

Vergaderjaar 2016–2017

**31 125**

**Defensie Industrie Strategie**

**Nr. 74**

**LIJST VAN VRAGEN EN ANTWOORDEN**

Vastgesteld 20 februari 2017

De vaste commissie voor Defensie heeft een aantal vragen voorgelegd aan de Minister van Defensie over de brief van 5 december 2016 inzake de Voortgangsrapportage IT en ERP (Kamerstuk 31 125, nr. 72).

De Minister heeft deze vragen beantwoord bij brief van 15 februari 2017. Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,  
Ten Broeke

De griffier van de commissie,  
De Lange

**1**

**Heeft de selectiefase van de aanbesteding van de nieuwe IT-infrastructuur inderdaad rond de jaarwisseling plaatsgevonden? Betekent dit dat de dialoofase inmiddels is aangevangen?**

De laatste fase van het beoordelingsproces heeft rond de jaarwisseling plaatsgevonden. Op 15 februari jl. is de definitieve selectiebeslissing genomen. De twee geselecteerde partijen worden gescreend volgens de Algemene Beveiligingseisen voor Defensie Opdrachten (ABDO). Ook het personeel van de partijen dat aan de dialoog zal deelnemen ondergaat, waar nodig, een veiligheidsonderzoek. Zodra deze en andere voorbereidingen zijn voltooid, start de dialoofase. De verwachting is dat de dialoofase in het voorjaar van start zal gaan.

**2**

**Welke voordelen zijn er wanneer gekozen zou worden voor één hoofdleverancier bij de bouw en het beheer van de IT-infrastructuur ten opzichte van een versnipperd leverancierslandschap?**

**3**

**In hoeverre sluit een keuze voor één hoofdleverancier bij de bouw en het beheer van de IT-infrastructuur ten opzichte van een versnipperd leverancierslandschap aan bij de ontwikkelingen in de IT-markt?**

Het werken met één hoofdopdrachtnemer biedt meer zekerheid voor een moderne en goed functionerende IT-infrastructuur. In de praktijk zal de hoofdopdrachtnemer meerdere onderaannemers en leveranciers aansturen. Het integratierisico van de afzonderlijke delen tot één geheel ligt daarmee bij de hoofdaannemer en niet bij Defensie. Dit voorkomt dat Defensie door verschillende leveranciers tegen elkaar wordt uitgespeeld. Een succesvolle integratie van IT-infrastructuur vraagt kennis en ervaring, die bij gespecialiseerde marktpartijen in grotere mate aanwezig is dan bij Defensie. Op deze wijze kan Defensie optimaal profiteren van de kennis en ervaring in de markt.

Defensie kiest ervoor één hoofdopdrachtnemer te contracteren en daarmee in een partnerschap dit programma tot uitvoer te brengen. Het is daardoor eenvoudiger om de dienstverlening aan te sturen en afspraken te maken over gemeenschappelijke inzet van personeel. Dat laatste is belangrijk in het licht van de eis van Defensie om in uitzendgebieden zelf het beheer te kunnen voeren.

De keuze voor één hoofdleverancier is gemaakt op grond van ervaringen uit het verleden en op grond van nieuwe en uitvoerige analyses van Defensie zelf en externe adviespartijen. In de markt wordt gewerkt met zowel één hoofdleverancier als met een verkaveld leverancierslandschap.

**4**

**Is de verwachting dat de reorganisatie tot extra uitstroom zal leiden?**

**5**

**Heeft de (voorgenomen) reorganisatie van JIVC/OPS tot extra uitstroom geleid?**

Op dit moment heeft de reorganisatie van JIVC/OPS nog niet tot extra uitstroom geleid. De huidige reorganisatie betreft de samenvoeging van JIVC en OPS, waarbij de verwachting is dat er sprake zal zijn van een beperkte boventaligheid. Over de personele gevolgen van de

vernieuwing van de IT-infrastructuur zal pas gedurende de dialoog met de geselecteerde marktpartijen in het programma Grensverleggende IT (GrIT) meer duidelijkheid ontstaan.

**6**

**Welke risico's onderkent u voor het project IT-vernieuwing wanneer de reorganisatie van JIVC/OPS per eind 2017 nog niet is voltooid? Hoe worden deze risico's beheerst?**

**12**

**Kunt u inzicht geven in de belangrijkste planningsrisico's voor de vernieuwing van de IT?**

**14**

**Kunt u inzicht geven in de belangrijkste planningsrisico's voor de vernieuwing van de IT?**

In het programma Grensverleggende IT (GrIT) wordt actief gestuurd op het mitigeren van de risico's, die inherent zijn aan een dergelijk complex programma. Risicomanagement is een continu proces waarin risico's worden herkend, onderzocht en gemitigeerd.

Het Bureau ICT Toetsing (BIT) heeft in zijn advies (Kamerstuk 31 125, nr. 70) inzake GrIT al gewezen op de belangrijkste risico's voor het programma. De adviezen van het BIT zijn overgenomen in het programmaplan.

Het planningsrisico bestaat dat partijen die gedurende het traject afvallen, de beslissing juridisch aanvechten. Dit risico wordt gemitigeerd door in de selectie uiterste zorgvuldigheid te betrachten. De Landsadvocaat is tot nu toe voortdurend betrokken en dit wordt gecontinueerd in de dialoogfase. Ook is er in het programmateam personeel ingehuurd dat ervaring heeft met dergelijke complexe aanbestedingstrajecten.

Een ander risico is het tijdig voorhanden hebben van capaciteit om na de dialoog, samen met de verkozen marktpartij, de IT-vernieuwing te realiseren. Die vernieuwing moet worden gerealiseerd terwijl de huidige IT nog een tijd doordraait en in die tijd ook onderhouden moet worden. Dit risico wordt gemitigeerd door het benodigde defensiepersoneel voor de vernieuwing vrij te spelen en hun bestaande werkzaamheden gedurende het programma door extra ingehuurd personeel te laten overnemen. Ook worden de aanpassingen van de bestaande IT tot een minimum beperkt.

De reorganisatie waarin JIVC en OPS worden samengevoegd, moet organisatorisch de juiste uitgangssituatie voor de nieuwe IT creëren. Indien deze reorganisatie eind 2017 nog niet is voltooid, kan het noodzakelijk zijn om op basis van de bestaande organisatie een tijdelijke beheerorganisatie voor de nieuwe IT-infrastructuur op te bouwen, die dan in een later stadium opgaat in de nieuwe definitieve organisatie. Tijdens de dialoogfase is het voorts noodzakelijk om niet alleen met de marktpartijen, maar ook met de medezeggenschap en de centrales voor overheids-personeel tijdig tot overeenstemming te komen over welk defensiepersoneel in de nieuwe IT-infrastructuur zal worden ingezet, de wijze waarop dat plaats zal vinden en de personele consequenties die daaruit voortvloeien. Een planningsrisico is dat deze overeenstemming niet tijdig kan worden bereikt. Dit risico wordt gemitigeerd door de medezeggenschap en centrales vroegtijdig te betrekken in dit traject en, binnen de gedefinieerde uitgangspunten voor de nieuwe IT, maximaal in te zetten op perspectief voor het personeel.

7

**Hoe lang zal de gunnings- en contractfase naar verwachting duren en wanneer kan de leverancier de werkzaamheden starten?**

Na afloop van de dialoog start de gunnings- en contractfase, die circa drie maanden in beslag zal nemen. De leverancier kan daarna volgens de afspraken in het contract direct, in samenwerking met Defensie, met werkzaamheden starten.

8

**Welke IT-problemen zijn er op dit moment nog, nu de IT-problemen volgens de voortgangsrapportage «grotendeels» zijn opgelost? Welke risico's bestaan er daardoor nog voor de continuïteit, beveiliging en/of operatie?**

11

**Welke IT-problemen zijn er op dit moment nog, nu de IT-problemen volgens de voortgangsrapportage «grotendeels» zijn opgelost? Welke risico's bestaan er daardoor nog voor de continuïteit, beveiliging en/of operatie?**

Op dit moment zijn er geen continuïteitsproblemen zoals die zich in 2014 voordeden. Er zijn maatregelen getroffen om de onverstoorde werking van de bestaande IT-infrastructuur de komende jaren te waarborgen. Deze zijn inmiddels op orde en toekomstvast ingericht. Terwijl een deel van de organisatie zich primair richt op de vernieuwing van de IT, is de continuïteit van de bestaande IT de belangrijkste prioriteit voor de rest van JIVC en OPS. Er is daarvoor veel meer aandacht dan enkele jaren geleden en het wordt ook veel planmatiger aangepakt, waardoor delen van de bestaande IT-infrastructuur tijdig worden aangepast of vervangen. Vanzelfsprekend vindt er afstemming plaats met het vernieuwingsprogramma GrIT om beide trajecten op elkaar te laten aansluiten.

9

**Kunt u een overzicht geven van hoeveel IT-verstoringen zich in de jaren 2014–2016 in totaal per jaar hebben voorgedaan, zowel klein als groot?**

	Aantal IT-verstoringen per jaar		
	2014	2015	2016
Crisis	1	0	0
Calamiteit	11	16	5
Grote verstoringen	549	524	397
Incidenten bij individuele klant	45.853	39.227	26.674

10

**Wat verstaat u onder een «grote verstoring»? Hoe onderscheidt zich dit van kleinere verstoringen?**

Een verstoring bij een individuele klant wordt aangeduid als een incident. Wanneer meer gebruikers worden getroffen door de verstoring, dan wordt gesproken van een grote verstoring. Deze worden dan ook op intranet gemeld, maar nog steeds routinematig aangepakt. Wanneer een routinematige oplossing niet mogelijk is of niet snel genoeg resultaat oplevert en de gevolgen van de storing dat rechtvaardigen, wordt een grote verstoring geëscaleerd tot calamiteit. Er treedt dan een afzonderlijk proces in werking waarbij mandaten, sturing en communicatie dusdanig

zijn aangepast dat een snelle oplossing van de verstoring mogelijk wordt gemaakt. Een crisis is een geëscaleerde calamiteit.

**11**

**Welke IT-problemen zijn er op dit moment nog, nu de IT-problemen volgens de voortgangsrapportage «grotendeels» zijn opgelost? Welke risico's bestaan er daardoor nog voor de continuïteit, beveiliging en/of operatie?**

Zie het antwoord op vraag 8.

**12**

**Kunt u inzicht geven in de belangrijkste planningsrisico's voor de vernieuwing van de IT?**

Zie het antwoord op vraag 6.

**13**

**Klopt het dat u voor de periode 2016–2021 ruim 811 miljoen euro heeft gereserveerd voor investeringen in IT bij Defensie, maar dat u nog niet zeker bent of dit voldoende is?**

**17**

**Zijn er vanaf 2020 wel voldoende middelen beschikbaar om structureel in IT te investeren, nu uit de tabel duidelijk wordt dat de post «voorzien in IT» flink terugloopt vanaf 2020?**

**18**

**Hoe kunt u garanderen dat er na 2020 voldoende middelen beschikbaar zijn om te kunnen investeren in IT vernieuwing zodat de organisatie niet wederom na jarenlange achterblijvende investeringen met dezelfde als de huidige IT problemen te maken krijgt, die immers het gevolg zijn van het over langere tijd onvoldoende investeren in vernieuwing?**

**19**

**Hoe gaat u er voor zorgen dat er ook op de langere termijn in de IT bij Defensie de noodzakelijke investeringen in vernieuwing gedaan zullen worden zodat de organisatie, zeker in dit digitale tijdperk, blijvend kan beschikken over een goed functionerende IT?**

Na 2020 daalt het IT-budget voor investeringen. Vanwege het kort-cyclische karakter van IT-projecten is het benodigde budget na 2020 op dit moment nog niet te ramen. Naarmate de tijd vordert, zijn projecten verder uitgewerkt. De concrete bedragen worden dan ingepast. In het kader van financiële duurzaamheid wordt momenteel onderzocht of in de investeringsbegroting met een vaste bandbreedte voor IT-uitgaven kan worden gewerkt waaruit projecten worden gefinancierd.

**14**

**Kunt u inzicht geven in de belangrijkste planningsrisico's voor de vernieuwing van de IT?**

Zie het antwoord op vraag 6

**15**

**Als onder de bedragen, zoals opgenomen in de post «IT-vernieuwing», de kosten voor de programmaorganisatie, (extern)personeel, versterking IT regie en IV-problematiek vallen, welk bedrag is dan gereserveerd voor de daadwerkelijke vernieuwing van de IT zelf, bestaande uit het kopen van**

**hardware, software(licenties), dienstverlening leverancier en dergelijke?**

**16**

**Onder welke post is een bedrag gereserveerd voor de daadwerkelijke vernieuwing van de IT zelf, bestaande uit het kopen van hardware, software(licenties), dienstverlening leverancier en dergelijke? Wat is de hoogte van het gereserveerde bedrag?**

De nieuwe IT zal deels worden gefinancierd uit investeringen, en deels uit exploitatie. De bedragen die op dit moment daarvoor beschikbaar zijn, zijn vermeld in het «overzicht uitgaven IT», zoals dat in de begroting 2017 is opgenomen.

**Totaaloverzicht van uitgaven aan IT x € 1.000**

Omschrijving	Begroting	2017	2018	2019	2020	2021
Voorzien in IT, exploitatie	Artikel 2	2.680	2.679	2.679	2.678	2.678
Voorzien in IT, investering	Artikel 6	185.382	180.270	180.154	80.093	50.160
– waarvan reservering van 40,2 miljoen vernieuwing IT (vanaf 2016)		22.200	6.800	5.100	700	
– waarvan reservering dubbele beheerlasten IT		27.000	30.000	30.000	30.000	
Bijdrage aan DMO/OPS /IT exploitatie	Artikel 7	181.442	182.112	189.323	189.432	188.816
Voorzien in IT, exploitatie (overig)	Artikel 7	43.137	43.135	40.164	40.982	40.982
<b>Totaal uitgaven IT</b>		<b>412.641</b>	<b>408.196</b>	<b>412.320</b>	<b>313.185</b>	<b>282.636</b>

In de dialoofase zal duidelijk worden hoe de kosten van de nieuwe IT zijn opgebouwd, en hoe de verhouding tussen investeringen en exploitatie zal komen te liggen. Daarbij is het overigens niet zo dat Defensie zelf de benodigde hardware en software zal aanschaffen. Volgens de uitgangspunten voor samenwerking met de markt in het High Level Ontwerp (Kamerstuk 31 125, nr. 57) ligt het eigenaarschap voor de middelen voor een belangrijk deel bij de markt, waarbij Defensie de IT in de vorm van een dienst afneemt. Tegenover de kosten hiervoor staan besparingen in de bestaande IT. Defensie gaat er vanuit dat de marktpartij daarbij ook met doelmatigere nieuwe oplossingen komt. Waar de balans van het eigenaarschap van middelen precies komt te liggen, zal pas in de loop van de dialoog duidelijk worden,

De reservering voor dubbele beheer, transitie en migratie is als risicoreservering opgenomen voor de overgangssituatie als zowel de huidige als de nieuwe IT-infrastructuur actief zijn.

**17**

**Zijn er vanaf 2020 wel voldoende middelen beschikbaar om structureel in IT te investeren, nu uit de tabel duidelijk wordt dat de post «voorzien in IT» flink terugloopt vanaf 2020?**

Zie het antwoord op vraag 13.

**18**

**Hoe kunt u garanderen dat er na 2020 voldoende middelen beschikbaar zijn om te kunnen investeren in IT vernieuwing zodat de organisatie niet wederom na jarenlange achterblijvende investeringen met dezelfde als de huidige IT problemen te maken**

**krijgt, die immers het gevolg zijn van het over langere tijd onvoldoende investeren in vernieuwing?**

Zie het antwoord op vraag 13.

**19**

**Hoe gaat u er voor zorgen dat er ook op de langere termijn in de IT bij Defensie de noodzakelijke investeringen in vernieuwing gedaan zullen worden zodat de organisatie, zeker in dit digitale tijdperk, blijvend kan beschikken over een goed functionerende IT?**

Zie het antwoord op vraag 13.

**20**

**Wat was de aanleiding voor een verhoging van 5 miljoen euro voor ondersteuning van de IT-regie?**

Medio 2016 is het budget voor het versterken van de regieorganisatie verhoogd van € 4,3 miljoen naar € 5 miljoen, omdat meer ondersteuning noodzakelijk bleek. Dit betreft ondersteuning vanuit KPMG als strategische regiepartner voor het inrichten van de regiefunctie binnen het IT-vernieuwingsprogramma.

**21**

**Kunt u het geraamde bedrag van 7 miljoen euro voor externe inhuur nader toelichten? Waarom is gekozen voor inhuur in plaats van bijvoorbeeld uitbreiding van de bestaande organisatie?**

De nieuwe IT-infrastructuur wordt stapsgewijs opgebouwd, terwijl de oude infrastructuur nog een tijd doordraait en onderhouden moet blijven worden. Dit veroorzaakt een tijdelijke extra behoefte aan personeel. Er wordt eigen personeel vrijgemaakt voor de vernieuwing, waarbij hun bestaande werkzaamheden voor de bestaande infrastructuur door extra ingehuurd personeel wordt overgenomen. Voorts heeft het programmeamteam behoefte aan specifieke deskundigheid gedurende de aanbesteding, die eveneens wordt ingehuurd. Aangezien de extra behoefte verdwijnt zodra de oude infrastructuur wordt uitgefaseerd, is er niet gekozen voor uitbreiding van de bestaande organisatie.

**22**

**Is de voorziening van 117 miljoen euro voor dubbele beheerslasten, transitie en migratie alleen gerelateerd aan het programma Grensverleggende IT? Zo nee, aan welke andere projecten is deze voorziening nog meer gerelateerd?**

De voorziening is alleen bedoeld voor activiteiten die gerelateerd zijn aan de vernieuwing IT.

**23**

**Zijn er naast de reservering van 40,2 miljoen euro voor de IT-infrastructuur ook al reserveringen gemaakt voor de vervolgstappen van de vernieuwing en modernisering van het gehele IT-domein van Defensie? Zo ja, voor welke bedragen?**

De reservering voor dubbele beheer, transitie en migratie is als risicoreservering opgenomen voor de overgangssituatie als zowel de huidige als de nieuwe IT-infrastructuur nog actief zijn. Deze omvat de € 40,2 miljoen, en is in de begroting 2017 aangevuld met € 117 miljoen (Kamerstuk 34 550 X, nr. 2). Vanwege het kort-cyclische karakter van IT-projecten is het

benodigde budget na 2020 op dit moment nog niet te ramen. Naarmate de tijd vordert, zijn projecten verder uitgewerkt. De concrete bedragen worden dan ingepast. In het kader van financiële duurzaamheid wordt momenteel onderzocht of in de investeringsbegroting met een vaste bandbreedte voor IT-uitgaven kan worden gewerkt waaruit projecten worden gefinancierd.

**24**

**Kunnen de uitkomsten van de dialoofase leiden tot een bijstelling van het begrote bedrag voor dubbele beheerslasten of ligt dat bedrag voor de komende periode vast?**

Uit de dialoog met de markt zal meer duidelijkheid ontstaan over de financiële gevolgen van de modernisering van de IT-infrastructuur en kan een steeds betere raming voor deze post worden opgesteld.

**25**

**In de laatste maanden van 2016 zouden nog eens veertien legacy-systemen worden uitgezet. Is deze uitfasering geslaagd?**

Van de veertien legacy-systemen zijn er inmiddels twaalf uitgezet. Voor de twee resterende systemen is de vervangende functionaliteit iets vertraagd. Deze zullen volgens de huidige planning uiterlijk in juni 2017 worden uitgefaseerd.

**26**

**Wanneer verwacht u de IT-infrastructuur uit te breiden naar operationeel gebruik in Nederland en het buitenland? Tot wanneer denkt u de beschikbaarheid van TITAAN te moeten garanderen?**

De planning is dat in 2019 wordt gestart met de uitbreiding naar operationeel gebruik. In overleg met de toekomstige leverancier zal de definitieve planning worden vastgesteld. Tot die tijd en gedurende de transitie zal de beschikbaarheid van TITAAN gegarandeerd moeten zijn. Dat gebeurt onder andere door tussentijdse updates, waarmee de technische levensduur wordt verlengd.

**27**

**Wat wordt bedoeld met de zinsnede dat het model, dat door de Algemene Rekenkamer is geïntroduceerd, is «aangepast aan de voorziene functionaliteiten»?**

In het algemeen overleg over IT, ERP en Sourcing van 5 juli 2016 (Kamerstuk 31 125, nr. 70) heeft u mij gevraagd om met behulp van het model van de Algemene Rekenkamer inzichtelijk te maken hoe de functionaliteiten van ERP in de verschillende domeinen zich verder ontwikkelen. De Algemene Rekenkamer heeft het model geïntroduceerd in haar brief over het programma SPEER aan de Tweede Kamer van 16 januari 2014 (Kamerstuk 31 460, nr. 39) om aan te geven welke processen wel en nog niet door ERP werden ondersteund. Daarbij zijn de processen verdeeld in vier lagen in afnemende mate van ondersteuning door ERP: Registreren (onderaan, volledig afgedekt door ERP), Beheersen korte termijn, Beheersen middellange termijn en Sturen (bovenaan, niet afgedekt door ERP). Dat model was een momentopname van de situatie begin 2014.

In de voortgangsrapportage is een geactualiseerde versie van dit model opgenomen. Enerzijds is het model uitgebreid met de financiële processen die door ERP worden ondersteund (vierde kolom naast



Materieel, Systeemlogistiek en Ketenlogistiek). Anderzijds zijn de opgenomen processen aangepast aan de huidige inzichten over de functionaliteiten die ERP nu en in de toekomst zal bieden.

**28**

**Welke gevolgen heeft het geven van prioriteit aan het werkend maken van huidige functionaliteiten op de planning van de ontwikkeling van nieuwe functionaliteiten?**

De nieuwe integrale bedrijfsvoering begint steeds meer voordelen op te leveren. Er is voor het eerst een integraal defensiebreed inzicht in de materieellogistiek, iets wat met de legacy-systemen voor de afzonderlijke krijgsmacht delen niet mogelijk was. Dit wordt bijvoorbeeld gebruikt bij het oplossen van de onvolkomenheid reservedelen, waar wordt gestuurd met behulp van een dashboard dat wordt gevuld met ERP-gegevens. Het is de bedoeling dat dit dashboard in de toekomst wordt uitgebreid, wat ten goede komt aan de beheersing op de middellange termijn en de integrale sturing.

Op verzoek van de defensieonderdelen is voor de korte termijn prioriteit gegeven aan het werkend maken van de huidige functionaliteiten boven het introduceren van nieuwe. De defensieonderdelen hebben momenteel hun handen nog vol aan de nieuwe bedrijfsvoering die ERP met zich meebrengt en aan het verbeteren van de materiële gereedheid van de wapensystemen. Het absorptievermogen van de materieellogistieke organisaties voor alle veranderingen is beperkt, zodat het nodig was om prioriteiten te stellen. Dat betekent niet dat er helemaal geen nieuwe functionaliteit wordt geïntroduceerd. Zo zal er de komende jaren meer worden geïnvesteerd in management informatie. Specifieke functionaliteiten ter ondersteuning van inzet zullen echter niet eerder dan 2018 in gebruik worden genomen.

**29**

**Is de F-16 inmiddels volledig gemigreerd?**

Ja, de F16 toestellen zijn volledig gemigreerd.

**30**

**Betreft de verdere optimalisatie van de migratie van het brandstoffenbedrijf in relatie tot het Caribisch gebied en het gebruik van de brandstofpas op defensielocaties een vertraging ten opzichte van eerdere plannen?**

Voor brandstof in het Caribisch gebied – dit gaat om circa 1 procent van de totale brandstofleveranties – is dit het geval. Bij de brandstofpassen op Defensielocaties is geen sprake van vertraging, maar van voortschrijdend inzicht. Het opnemen van deze functionaliteit in ERP zou in ERP maatwerk betekenen en niet bieden wat de gebruiker beoogt. Daarom wordt er momenteel naar een andere oplossing gezocht.

**31**

**In de voortgangsrapportage van 4 mei 2016 werd gemeld dat eind 2016 in totaal 42 legacy systemen zouden zijn ontmanteld. Kunt u toelichten waarom deze planning is aangepast naar 35 systemen, oplopend tot 39 in de eerste maanden van 2017?**

De uitfasering heeft enige vertraging. In de eerste maanden van 2017 zullen 39 van de 50 legacy systemen worden ontmanteld. Dat zijn drie systemen minder dan de planning in mei 2016. Voor deze systemen geldt

dat er vertraging is opgelopen in de oplevering van de vervangende functionaliteit.

### 32

**Wanneer is het gereed zijn van de functionaliteiten voor «beheersen op de korte termijn» gepland?**

### 33

**Wanneer is het gereed zijn van de functionaliteiten voor «beheersen middellange termijn» gepland?**

### 34

**Wanneer is het gereed zijn van de functionaliteiten voor «integraal sturen» gepland?**

De verschillende functionaliteiten hangen nauw met elkaar samen. Er is geen scherpe scheidslijn te trekken tussen deze functionaliteiten. Het model is vooral bedoeld om de samenhang inzichtelijk te maken. Om een voorbeeld te geven: beheersen op middellange termijn betreft het voorspellen van vraag en trends en het sturen daarop. Het realiseren hiervan zal niet eerder plaatsvinden dan 2019. Randvoorwaardelijk hiervoor is niet alleen historische data, maar ook alle onderhoudsplannen van wapensystemen. Deze dienen volledig en correct in ERP M&F te zijn weergegeven. Dat valt in de functionaliteit «registreren». Sturen op uitkomsten kan ertoe leiden dat de behoefte aan stuurinformatie wijzigt. Zoals uit de voortgangsrapportage blijkt, loopt de ontwikkeling van de verschillende functionaliteiten door tot na 2018.

	2016	2017	2018 e.v.
Registeren en beheersen korte termijn	<ul style="list-style-type: none"> <li>– Eind 2016 migratie F-16 en brandstoffen voltooid</li> <li>– 35 <i>legacy</i>-systemen uitgefaseerd</li> </ul>	<ul style="list-style-type: none"> <li>– Kennis en kunde ERP verder versterkt</li> <li>– Tool controle datainvoer ingericht</li> <li>– 4 <i>legacy</i>-systemen uitgefaseerd</li> <li>– Evaluatie SPEER afgerond</li> </ul>	<ul style="list-style-type: none"> <li>– 11 <i>legacy</i>-systemen uitgefaseerd</li> <li>– Functionaliteit munitie geïmplementeerd</li> <li>– Functionaliteit ondersteuning operationeel optreden geïmplementeerd.</li> <li>– Gebruikersschermen vereenvoudigd</li> </ul>
Beheersen middellange termijn	<ul style="list-style-type: none"> <li>– Begroting en voorafgaand toezicht in ERP geoptimaliseerd</li> <li>– Standaardrapportages en analyse tools ter beschikking gesteld</li> </ul>	<ul style="list-style-type: none"> <li>– Proces-indicatoren opgeleverd</li> </ul>	<ul style="list-style-type: none"> <li>– Proces-indicatoren opgeleverd</li> <li>– Tool vraagvoorspelling geoptimaliseerd</li> </ul>
Sturen	<ul style="list-style-type: none"> <li>– Dashboard materiële gereedheid gereed</li> <li>– Dashboard financiën gereed</li> </ul>	<ul style="list-style-type: none"> <li>– Dashboard inkoop ontwikkeld</li> </ul>	<ul style="list-style-type: none"> <li>– Functionaliteit simulatie opgeleverd</li> </ul>

### 35

**Welke factoren bepalen het tempo van het toevoegen van nieuwe functionaliteiten? Is het budget daarbij een beperkende factor?**

Het tempo van toevoegen nieuwe functionaliteiten wordt vooral bepaald door het verandervermogen van de logistieke organisatie en door de planning van operationele activiteiten. Het verandervermogen is in eerste aanleg nodig om de bedrijfsvoering te optimaliseren. Voor het implementeren van nieuwe functionaliteiten is minder ruimte.

Voor IT-aanpassingen wordt gewerkt met een bandbreedte van € 12 miljoen per jaar. Twee derde van dit geld wordt uitgegeven aan verbeteren van de datakwaliteit en de optimalisatie van de bedrijfsvoering met het huidige ERP M&F. Het overige deel wordt gebruikt voor de realisatie van nieuwe functionaliteiten.

### 36

**Wat houdt de controle van de ADR van de doorgevoerde maatregelen voor de continuïteit van IT precies in? Welke vragen onderzoekt de ADR?**

**37**

**Controleert de ADR ook de robuustheid van de maatregelen voor de toekomst in het licht van risico's, bijvoorbeeld verdere vertraging van de realisatie van de nieuwe IT-infrastructuur?**

**38**

**Wanneer kunt u de Kamer informeren over de uitkomsten van de controle van de ADR van de continuïteitsmaatregelen?**

De ADR is gevraagd te beoordelen op welke wijze de eerder vastgestelde continuïteitsmaatregelen zijn uitgevoerd, niet om de inhoud van die maatregelen zelf te beoordelen. De ADR controleert dus of terecht de status «gereed» aan de afzonderlijke maatregelen is toegekend. De robuustheid van de maatregelen en het onderkennen van nieuwe risico's is geen specifiek onderdeel van de onderzoeksopdracht.

In het jaarverslag 2016 en de volgende voortgangsrapportage IT en ERP, die de Kamer in mei 2017 zal ontvangen, zal ik de Kamer informeren over de uitkomsten van de controle van de ADR.

**39**

**Wat houdt de controle van de ADR van het autorisatiebeheer precies in? Welke vragen onderzoekt de ADR?**

**40**

**Wanneer kunt u de Kamer informeren over de uitkomsten van de controle van de ADR van de uitvoering van het plan voor verbetering van het autorisatiebeheer?**

De ADR voert een quick scan uit naar de voortgang van realisatie van het geactualiseerde actieplan autorisatiebeheer 2016. De centrale vraag in het onderzoek is: In welke mate zijn de producten van het actieplan autorisatiebeheer 2016 gerealiseerd?

In het jaarverslag 2016 en de volgende voortgangsrapportage IT en ERP, die de Kamer in mei 2017 zal ontvangen, zal ik de Kamer informeren over de uitkomsten van de controle van de ADR.