gebruik wordt gemaakt van een centrale hub, dan dient de authenticatie tevens getoetst te worden op

de SAP Fiori Gateway. Indien het "embedded deployment" model zal worden gebruikt door Defensie, dan zijn er geen additionele authenticatie controles benodigd dan degene die worden uitgevoerd op de SAP S/4HANA productie omgeving.

- Indien er gebruik wordt gemaakt van Single Sign-On waarbij gebruikers zich door middel van SNC dient er door middel van tabel USRACL vastgesteld te worden of de gebruikers de SAP GUI kunnen gebruiken om door middel van wachtwoord login. Daarnaast geeft S/4HANA ook de mogelijkheid om gebruikers (groepen) specifieke instellingen voor wachtwoord regels, wachtwoord wijzigingen, het wijzigingsbeleid voor wachtwoorden en voor login restricties te definiëren. Dit kan worden gedaan door middel van het toekennen van Security Policies aan gebruikers. De gerelateerde IT controles dienen uitgebreid te worden om deze aspecten te kunnen implementeren en monitoren.

- **Wijzigingsbeheer en development toegang**

- Binnen SAP ECC is voor het verkrijgen van development (ontwikkel) toegang op de productie omgeving toegang benodigd tot:
  1. De juiste autorisaties
  2. Het toegewezen hebben van een Developer Key
  3. System- en Client instellingen
- Bij de implementatie van S/4HANA zal de Developer Key niet meer worden toegepast en kan er derhalve middels de juiste autorisaties en de system- en client instellingen toegang worden verschaft tot development toegang op de productie omgeving. Binnen SAP ECC wordt middels transactie SE11\_OLD toegang verschaft tot het onderhouden van de ABAP dictionary, deze transactie is niet meer beschikbaar in de S/4HANA omgeving.
- In het geval van toegang tot het uitvoeren van programma's is SAP note 1596907 standaard onderdeel van SAP S/4HANA, welke in de eerdere versies van SAP ECC nog geïnstalleerd diende te worden. Derhalve dienen gebruikers met toegang tot ACTVT 03 ook toegang te hebben tot ACTVT 16 om ook daadwerkelijk programma's uit te voeren via transactie SE38 of SA38.
- Toegangsrechten om de client open te zetten, worden onder andere verschaft door middel van transactie SCC4. Echter wordt er binnen SAP S/4HANA toegang tot de SCC4 transactie code gecontroleerd met daarbij de EN relatie met SM30/SM31/OY25/S\_B20\_88000036.

### 3.2.1.7 Aandachtspunten en aanbevelingen

Op basis van de uitgevoerde validatiewerkzaamheden, waarbij er een vergelijking is gemaakt van general IT controls in de SAP ECC omgeving versus de POC-omgeving, is naar voren gekomen dat er door de overgang van SAP ECC naar SAP S/4HANA beperkte impact is.

#### 1. Adresseren Fiori en simplificatie

De impact die migratie naar S/4HANA heeft op de generieke IT-maatregelen is beperkt. De belangrijkste aandachtsgebieden zijn het opnemen van relevante controles rondom Fiori en een beperkt aantal wijzigingen voortkomend uit simplificatie, zoals het wegvallen van de developer key.

#### 2. Documentatie

Er is veel documentatie aanwezig binnen de toetsingskaders, echter de beschikbaarheid en bekendheid van deze documentatie binnen Defensie is niet breed verspreid. Alhoewel niet direct gerelateerd aan de implementatie van S/4HANA, verdient het hierbij de aanbeveling om tevens de algemene processen rondom gebruikersbeheer- en wijzigingsbeheer te documenteren en op een centrale plaats beschikbaar te maken voor de relevante medewerkers van Defensie.

### 3.3 Samenvatting observaties en aanbevelingen

In de onderstaande tabel zijn alle in hoofdstuk drie beschreven observaties en aanbevelingen samengevat om zo één totaaloverzicht te geven.

| Paragraaf                      | Onderwerp                                                | Observatie/aanbevelingen                                                                                                                                                                                                                                                                                           |
|--------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.1.1 Security en autorisatie  | Toegangsrechten                                          | Toegangsrechten dienen zowel op de SAP S/4HANA omgeving als apart voor de Fiori omgeving te worden gerealiseerd en beheerd.                                                                                                                                                                                        |
|                                | Autorisatiemodel                                         | Veranderingen in het datamodel en beschikbare transacties (simplificatie) zorgen dat de autorisatie- en securityinrichting mogelijk niet meer juist werkt                                                                                                                                                          |
|                                | Functionaliteiten                                        | Aanpassingen van functionaliteiten of introductie van nieuwe functies leidt tot opzetten nieuwe autorisaties                                                                                                                                                                                                       |
|                                | Datatoegang                                              | HANA DB en Data Control Language (DCL) die ook CDS-weergaven omvat worden als nieuwe autorisatietechnieken toegevoegd aan het concept en dienen opgenomen te worden in security architectuur en proces.                                                                                                            |
|                                | Functionaliteiten                                        | UI Masking en UI Logging functionaliteiten dienen overwogen te worden als aanvulling tot afschermen vertrouwelijke data.                                                                                                                                                                                           |
|                                | Security by design                                       | Autorisaties en security dienen als integraal onderdeel mee te worden genomen binnen de totale project aanpak                                                                                                                                                                                                      |
| 3.1.2 Security-Beheerprocessen | Procesbeschrijving                                       | Beschikbare documentatie is niet altijd volledig en up-to-date. Het verdient aanbeveling om voor de implementatie van S/4HANA met Fiori, de nieuwe en geoptimaliseerde processen in een vast format te documenteren en helder te communiceren naar de betrokkenen binnen het proces                                |
|                                | Gebruikersbeheer                                         | In het geval van een centrale hub worden gebruikersbeheerprocessen significant complexer wegens het veranderende rollenmodel. Additioneel werk is benodigd om beide rollen af te stemmen en vergroot risico dat niet alle ouden rechten worden verwijderd bij uitdiensttreding of doorstroom.                      |
|                                | Processen – standaard accounts                           | Door middel van de overgang naar S/4HANA zullen de standaard accounts niet veranderen. Echter dienen deze accounts wel opnieuw ingesteld te worden, waarbij het standaard wachtwoord van de accounts gewijzigd dienen te worden alsmede de accounts bij default op geblokkeerd dienen te staan.                    |
|                                | Processen – gebruikersreview en functiescheidings review | Door de komst van S/4HANA zal er een impact zijn op de rulesets die gebruikt worden voor monitoring, zoals de SOD-matrix. Dit komt door de komst van verwijderde, aangepaste en nieuwe transacties, tabellen en SAP-functionaliteiten.                                                                             |
|                                | Fiori toegangsbeheer                                     | Vanuit het perspectief voor toegangsbeheer verdient het aanbeveling de Fiori front-end server in te richten volgens het embedded model. Dit zal de toekenning en het beheer van rechten efficiënter maken en zal een relatief kleiner risico vormen voor het toekennen van onvoldoende of ongeautoriseerde rechten |

|                              |                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | Tooling                             | Het datamodel in S/4HANA wijzigt niet significant voor de dataobjecten die relevant zijn voor autorisaties en security. Daarmee wordt verwacht dat CUA, CSI en NextLabs zullen blijven werken op de S/4HANA omgeving. Wel zullen inhoudelijke aspecten zoals functiescheidingsregels vernieuwd moeten worden om eventuele aanpassingen in processen en de toevoeging van Fiori te kunnen ondersteunen.                                                                                                                                                                                                                                                               |
|                              | Tooling                             | Het verdient aanbeveling om naast de analyse van wijzigingen in toegangsrechten, configuratie en beheerprocessen (zie 3.1.1 en 3.1.2) ook te kijken naar het totaal aan tooling dat deze aspecten op efficiënte en effectieve wijze kan ondersteunen. Er dient daarbij rekening gehouden te worden met de IT-beveiliging en toegangsvereisten, gegevenstoegang en -bescherming, ITGC en applicatiecontroles, monitoring en de roadmap van de Defensie-infrastructuur. Daarbij verdient het aanbeveling om dit op holistisch niveau uit te voeren, om overlap tussen toolfunctionaliteit of ongeadresseerde aspecten te voorkomen.                                    |
| 3.2.1<br>Applicatiecontroles | Modules en nieuwe functionaliteiten | De impact van de SAP S/4HANA modules op het interne controle raamwerk is in grote mate afhankelijk van de mate waarin de SAP Modules wijzigen in het nieuwe systeem. Bij een migratie naar S/4HANA is het benodigd om een aantal SAP-modules en systemen te vervangen. Daarnaast brengt S/4HANA nieuwe functionaliteit met zich mee. Dit betreft onder andere DF-PS/D&S, FMS, Universal Ledger, Business Partners, House Banks, Foreign Trade, TM, MDG, eWM en de introductie van Fiori apps. Deze gewijzigde SAP-modules en systemen resulteren in nieuwe en gewijzigde processen en functionaliteiten waar het interne controle raamwerk op moet worden aangepast. |
|                              | Standaard SAP functionaliteiten     | Analyseren welke controles maatwerk bevatten en of deze controles omgezet kunnen worden naar maatregelen die uitgaan van standaard SAP-functionaliteit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                              | Verplichte velden                   | De verplichte velden die vanuit de configuratie zijn ingeregeld blijven binnen de SAP S/4HANA omgeving met het gebruik van Fiori tegels. Echter, indien er gebruik wordt gemaakt van een transactievariant die zelf specifiek is ingeregeld door Defensie, dan zal deze niet automatisch aangepast worden in de SAP S/4HANA Fiori omgeving.                                                                                                                                                                                                                                                                                                                          |
|                              | Businesspartners                    | Verdwijnen van transacties/tabellen door de komst van business partners. Hierdoor dienen de specifieke controles tevens in business partner te worden ingeregeld.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                              | Maatwerk                            | <p>Bij de standaard customizing op basis van de SPRO wordt de data in principe overgenomen. Echter is wel vastgesteld, dat wanneer bijvoorbeeld de namen van tabel items worden gewijzigd, deze niet worden overgenomen.</p> <p>Verplichte velden die vanuit de configuratie zijn ingeregeld (transactie SPRO), blijven verplichte velden binnen de SAP S/4HANA omgeving met het gebruik van Fiori tegels. Echter, indien er gebruik wordt gemaakt van een transactievariant die zelf specifiek is ingeregeld door</p>                                                                                                                                               |

|                              |                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                        | Defensie, dan zal deze niet automatisch aangepast worden in de SAP S/4HANA Fiori omgeving.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                              | Simplificatie          | Bij de overgang naar S/4HANA zullen bestaande transacties en tabellen komen te vervallen. SAP heeft voor de transacties die komen te vervallen, een simplificatie lijst gepubliceerd waarbij wordt aangegeven welke transacties dit betreft. Een eerste stap is om deze kritische transacties te vertalen naar het huidige interne controle raamwerk, en vast te stellen binnen welke controles kritische- en gewijzigde transacties worden gebruikt. Een volgende stap in het kader van SAP S/4HANA Fiori app is om vast te stellen welke native Fiori apps er gebruik maken van de als kritiek geïdentificeerde transacties. Er dient derhalve een mapping gemaakt te worden tussen transacties en de native Fiori apps om vervolgens te bepalen of de gewenst maatregelen in de nieuwe Fiori apps op de juiste wijzen kunnen worden geïmplementeerd. Eenzelfde analyse dient uitgevoerd te worden voor de tabellen die komen te vervallen. |
|                              | Controle raamwerk      | <p>Het huidige controle raamwerk is niet volledig en up-to-date gedocumenteerd. Controles blijken in de praktijk niet altijd te zijn ingericht zoals beschreven, waardoor het valideren van de inrichting in S/4HANA niet goed mogelijk is. Hierdoor is het ook niet altijd goed mogelijk om de maatregelen in het huidige controle raamwerk op efficiënte wijze te monitoren.</p> <p>Het verdient aanbeveling om het huidige controle raamwerk als een integraal onderdeel van het SAP S/4HANA project te vernieuwen zodat optimaal gebruik gemaakt kan worden van standaard S/4HANA functionaliteiten, controles goed aansluiten bij de (vernieuwde) procesgang en vanaf de migratie direct met een goed beheerste omgeving gewerkt kan worden.</p>                                                                                                                                                                                         |
|                              | In control by design   | Voor een effectieve migratie naar S/4HANA is het van belang dat interne beheersing als integraal onderdeel wordt meegenomen binnen de project aanpak. Dit betreft het tijdig definiëren van de benodigde maatregelen op basis van de relevante risico's.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 3.2.2 Generieke IT-controles | Fiori en simplificatie | De impact die migratie naar S/4HANA heeft op de generieke IT-maatregelen is beperkt. De belangrijkste aandachtsgebieden zijn het opnemen van relevante controles rondom Fiori en een beperkt aantal wijzigingen voortkomend uit simplificatie, zoals het wegvallen van de developer key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                              | Documentatie           | Er is veel documentatie aanwezig binnen de toetsingskaders, echter de beschikbaarheid en bekendheid van deze documentatie binnen Defensie is niet breed verspreid. Alhoewel niet direct gerelateerd aan de implementatie van S/4HANA, verdient het hierbij de aanbeveling om tevens de algemene processen rondom gebruikersbeheer- en wijzigingsbeheer te documenteren en op een centrale plaats beschikbaar te maken voor de relevante medewerkers van Defensie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## **4 Relatie met andere deelproducten**

### **4.1 *Input van deelproduct***

- 2.3 Roadmaps
- 2.6 Migratieaanpak
- D09 Huidige architectuur en beheer

### **4.2 *Input voor deelproduct***

- 2.13 Afstemming andere projecten
- POC 1 – report out
- POC 2 – report out

## 5 Akkoord

| Datum | Naam | Akkoord | Opmerking |
|-------|------|---------|-----------|
|       |      |         |           |
|       |      |         |           |
|       |      |         |           |
|       |      |         |           |

## **6 Bijlage(n)**