

Technische Marktconsultatie

“Defensie Ontwerp IT”

Datum: 29 juli 2015
Status: Definitief

Colofon

Ministerie van Defensie
Defensie Materieel Organisatie

Joint IV Commando
JIVC

Herculeslaan 1
2509 LV Utrecht

Contactpersoon	F.T. Akdeniz Tel. +31 683 645 203 technische.marktconsultaties.it@mindef.nl
Opdrachtgever	drs. R. Kolkman

Intellectueel eigendom

Het intellectueel eigendom van dit document en meegeleverde bijlagen ligt bij de Staat der Nederlanden, DMO/JIVC (hierna te noemen JIVC). Het is uitsluitend toegestaan dit document te kopiëren en te verstrekken voor eigen gebruik waaronder begrepen de door u binnen dit traject in te schakelen onderaannemers. Het verstrekken van dit document aan derden zonder voorafgaande schriftelijke toestemming JIVC is niet toegestaan. Op haar beurt zal de JIVC de door de respondent verstrekte informatie vertrouwelijk behandelen.

Utrecht, 29 juli 2015

“ Think big, act small!”

Bijgaand treft u de technische marktconsultatie van het Defensie Ontwerp IT in een 0.7 concept versie aan. Zoals velen van u hebben aangegeven wilt u vroegtijdig betrokken zijn bij ons ontwerp en de realisatie van onze nieuwe IT.

Niet achteraf geconfronteerd worden met de uitkomsten van een denkproces maar actief meedenken en meewerken aan de oplossing van de grensverleggende IT voor Defensie.

Defensie heeft er voor gekozen om te beginnen met een groeikern. Vanuit deze groeikern zullen er gaandeweg meer en sneller innovaties op de IT worden uitgevoerd. Dit past volledig binnen de door ons gevolgde filosofie “Think big, act small!”.

U wordt uitgedaagd om gezamenlijk het Defensie Ontwerp te vervolmaken, te komen tot die versie 1.0, te komen tot de realisatie van de groeikern medio 2016.

In deze marktconsultatie vindt u niet alleen vragen maar ook dilemma’s waar juist uw kracht als marktpartij een antwoord op kan geven. In kleine stappen, op weg naar het grote doel.

Wellicht kunt u niet alle vragen beantwoorden, maar mocht u een bijdrage denken te kunnen leveren, aarzel niet.

U wordt van harte uitgenodigd om de informatiebijeenkomst bij te wonen. De bijeenkomst vindt plaats op 4 augustus as op de Kromhoutkazerne te Utrecht.

Inhoudsopgave

1. Inleiding en doel van de technische marktconsultatie.....	5
2. Instructies voor beantwoording	8
3. Markt.....	9
3.1 Algemene Vragen	9
3.2 Kader voor inhoudelijke beantwoording	11
3.3 Focus - IT Beveiliging	12
3.4 Focus - IT Toepassingen.....	12
3.5 Focus - IT Infrastructuur.....	15
3.6 Focus - IT Rationalisatie.....	18
3.7 Focus - IT Management	18
Bijlage 1: (concept) Eindrapport Defensie Ontwerp IT V0.7	20
Bijlage 2: (concept) deelrapport A – Informatiebeveiliging V1.0.....	20
Bijlage 3: (concept) deelrapport B – IT Toepassingen V0.7.....	20
Bijlage 4: (concept) deelrapport D – IT Specificatie V0.7	20
Bijlage 5: Antwoordformulier	21
Bijlage 6: Afkortingen	22
Bijlage 7: Informatie inzake de reviewsessies.....	23

1. Inleiding en doel van de technische marktconsultatie

Defensie is naar aanleiding van de huidige situatie met betrekking tot haar IT een verbeterprogramma gestart onder de naam "Grensverleggende IV/ICT". De eerste belangrijke stap was het vaststellen van de nieuwe visie. Deze is uitgewerkt in "Let's make IT happen!". Vanuit deze visie is het Defensie High Level Ontwerp-IT (Defensie High-Level Ontwerp-IT; zie rijksoverheid.nl) voor Defensie opgesteld. De focus van het HLO ligt op het vertalen van de visie naar meer concreet te bereiken effecten van de nieuwe IT voor Defensie.

Het Concept Defensie Ontwerp IT (zie Bijlage 1: Concept Defensie Ontwerp IT versie 0.7, DoIT) is de eerste stap in het uitwerken van het HLO om te komen tot een samenwerking met de markt en het realiseren van de nieuwe IT voor Defensie. Deze documenten zullen de respondent helpen bij de beantwoording van de vragen zoals gesteld in de volgende hoofdstukken van deze technische marktconsultatie.

Haalbaarheidstoets

In nauwe samenwerking met Nederland ICT is in juni 2015 een ICT Haalbaarheidstoets op het HLO uitgevoerd. De resultaten van deze haalbaarheidstoets zijn inmiddels gepubliceerd. Zie: <http://www.nederlandict.nl/index.shtml?id=13924&ch=ICT>. Deze marktconsultatie borduurt voort op onderstaande hoofdonderwerpen uit de haalbaarheidstoets:

- de roep om meer gedetailleerde informatie over de richting die Defensie in wil slaan,
- het signaal dat in het HLO gekozen richtingen niet steeds aansluiten bij marktmogelijkheden en -ontwikkelingen en
- de vaststelling dat (nog) geen sprake is van een gezamenlijk taalgebruik.

Doel

Met de technische marktconsultatie beoogt het Ministerie van Defensie:

1. inzicht te krijgen in het antwoord op de vraag of het Defensie Ontwerp IT voldoende (technische) basis vormt om te kunnen starten met (een) realisatietraject(en);
2. te onderzoeken welke logische samenhangende (deel-)oplossingen de marktpartijen zien bij de realisatie zowel technisch als in relatie tot haalbaarheid, met een primaire focus op de groeikern;
3. materiaal te verzamelen voor de kwantitatieve businesscase(s) voor de groeikern met een doorkijk naar de verdere ontwikkelingen.
4. inzicht te krijgen in de mogelijke Design, Build, Finance, Maintain en Operate aspecten van de oplossingen die de markt kan bieden. Het wordt op prijs gesteld dat u basale doch voldoende informatie verstrekt over de beschikbare oplossingen. Dit is noodzakelijk voor het krijgen van een goed beeld over de mogelijkheden, beperkingen en globale kosten hiervan.
5. inzicht in hoe de markt een eventuele strategische en operationele samenwerking met JIVC ziet om de doelen in het concept Defensie Ontwerp IT (Do IT) zijn vervat te bereiken.

Brede scope

De onderhavige technische marktconsultatie heeft een brede scope waardoor u mogelijk, naast de verplicht te beantwoorden vragen, niet alle vragen kunt beantwoorden. In uw beantwoording kunt u de voor uw segment relevante vragen beantwoorden. De marktconsultatie verloopt schriftelijk. U kunt zich aanmelden via technische.marktconsultaties.it@mindef.nl. Het ministerie dankt u bij voorbaat voor alle moeite en inspanningen.

Reflectie

Naast de schriftelijke marktconsultatie worden marktpartijen in de gelegenheid gesteld om deel te nemen aan openbare sessies die geleid en georganiseerd worden door het Programma Vernieuwing IT.

Defensie nodigt alle marktpartijen uit om te reflecteren op DoIT met als doel om kennis bij marktpartijen in te zetten om het document klaar te maken voor besluitvorming binnen Defensie. Daartoe is een set met vragen opgesteld, waarvan de beantwoording die verrijking moet ondersteunen. In het verlengde van de uitgevoerde haalbaarheidstoets heeft Defensie ervoor gekozen om het bespreken van die vragen in een bijeenkomst te doen waarbij marktpartijen in staat gesteld worden om hun antwoorden te geven. Die bijeenkomst wordt uitgevoerd in een aantal electronic sessies.

De aanpak van deze sessies is zo georganiseerd dat steeds - op inhoud - samenhangende vragen in één sessie worden behandeld. Op het moment van publiceren van deze oproep zijn in ieder geval onderstaande sessies voorzien:

1. IT Management & IT Beveiliging;
2. IT Toepassingen;
3. IT Infrastructuur;
4. IT Rationalisatie.

Bij de uitvoering van de sessie geven deelnemers hun antwoorden/reacties op een zodanige wijze dat alle informatie met elkaar wordt gedeeld, maar dat voor de deelnemers onderling niet te herleiden is welke informatie door wie is geleverd. Defensie beschikt wel over de auteurs van de informatie.

Kort na afloop van de bijeenkomsten, wordt de verzamelde input bekend gemaakt zodat alle marktpartijen - dus niet alleen de deelnemers aan de sessies - kennis kunnen nemen van de geanonimiseerde input. Om deel te kunnen nemen aan deze sessies dient u zich uiterlijk 3 augustus as. aan te melden bij de heer v.d. Loo: <mailto:am.vd.loo@mindef.nl>. Zie bijlage 'Informatie inzake de reviewsessies'.

Planning

De planning van deze marktconsultatie is als volgt:

	Datum	Taak	Resultaat
Fase 1	28-07-15	Publicatie marktconsultatie en uitsturen document naar geïnteresseerden	Delen van dit document, inclusief bijlagen
Fase 2	04-08-15	Briefing proces Do IT en toelichting	
Fase 3	11-08-15	Sluitingsdatum en -tijd voor het stellen van vragen.	Vragen van geïnteresseerden ontvangen door JIVC
Fase4	17-08-15	Beantwoording van de vragen door JIVC	Beantwoording vragen aan geïnteresseerden
Fase 5	27-08-15	Ontvangst antwoorden/oplossingen van de geïnteresseerden door JIVC	
Fase 6	21-09-15	Evaluatie van de marktconsultatie en het concretiseren van het definitieve pakket van eisen	Duidelijk beeld van de eisen van het project
Fase7	Ntb	Voorbereiden verwerving strategieën	

Informatiebijeenkomst

Wij moedigen u aan om de informatiebijeenkomst op 4 augustus 2015 bij te wonen. Defensie zal in die bijeenkomst uitleg geven over deze procedure en toelichting verschaffen over de inhoud van de stukken en de achtergrond van de gestelde vragen. U wordt in de gelegenheid gesteld om vragen te stellen over de procedure, de vraagstelling en op de vraagstelling te reflecteren.

De informatiebijeenkomst zal worden gehouden op de Kromhoutkazerne te Utrecht, Gebouw V5 in de Waterliniezaal. Aanvang 15:00, verwacht einde 16:30.

2. Instructies voor beantwoording

Omwille van een efficiënte tijdsbesteding bij zowel JIVC als de respondenten wil JIVC graag een compact beschreven oplossing ontvangen. We willen u dan ook verzoeken om informatie die niet direct de kern van de oplossing (lees: vraag) raakt, als bijlage op te nemen en niet in het hoofddocument te verwerken.

Per vraag dient het antwoord op maximaal 2*A4 document aangeboden te worden. Bij uitzondering kunt u aan het antwoord een bijlage toevoegen van maximaal 10*A4. In hoofdstuk 3 en 4 zijn de vragen opgenomen die we graag beantwoord willen zien omdat ze de kern raken van deze marktconsultatie. Voor het hoofddocument verzoeken wij u gebruik te maken van het bijgevoegde antwoordformulier (Bijlage 5: Antwoordformulier). Op dit antwoordformulier treft u tevens algemene vragen over uw bedrijf die ingevuld dienen te worden.

Daarnaast zijn er vragen (de vragen in hoofdstuk 3.4 & 3.1 die altijd beantwoord moeten worden.

De beantwoording van de overige vragen is afhankelijk van de oplossingen die u kunt aanbieden.

Eisen aan de beantwoording

Respondenten dienen duidelijk de naam en adresgegevens van alle betrokken personen die optreden als vertegenwoordiger van hun organisatie aan te geven. De communicatie vindt bij voorkeur plaats via e-mail. Hierbij kan ook aangegeven worden welke vragen volgens geïnteresseerden leiden tot onjuistheden in de aanpak of niet op de geïnteresseerde van toepassing zijn.

Mocht u vragen hebben of onvolkomenheden constateren dan verzoeken we u vriendelijk per e-mail contact op te nemen. Schriftelijke vragen welke voor 12-08-2015 door respondenten per e-mail zijn gesteld, zullen op 17-08-2015 geanonimiseerd worden beantwoord. Elke respondent dient uiterlijk op 27-08-2015 om 17.00 uur een papieren en een elektronische versie van zijn bijdrage in. De elektronische documenten dienen leesbaar te zijn met de Microsoft Office 2003 suite of als PDF of als ODF te worden aangeleverd. De beantwoording van de antwoorden op deze marktconsultatie kan worden bezorgd bij:

Ministerie van Defensie/Defensie Materieel Organisatie
JIVC
T.a.v. mevrouw F.T. Akdeniz
Herculeslaan 1
2509 LV Utrecht

Mevrouw Akdeniz zal tevens optreden als enige contactpersoon voor de schriftelijke marktconsultatie JIVC en is te bereiken via:

Email: technische.marktconsultaties.it@mindef.nl
Telefoon: +316 83 64 52 03

Voorbehouden

Defensie hanteert een tweetal voorbehouden. Indien u wenst mee te werken aan deze marktconsultatie dient u in te stemmen met deze voorbehouden:

- Voorbehoud 1.2.a* JIVC vergoedt op geen enkele wijze kosten verbonden aan beantwoording van de vragen van deze marktconsultatie, of daaraan gerelateerde activiteiten.
- Voorbehoud 1.2.b* JIVC houdt zich het recht voor om geen vervolg te geven aan deze marktconsultatie.

3. Markt

Leeswijzer

In dit hoofdstuk zijn de vragen opgenomen. De indeling van de vragen is vanaf paragraaf 3.3 gebaseerd op de in bijlage 1, 2, 3 en 4 gevoegde documenten. De vragen zijn zodanig dat enerzijds een verificatie op het Defensie Ontwerp IT kan plaatsvinden en anderzijds er informatie beschikbaar komt om de eisen van de groeikern te vervolmaken.

Reflectievragen

Deze vragen ter reflectie op het Defensie Ontwerp IT zijn gesteld ten behoeve van de sessies op 11 en 12 augustus 2015 (zie publicatie Tendered op 28 juli j.l.). Wij stellen het zeer op prijs indien u de beantwoording van deze vragen onderdeel laat uitmaken op uw reactie op de technische marktconsultatie.

1. Wat is uw 'expert opinion' van het Defensie Ontwerp IT in het algemeen en de groeikern in het bijzonder?
2. Welke onderdelen van het Defensie Ontwerp IT / Groeikern vindt u goed?
3. Welke onderdelen van het Defensie Ontwerp IT / Groeikern kunnen verbeterd worden?
4. Welke 'witte vlekken' ziet u in het Defensie Ontwerp IT / Groeikern?
5. Welke logische stappen zou u voorstellen; kunt u daarbij specifiek inzoomen op de realisatie van de groeikern?
6. In hoeverre acht u de ambitie van Defensie beschreven in het Defensie Ontwerp IT haalbaar?
7. Hoeveel tijd schat u in dat nodig is om de gewenste groeikern te realiseren?
8. Hoe zou volgens u de governance over IT vorm moeten krijgen onder de voorwaarden zoals geschetst in het Defensie Ontwerp IT?
9. Zijn de geformuleerde ambities van het Defensie Ontwerp IT vanuit het oogpunt IT Beveiliging realistisch?
10. Zijn de in het Defensie Ontwerp IT gehanteerde set aan beheer- & ontwikkel standaarden en frameworks marktconform, zo nee; welke aanpassingen adviseert u?
11. Gaat Defensie volgens u met de in het Defensie Ontwerp IT beschreven rationalisatie methodiek zijn ambitie realiseren, zo nee; welke aanpassingen adviseert u?
12. Welke kansen en mogelijkheden ziet u om het proces van rationalisatie en migratie te versnellen?

3.1 Algemene Vragen

Onderstaande vragen binnen deze paragraaf dienen altijd beantwoord te worden. Defensie zoekt naar een samenwerkingsvorm met de markt waarbinnen kort cyclisch gewerkt kan worden. Defensie denkt dat het niet langer haalbaar is om volledige specificaties vooraf te definiëren om die met resultaatverplichting in de markt te zetten. Defensie wil echter ook niet alleen uren van de markt afnemen en alles zelf ontwerpen, bouwen en beheren. Het leveren van IT die naadloos past in het operationele proces betekent dat er heel veel domeinkennis nodig is, en dus een nauwe samenwerking tussen Defensie en leveranciers.

- Vraag 3.1.1 Is dit een haalbare wens van Defensie vanuit uw oogpunt?
Kunt u voorbeelden geven van samenwerkingen die voldoen aan bovenstaande wensen waarin u bent betrokken?
In een dergelijke samenwerking moeten de belangen van Defensie en de partner beiden geborgd zijn. Hoe kan dit het beste geborgd worden?*

Defensie zal hoog gerubriceerde systemen en systemen die worden ingezet in operationele omstandigheden altijd zelf moeten kunnen beheren. Dat betekent dat alle IT beslissingen afgestemd moeten zijn met de eisen van het hoog gerubriceerde en het operationele domein. Afstemming moet bijvoorbeeld plaatsvinden over benodigde opleidingen en kennis van Defensiepersoneel, de geschiktheid voor lage bandbreedtes in het mobiele en uitgestegen domein, en de geschiktheid om te voldoen aan de beveiligingseisen van het hoog gerubriceerde domein.

Vraag 3.1.2 Hoe zou volgens u de governance over IT beslissingen moeten plaatsvinden zodanig dat ze zowel de Defensiebelangen als de belangen van de partners recht doen? Kunt u aangeven op welke manier de verantwoordelijkheden tussen Defensie en de markt moeten worden verdeeld in het kader van beheer en beveiliging? Heeft u voorbeelden van dergelijke samenwerkingen?

Defensie moet onder alle omstandigheden met IT de primaire taken van de krijgsmacht ondersteunen. Afhankelijk van de (politieke)situatie kan het zijn dat bepaalde IT services meer of minder gebruikt worden of dat er meer of minder (buitenlandse) missies zijn. Defensie zoekt daarom een partner die op basis van prestatie afspraken snel capaciteit bij kan schakelen indien performance of capaciteit onder druk komen te staan. Het opschalen en afbouwen moet dus "on-the-fly" mogelijk zijn.

Vraag 3.1.3 Hoe denkt u als partner van Defensie te kunnen acteren op het gebied van (proactief) capaciteit- en performance management? Bent u in staat om op basis van een prestatie contract, binnen een bepaalde bandbreedte, de capaciteit en performance van de Defensie IT op peil te houden? Heeft u hier referenties van bij andere klanten?

Vraag 3.1.4 Bent u in staat om infrastructuur hard- en software terug te nemen of anders in te zetten indien de vraag vanuit Defensie afneemt?

Vraag 3.1.5 Hoe denkt u bij te kunnen dragen aan de logistiek rondom nieuwe missies, waarbij op zeer korte termijn IT middelen klaargemaakt moet worden voor een missie?

Defensie wil graag met een samenspel van kennisinstituten en bedrijven samen aan de nieuwe IT werken. Daarbij wil Defensie expliciet de ruimte hebben om met kleine innovatieve bedrijven te werken.

Vraag 3.1.6 Op welke wijze kan dit het beste worden ingevuld? Hoe moet de regie tussen de verschillende partners geregeld worden vanuit uw optiek?

De invulling van het Defensie Ontwerp IT vraagt van de organisatie zowel een innovatieve/agile modus als een beherende modus (ook wel type 1 of type 2 mode organisatie genoemd).

Vraag 3.1.7 Welke competenties zijn hiervoor benodigd? Is de combinatie van een type 1 of type 2 mode binnen één organisatie gebruikelijk in de markt? Zo ja, kunt u daar voorbeelden van geven? Welke consequenties heeft het Defensie Ontwerp IT volgens u op de kwantiteit en kwaliteit (capaciteiten en competenties) van het Defensiepersoneel?

Vraag 3.1.8 Op welke wijze geeft u inhoud aan de samenwerking tussen uw personeel en het personeel van Defensie.

Vraag 3.1.9 Welke risico's ziet u in de realisatie van de IT in het algemeen en de groeikern in het bijzonder, welke kritische succesfactoren en lessons learned?

Conform het kabinetsbeleid moet de IT omgeving van Defensie worden gerealiseerd door gebruik te maken van Open Standaarden. Voor de Rijksoverheid geldt bij ICT-opdrachten (JIVC en aanbestedingen) vanaf 2 april 2008 het "comply-or-explain and commit"-principe voor het toepassen van open standaarden bij nieuwbouw, verbouw of contractverlenging. Om een vendor lock-in situatie voor JIVC zo veel mogelijk te voorkomen dient de oplossing zoveel als mogelijk gebaseerd te zijn op open standaarden.

Vraag 3.1.10 Maakt uw oplossing volledig gebruik van breed geaccepteerde open standaarden of zijn delen leverancier specifiek?

- Vraag 3.1.11 Indien delen leverancier specifiek zijn, welke standaarden en leverancier specifieke onderdelen betreft het hier?*
- Vraag 3.1.12 Het kiezen voor open source software zou kunnen betekenen dat er software gekozen wordt waar geen leverancier achter zit die de benodigde support kan leveren. Op wat voor manier kunt u organiseren dat Defensie daar niet door gehinderd worden?*
- Vraag 3.1.14 Welke bandbreedte in kosten voorziet u in realisatie van uw (deel)oplossing binnen de groeikern? Kunt u deze kosten specificeren in zowel eenmalige als terugkerende kosten?*
- Vraag 3.1.15 Wat zijn globaal de eenmalige en jaarlijkse kosten voor de aanschaf, bouw, garantie en onderhoud van uw (deel)oplossing?*
- Vraag 3.1.16 Kunt u aangeven hoe de prijs wordt opgebouwd per (deel)oplossing.*
- Vraag 3.1.17 Zijn er naast koop ook mogelijkheden zoals leasing en/of huur en biedt u daarnaast nog andere financiële constructies die mogelijk interessant kunnen zijn voor JIVC?*
- Vraag 3.1.18 Hoe zou het streven naar verlaging van de kosten in de samenwerkingsvorm geregeld moeten worden zodanig dat het de belangen van beide partijen dient? Ziet u mogelijkheden om de (hoge) licentiekosten te verlagen? Hoe zou een samenwerkingsvorm moeten omgaan met ideeën voor kostenverlagingen die vanuit Defensie komen zodanig dat er een kostenbesparing gehaald wordt, maar dat ook uw belangen gediend worden?*

3.2 Kader voor inhoudelijke beantwoording

Dit is het te hanteren kader voor de inhoudelijke beantwoording van de vragen met betrekking tot de (deel)oplossing.

3.2.1 De functionaliteit(en) van de oplossing(en);

op welke wijze de (deel-)oplossing naar uw mening voldoet aan de in het HLO en DoIT beschreven uitgangspunten en eisen waarbij u uitspraken doet over:

3.2.2 de leverbaarheid als 'informatiedienst', inclusief de granulariteit van de diensten;

3.2.3 de beschikbaarheid in alle beschreven gebruiksomstandigheden ('SOMUT');

3.2.4 de wijze waarop uw (deel-)oplossing kan voldoen aan de beveiligingseisen zowel in niet gerubriceerde domein als in het LGI en HGI-domein;

3.2.5 de mate waarin uw oplossing gebruik maakt van open standaarden en voldoet aan de standaarden die Rijksbreed door het College Standaardisatie zijn vastgesteld;

3.2.6 in hoeverre Defensie met de oplossing zou kunnen werken zonder maatwerk aanpassingen;

3.2.7 de mate waarin uw oplossing bruikbaar is in situaties waarin Defensie een missie uitvoert (beperkte of geen netwerk connectiviteit).

3.3 Focus - IT Beveiliging

- Vraag 3.3.1 *Hoe of waarmee borgen we:*
- De vereiste beschikbaarheid van IT ten tijde van grootschalige crises en duurzame maatschappelijke ontwrichting.
 - De vereiste exclusiviteit bij het beschermen van staatsgeheimen rekening houdend met het daderprofiel
 - De vereiste integriteit van informatie zodat Defensie verantwoording kan afleggen en superieure informatiepositie heeft ten opzichte van tegenstanders.
- Vraag 3.3.2 *Zijn geformuleerde ambities van het Defensie Ontwerp It vanuit het oogpunt IT beveiliging realistisch? Welke risico's onderkent u bij de realisatie van het Defensie Ontwerp IT en welke randvoorwaarden zouden hierbij door Defensie ingevuld moeten worden Vanuit het oogpunt IT beveiliging? Heeft u (marktconforme) voorstellen hoe bovengenoemde risico's gemitigeerd kunnen worden?*
- Vraag 3.3.3 *Welk invoeringsscenario draagt vanuit het oogpunt IT beveiliging het beste bij aan de doelen "think big, act small" en "move fast and take numerous small steps"?*
- Vraag 3.3.4 *Is het combineren van niet, laag en hoog gerubriceerde informatie verwerkende applicaties mogelijk binnen één Workspace, rekening houdend met eisen aan IT Beveiliging? Zo niet, op welke punten raadt u aan het Defensie Beveiligingsbeleid te wijzigen en tegen welke restrisico's om diverse rubriceringen wel te kunnen combineren binnen één Workspace?*
- Vraag 3.3.5 *Hoe voorkomt de Workspace lekken van informatie van infrastructuur voor hoger gerubriceerde informatie naar infrastructuren voor niet en lager gerubriceerde informatie? Hoe faciliteer je het gebruik van verschillend gerubriceerde en publieke (of privé) informatie binnen één Applicatie, waarbij de gegevens uit verschillende bronnen komen? Hoe zijn publieke Applicaties op de Workspace te delen met federatieve Applicaties Services van Defensie en partners? Moet Defensie eisen stellen aan (publieke) Applicaties Services voor gebruik binnen de Defensie Workspace? Zo ja, welke?*

3.4 Focus - IT Toepassingen

Cluster User Facing Capabilities

- Vraag 3.4.1 *Hoe ziet u de persoonlijke- en/of taakgerichte werkomgeving van de gebruikers en op welke manier zou u hieraan een invulling kunnen geven binnen de Groeikern?*
- Vraag 3.4.2 *Welke invulling kunt u geven aan een geïntegreerd platform van productiviteits-, samenwerkings- en social media tooling voor de Groeikern?*
- Vraag 3.4.3 *Welke invulling kunt u binnen de Groeikern geven aan Unified Communications?*
- Vraag 3.4.4 *Het doel is Crossdomain gateways te gebruiken om federatieve samenwerking met partners te realiseren. Hoe zouden de federatieve koppelingen eruit moeten zien? Welke beveiligingscomponenten moeten er in zitten? Hoe zit de federatieve samenwerking uit? Hoe kunnen we de gebruikers identiteit geheim houden, terwijl we de communicatie willen stimuleren en federatief willen samenwerken? Hoe ziet de architectuur van UC uit o.b.v. geheimhouding/anonimiseren van informatie uit?*
- Vraag 3.4.5 *Op welke manier kunt u, ter ondersteuning van de operationele besluitvorming, binnen de Groeikern, een invulling geven aan het (Business) Operational Picture concept?*

Cluster COI en Core Services

- Vraag 3.4.6 *Welke invulling van generieke Geospational services voorziet u en zijn noodzakelijke om een geografische informatie infrastructuur architectuur mogelijk te maken ter ondersteuning van de gewenste IT-toepassingen?*
- Vraag 3.4.7 *Composition Services. Op welke wijze zou volgens u, binnen de groeikern, compositie services kunnen en moeten worden ingezet?*
- Vraag 3.4.8 *Welke standaard proces- en casemodellen voorziet u in de Groeikern? Hoe ziet u de ontwikkeling rondom casemanagement in een organisatie als Defensie?*
- Vraag 3.4.9 *Hoe ziet u vanuit de orchestration de aansluiting met taakgericht werken?*
- Vraag 3.4.10 *Hoe ziet u de invulling van de modelleer tooling in relatie tot "design- is- run" concept?*

Information Management Services

- Vraag 3.4.11 *Op welke wijze kunt u invulling geven aan een (generieke) zoekarchitectuur binnen de groeikern?*
- Vraag 3.4.12 *Hoe ziet u de invulling van een (big data) analytics architectuur binnen de groeikern?*
- Vraag 3.4.13 *Hoe kan een acceptabele doorlooptijd van het hele analytics proces worden bereikt? (Van verzamelen, via verwerken tot het opstellen van een bruikbaar eindproduct. In sommige operationele processen is realtime de norm).*
- Vraag 3.4.14 *Hoe ziet u binnen de groeikern, een architectuur voor opslag en verwerking van streaming data? Hoe kan die data gecombineerd worden met minder fluïde data?*
- Vraag 3.4.15 *Met welke processen en algoritmes kunt u efficiënt en snel relevante informatie uit beeldinformatie afleiden, zodat de ruwe data alleen nog voor verificatie gebruikt hoeft te worden? Welke technologie voor hoogwaardige geautomatiseerde ondersteuning van analyse van (beeld)informatie, t.a.v. herkenning/classificatie, identificatie, gedrags/intentieherkenning en tracking over meerdere sensoren heen, is naar uw mening beschikbaar voor gebruik in de Groeikern? Kunnen binnen de groeikern, algoritmes voor beeldanalyse ook zinvol toegepast worden op bijvoorbeeld radar- of sonarplots en Search and Rescue (SAR)-beeldinformatie?*
- Vraag 3.4.16 *Welke bijdragen kunt u leveren op het gebied van Data Analytics services? Hoe en op welke manier kunt u, binnen data analytics, de integriteit van data en informatie garanderen die een complex stelsel van bewerkingen en services heeft doorlopen? Hoe kan volgens u, binnen data analytics, de exclusiviteit van data en informatie blijvend gegarandeerd worden in een omgeving waar een verscheidenheid van bron data, met wisselend vertrouwelijkheidsniveaus en doelbinding, wordt samengebracht en continu wordt gecorrigeerd/gecombineerd? Hoe ziet u dat ad-hoc query op data kan worden toegestaan binnen data analytics?*
- Vraag 3.4.17 *Welke eisen kunnen gesteld worden aan IT-toepassingen, zodat data aanwezig binnen de IT-toepassing geanalyseerd kan worden binnen Analytics Services? Welk groeipad ziet u om, ondanks de verschillende vormen van data en analysetechnieken, toch te komen tot een coherent geheel van Data Analytics Services? Hoe zou u de eisen formuleren die aan de onderliggende infrastructuur gesteld moeten worden om de verschillende vormen van data analyse te kunnen faciliteren?*
- Vraag 3.4.18 *Welke taalgerichte technologie is volgens u nodig om "taalonafhankelijk" tekstanalyse te kunnen uitvoeren?*
- Vraag 3.4.19 *Hoe kan Defensie een taxonomie van de begrippen beheren en beheersen?*

- Vraag 3.4.20 *Hoe ziet u dat Defensie binnen de groeikern haar service inventory het beste kan inrichten (inclusief Governance) rekening houdend met de omvang en complexiteit van de Defensieorganisatie?*
- Vraag 3.4.21 *Hoe ziet u de implementatie van bedrijfsregels binnen de groeikern? Hoe ziet u de aansluiting met architectuur op het gebied van Business Rule Management (BRM) en het dagelijks beheer van de uitvoer van bedrijfsregels?*
- Vraag 3.4.22 *Hoe ziet u de Master Data Management-architectuur binnen de groeikern en welke methode van high precision matching wordt daarbij meegenomen? Hoe ziet u Master Data Management (MDM) in een omgeving waarbij Defensie data heeft c.q. gebruikt uit zowel de private cloud, public cloud en tevens gebruik maakt van SAAS uit "een cloud" waarbij het essentieel is dat de informatie tussen de verschillende toepassingen "in sync" moet zijn?*
- Vraag 3.4.23 *Hoe ziet u hoe omgegaan moet worden met gelijktijdige wijzigingen op dezelfde data in meerdere systemen en bronnen? Welke architectuuroplossing voorziet u en met welk beheerinstrumentarium kunt u dit invullen? Welke eisen stelt naar uw mening Master Data Management (MDM) aan de legacy IT-toepassingen? Welke rol ziet u weggelegd voor Master Datamanagement bij het beheren van historische data?*
- Vraag 3.4.24 *Hoe ziet u de realtime en batch synchronisatie van data binnen de groeikern? Hoe ziet u binnen de Groeikern het invullen van Data Quality Management (DQM) en bijbehorend Data Governance?*

Enterprise Support SMC Services

- Vraag 3.4.25 *Hoe ziet u binnen de groeikern, de manier waarop Defensie haar DML (Definitive Media Library) het beste kan inrichten?*
- Vraag 3.4.26 *Hoe ziet u de manier waarop Defensie de DEASS (Defensie Enterprise Applicaties Store Services) op een efficiënte en effectieve manier kan inrichten, rekening houdend dat ook andere organisaties dan Defensie er gebruik van moeten kunnen maken? Wat zijn naar uw mening de basiscomponenten die voor een toekomst vaste Defensie Enterprise Applicaties Store (DEAS) benodigd zijn? Hoe zien naar uw mening de koppelingen vanuit DEASS naar de DML eruit?*

Message Oriented Middleware Services and Mediation Services

- Vraag 3.4.27 *Hoe ziet u binnen de groeikern de benodigde Message Oriented Middleware Architectuur?*
- Vraag 3.4.28 *Hoe ziet u de rol van deze Message Oriented Middleware en Mediation services in relatie tot het uitwisselen sensor informatie?*
- Vraag 3.4.29 *Hoe ziet u de rol van Message Oriented Middleware services in relatie met het ontsluiten van de legacy IT-toepassingen?*
- Vraag 3.4.30 *Hoe ziet u binnen de groeikern de Enterprise Service Bus (ESB)?*

ERP Services

- Vraag 3.4.31 *Hoe ziet u de ontwikkeling van ERP systemen naar ERP services? Hoe ziet u de overgang van ERP systemen naar de invoering van ERP services?*
- Vraag 3.4.32 *Welke standaard ERP Services, op het gebied van Financiën, Organisatie, Personeel, Ketenlogistiek, Systeemlogistiek en Project en Procesmanagement, ziet u in de markt?*
- Vraag 3.4.33 *Hoe ziet u dat de huidige ERP systemen die Defensie in huis heeft (PeopleSoft en SAP), optimaal kunnen samenwerken met de groeikern?*

Web Platform Services

Vraag 3.4.34 Hoe ziet u, voor de Groeikern de inrichting van een toekomstvast webplatform dat de nieuwe IT-infrastructuur ondersteunt en met welke componenten kunt u hier aan bijdragen?

Cluster Hybrid Integration Platform en Externe Services

Vraag 3.4.34 Hoe ziet u, de inrichting van een Hybride Integration Platform voor Defensie, waarbij sprake is van on-premise gehoste diensten en public gehoste clouddiensten?

Vraag 3.4.35 Kunt u aangeven hoe een naadloze samenwerking tussen on-premise gehoste diensten en public gehoste diensten op de nieuwe IT Infrastructuur van Defensie wordt gerealiseerd en ondersteund?

Vraag 3.4.36 Welke eisen stelt, volgens u, een hybride cloud aan de private cloud t.a.v. het koppelvlak?

Vraag 3.4.37 Hoe ziet u de mogelijkheden van iPaas voor de Defensie?

Ontsluiten legacy toepassingen

Vraag 3.4.38 Welk scenario met bijbehorende techniek voorziet en acht u het meest toepasbaar om bestaande IT-toepassingen c.q. data vanuit de nieuwe IT-infrastructuur te ontsluiten, zonder vergaande aanpassingen aan de toepassingen te moeten doorvoeren:

- 1. Bij ontsluiting waarbij de IT-toepassing c.q. data op de huidige IT-infrastructuur blijft staan.*
- 2. Bij ontsluiting waarbij de IT-toepassing c.q. data op de nieuwe IT-infrastructuur binnen het migratie domein wordt geplaatst.*

Vraag 3.4.39 Welke technieken geven de beste ontsluitingsmogelijkheden, gelet op de toepassing van Service Oriented Architecture (SOA) in de nieuwe IT-infrastructuur, en toekomstvastheid? Welke criteria kunnen worden gebruikt om te bepalen welk scenario voor ontsluiting het meest geschikt is voor een IT-toepassing? Welke (migratie) scenario's kunnen worden gebruikt voor het daadwerkelijk ontsluiten en welke voor- en nadelen hebben deze scenario's?

Vraag 3.4.40 Welke technieken zijn volgens u het meest geschikt als voorbereiding op een eventuele herbouw van een toepassing, waarbij volledige inpassing in het nieuwe SOA IT-infrastructuur wordt beoogd?

3.5 Focus - IT Infrastructuur

Algemeen

Vraag 3.5.1 Zijn de ambities t.a.v. IT infrastructuur realistisch? Welke risico's kunt u identificeren? Welke maatregelen stelt u voor om deze risico's te mitigeren? Welke randvoorwaarden moeten aanwezig zijn om de ambitie te kunnen realiseren? Welke scenario stelt u voor bij het realiseren van de ambitie?

Vraag 3.5.2 Het ontwerp van de groeikern binnen de IT-infrastructuur gaat uit van loosely coupled componenten. Hoe garandeert u dat de componenten in een brokerplatform dermate interoperabel zijn dat uitwisseling voor een beter passend component eenvoudig kan worden uitgevoerd of dat componenten onafhankelijk van elkaar kunnen worden geüpgraded zonder de continuïteit aan te tasten?

Vraag 3.5.3 Hoe borgt u dat de IT infrastructuur vanaf de groeikern voortdurend mee kan bewegen met de technologische ontwikkelingen in de markt? Dit betekent ook dat Defensie gebruik kan maken van innovaties buiten uw organisatie. Hoe borgt u dat de IT voortdurend mee kan bewegen met de veranderende behoeftes vanuit Defensie? Hoe borgt u dat de IT voortdurend mee kan bewegen met het veranderende dreigingsbeeld in de wereld? Denk hierbij aan de toenemende mate van samenwerking met derden.

Werkplekken

- Vraag 3.5.4 Geeft het onderscheid tussen Workspaces en Devices voldoende houvast om uitspraken te doen over de invulling onder diverse omstandigheden? Heeft u ervaring met het invullen van Workspaces voor de verwerking van verschillend gerubriceerde informatie? Heeft u praktijkvoorbeelden op basis van gegeven omschrijving van Workspaces?*
- Vraag 3.5.5 Heeft u praktijkvoorbeelden waardoor een any device en any workspace als model toepasbaar is? Wat raadt u aan om essentiële legacy (Windows) applicaties aan te kunnen bieden op een zo breed mogelijk portfolio van Devices? Welke voorwaarden aan Devices garanderen ondersteuning van een zo breed mogelijk portfolio van services en applicaties?*
- Vraag 3.5.6 Hoe ziet u de ontwikkelingen in de komende 5 jaar op device gebied in de breedste zin van het woord, dus ook met sensor en wapensystemen? Hoe ziet u het toenemend gebruik van sensoren als Devices? Hoe ziet u het toenemend gebruik van wearable Devices? Hoe ziet u de deployment van Devices (denk aan Self Service en rechtstreekse levering door de markt maar ook aan zaken zoals locatie versus persoonsgebonden en in Nederland versus daarbuiten). Hoe ziet u de deployment van software en configuraties naar verschillende Devices? Hoe ziet u het automatisch installeren en handhaven van policies op diverse Devices?*
- Vraag 3.5.7 Welke oplossing stelt u voor bij draadloos werken, rekening houdend met de eisen vanuit IT Beveiliging? Is deze oplossing wat u betreft, conform beveiligingseisen, toepasbaar bij verwerking van data met iedere rubricering (met eventueel additionele maatregelen)? Zo niet, wat zijn de restrisico's? Welk mechanisme stelt u voor?*
- Vraag 3.5.8 Ziet u verschillen tussen het gebruik van persoonsgebonden en locatie gebonden Devices? Is dit, conform beveiligingseisen en toepasbaar bij iedere rubricering (met eventueel additionele maatregelen)? Zo niet, wat zijn de restrisico's? Welk mechanisme stelt u voor? Hoe ziet u het gebruik van sterke authenticatie bij het gebruik van persoonlijke devices (bijvoorbeeld smartcards bij onder andere smartphones en tablets)? Is dit, conform beveiligingseisen, toepasbaar op bij iedere rubricering (met eventueel additionele maatregelen)? Zo niet, wat zijn de restrisico's?*
- Vraag 3.5.9 Hoe zou u het onderscheid in managed/unmanaged voorstellen in relatie tot de diverse rubriceringscompartimenten waartoe een device toegang moet kunnen hebben? Kan een gebruiker bijvoorbeeld zelf een publieke app installeren op een managed device of is deze optie geheel dichtgezet en is deze niet beschikbaar voor de gebruiker? Hoe beheert u persoonsgebonden devices over verschillende rubricering domeinen heen?*
- Vraag 3.5.10 Welk mechanisme stelt u voor om draagbare gegevensdragers te beveiligen? Welk mechanisme stelt u voor om cliënts tegen gegevensdragers (en willekeurige andere peripheral devices) te beveiligen (denk aan kwetsbaarheid "Bad USB")? Is dit, conform beveiligingseisen, toepasbaar op bij iedere rubricering (met eventueel additionele maatregelen)? Zo niet, wat zijn de restrisico's? Welke mogelijkheden ziet u tot het draadloos verbinden van randapparatuur (Smart Office)? Ziet u hiervoor beperkingen in het verwerken van gerubriceerde of gemerkte informatie? Zo ja, welke?*

Koppelingen

- Vraag 3.5.11 *Is het aan te bevelen om één guard te hanteren voor alle koppelpunten (kostenreductie door standaardisatie) of toch per rubriceringsniveau aparte guards te gebruiken? De eisen aan de guard zijn bepaald op basis van extern vastgestelde kaders en protection profiles (zoals nationaal Beveiligings Autoriteit, NATO Security Authority). Aan welke eisen kan een invulling worden gegeven? Zijn er door NATO gecertificeerde guards dan wel gecertificeerde componenten beschikbaar voor een cross domain gateway (Secret – Unrestricted)?*
- Vraag 3.5.12 *Zijn er oplossingen die voor controle van datastromen via de gateway gebruik maken van data labels ter controle van de datastroom?*

Datacenters

- Vraag 3.5.13 *Wat is volgens u de meest optimale datacenter architectuur (inclusief topologie) voor de groeikern, rekening houdend met traditionele (scale-up) en moderne (scale-out) IT-toepassingen waarbij u een advies geeft over:*
- 1. Het aantal modules;*
 - 2. De inrichting (TIER niveaus conform uptime institute);*
 - 3. De locaties ten opzichte van elkaar (afstanden, bandbreedtes).*
- Vraag 3.5.14 *Hoe denkt u vorm te kunnen geven aan de invulling van het modulaire datacenter concept van de groeikern, wat snel op- en af kan schalen, voor zowel statische als ontplooiende datacenters voor verwerking en opslag van zowel hoog- als laag gerubriceerd informatie en hoog beschikbaar?*
- Vraag 3.5.15 *Hoe denkt u vorm te kunnen geven aan de behoefte aan toenemende opslag vraag, zowel voor real-time analyse van (big)data als voor betrouwbare archivering van oudere data?*
- Vraag 3.5.16 *Hoe denkt u vorm te kunnen geven aan de benodigde rapid deployment mogelijkheid, voor zowel statische als ontplooiende datacenters, waarbij herbruikbaarheid van methodes en configuraties over alle rubriceringen en omstandigheden heen mogelijk wordt?*
- Vraag 3.5.17 *Hoe denkt u vorm te kunnen geven aan de behoefte om autonoom te kunnen werken in geval van(tijdelijk) slechte of ontbrekende verbinding tussen de gedistribueerde datacenter modules (statisch en ontplooid)?*
- Vraag 3.5.18 *Hoe denkt u vorm te kunnen geven aan de ambitie om via een private cloud naar een hybride cloud model te groeien, waarin externe cloud diensten op basis van open standaarden in het Defensie netwerk kunnen worden toegelaten? Hoe ziet u de eerste stap naar een private cloud, rekening houdend met de eerder genoemde verdeling in traditionele (scale-up) applicaties en moderne (scale-out) applicaties?*
- Welke middelen kunt u bieden om de regie (cloud broker rol) die benodigd is voor een hybride cloud model goed in te kunnen vullen? Over welke standaarden (open en proprietary) dient de defensie private cloud te beschikken voor interoperabiliteit in een hybrid cloud omgeving (en/of community clouds). De hybrid cloud kan publieke, NATO, Overheids clouds omvatten.*

Netwerken

- Vraag 3.5.19 *Welke oplossingen bestaan er om breedbandige Transmission Services te leveren binnen OMUT omstandigheden voor zowel binnen 'line of sight' en 'beyond line of sight' waarbij 'time-to-move 0' is?*

- Vraag 3.5.20 Op welke wijze kan er horizontale in plaats van verticale integratie tussen netwerken plaatsvinden waardoor Quality of Service (QoS) en dynamische schaalbaarheid over de gehele keten kan plaatsvinden?*
- Vraag 3.5.21 Op welke wijze kan invulling gegeven worden aan een netwerk dat aanpasbaar is op wijzigende operationele omstandigheden met minimale beheerinspanning? En, wat is de resterende beheerinspanning? De wijzigende operationele omstandigheden betreffen:*
- *Initiële uitrol van het netwerk;*
 - *Opschalen en terugbrengen van het aantal werkstations;*
 - *Opschalen en terugbrengen van het aantal locaties;*
 - *Verplaatsen van eenheden wat leidt tot verandering in de netwerktopologie en verplaatsing van gebruikers en lokale datacenters;*
 - *Opschalen en terugbrengen van de datacentercapaciteit.*
- Vraag 3.5.22 Welke mogelijkheden zijn er om schaarse bandbreedte optimaal te benutten; gebruik te maken van parallelle verbindingen en prioriteit te geven aan bedrijfskritische gegevens (deze kunnen wisselen tijdens een operatie)?*

3.6 Focus - IT Rationalisatie

Vragen in relatie tot rationalisatie en migratie dienen om de witte vlekken af te dekken en de haalbaarheid te toetsen. De vragen liggen in de opbouw van de basisregistratie, de informatie over IT-toepassingen en IT-infrastructuren en principes die benodigd zijn om goede en haalbare rationalisatie beslissingen te nemen, die uitvoerbaar zijn.

- Vraag 3.6.1 Hoe ziet de markt een basisadministratie IT-toepassingen die Defensie kan ondersteunen bij rationalisatie en migratie? Hierbij rekening houdend met de vele generieke en specifieke taken (zie functionele domeinen) die de defensieorganisatie uitvoert.*
- Vraag 3.6.2 Gaat Defensie volgens u met de rationalisatie methodiek, zoals beschreven in het Defensie Ontwerp IT (met zijn principes, faseringen, assessment criteria en governance), zijn rationalisatie doelstelling behalen? Waar zijn aanpassingen nodig?*
- Vraag 3.6.3 Is met de beschreven methodiek, de grote hoeveelheid rationalisaties en migraties effectief en beheersbaar te verwerken? Waar zijn volgens u aanpassingen nodig?*
- Vraag 3.6.4 Welke rekenregels gebruikt de markt voor het schatten van doorlooptijd, financiële- en capaciteitsplanning om rationalisatie en migratie doelstellingen te behalen?*
- Vraag 3.6.5 Welke beslissers, governance, expertise, kennis en kunde zal Defensie minimaal moeten hebben en of behouden om succesvol de rationalisatie en migratie doelstellingen van defensie te behalen?*
- Vraag 3.6.6 Waar in het proces en hoe kan de markt het meest efficiënt bijdragen om de rationalisatie en migratie maximaal te versnellen?*
- Vraag 3.6.7 Waar ziet de markt kansen om het proces van rationalisatie en migratie te versnellen?*

3.7 Focus - IT Management

- Vraag 3.7.1 Welke verbindingseisen en standaarden stelt u aan het koppelen van "loosely coupled" IT-toepassingen, services en componenten? Hoe controleert en bewaakt u de kwaliteit en het gebruik van deze IT-toepassingen, services en componenten?*
- Vraag 3.7.2 Beschikt u over een cloud management platform dat de genoemde functies in samenhang vervult? Kunt u deze functies detailleren en aangeven wat per functie de noodzakelijke randvoorwaarden zijn?*

- Vraag 3.7.3 *Hoe garandeert u de integriteit, beschikbaarheid, exclusiviteit en onweerlegbaarheid? (Van services en data)*
- Vraag 3.7.4 *Welke mogelijkheden ziet u om de provisioning van services van verschillende leveranciers zo in te richten dat afhankelijk van het gebruik ketens of individuele services door de gebruiker kunnen worden gewisseld (selfservice van services)?*
- Vraag 3.7.5 *Stel dat u de brokerrol voor Defensie gaat vervullen hoe garandeert u dan dat Defensie up-to-date blijft en toegang behoudt tot best-of-breed services ongeacht van welke partij?*
- Vraag 3.7.6 *Hoe ziet u, in relatie tot IT Service Management, de rol van de CMDB (of: het CMS in ITIL2011)?*
- Vraag 3.7.7 *Hoe ziet u de proces, en tooling implementatie van Development/Operations (DevOps) en het Scaled Agile Framework™ bij Defensie en in samenwerking met de markt en kennis instituten? Heeft u referentie kaders en/of (aanvullende) best-practices.*
- Vraag 3.7.8 *Hoe gaat u om met ontwikkelingen die impact hebben op een hele keten aan toepassingen waarbij meerdere partijen verantwoordelijk zijn voor individuele onderdelen in die keten? Hoe koppelt u die afhankelijkheden zoveel mogelijk los?*
- Vraag 3.7.9 *Hoe gaat u om met de lifecycle van de hele IT stack? Hoe richt u lifecycle- release management en versiebeheer in, gelet op de (zeer) korte doorlooptijden en het cyclische karakter van Scaled Agile Framework™ en DevOps?*
- Vraag 3.7.10 *Welke technieken en tooling zijn, volgens u, beschikbaar voor het implementeren van `zero downtime deployment`? Kunt u schetsen hoe de "Automation" van de diverse onderdelen (build, test, quality, security, integration, deployment, etc.) eruit ziet in een heterogeen landschap?*
- Vraag 3.7.11 *Welke invulling kunt u geven aan het consolidated (security) event management vanuit een ontplooid domein naar het centrale beheerdomein, rekening houdend met het wegvallen van verbindingen, rubriceringen en beperkte bandbreedte?*
- Vraag 3.7.12 *Welke invulling kunt u geven aan het IT Service Management, rekening houdend met de scheiding tussen LGI/HGI en Statisch/Ontplooid, de communicatie tussen de afzonderlijke ITSM platformen en de aspecten Agile/DevOps, LEAN & out-of-the-box?*
- Vraag 3.7.13 *Hoe ondersteunt u Business Continuity Management binnen uw (beheer) oplossing?*

Bijlage 1: (concept) Eindrapport Defensie Ontwerp IT V0.7

Bijlage wordt als separaat document bijgevoegd.

Bijlage 2: (concept) deelrapport A – Informatiebeveiliging V1.0

Bijlage wordt als separaat document bijgevoegd.

Bijlage 3: (concept) deelrapport B – IT Toepassingen V0.7

Bijlage wordt als separaat document bijgevoegd.

Bijlage 4: (concept) deelrapport D – IT Specificatie V0.7

Bijlage wordt als separaat document bijgevoegd.

Bijlage 5: Antwoordformulier

Vraag	Antwoord
Algemene vragen over de Respondent	
Vraag A.1	<i>Wat is de naam van het bedrijf?</i>
Vraag A.2	<i>Indien het bedrijf een dochteronderneming is, wat is de naam van de moedermaatschappij?</i>
Vraag A.3	<i>Wat zijn de adressen van het bedrijf?</i> <ul style="list-style-type: none"> • <i>Hoofdkantoor.</i> • <i>Lokale vestigingen in Nederland.</i>
Vraag A.4	<i>Wie is/zijn degene(n) die verantwoordelijk is/zijn voor de beantwoording van deze marktconsultatie?</i>
Vraag A.5	<i>Wat zijn de contact gegevens van de verantwoordelijke(n):</i> <ul style="list-style-type: none"> • <i>Telefoon</i> • <i>Fax</i> • <i>Email</i>
Vraag A.7	<i>Verwacht u binnen afzienbare tijd te maken te krijgen met fusies over overnames? Zo ja heeft dit invloed op uw portfolio?</i>
Voorbehouden	
<i>Voorbehoud 1.2.a JIVC vergoedt op geen enkele wijze kosten verbonden aan beantwoording van deze marktconsultatie, of daaraan gerelateerde activiteiten.</i>	
<i>Voorbehoud 1.2.b JIVC houdt zich het recht voor om geen vervolg te geven aan deze marktconsultatie.</i>	
Antwoorden op de vragen	
<i>Hierbij de indeling en nummering volgen zoals is opgenomen in hoofdstuk 3.</i>	
<i>Per vraag het antwoord op maximaal 2*A4 document aanbieden. Indien nodig kunt u aan het antwoord een bijlage toevoegen van maximaal 10*A4.</i>	

Bijlage 6: Afkortingen

APM	Applicatie Portfolio Management
COTS	commercial of the shelf
CMDB	Configuration Management DataBase
ESB	Enterprise Service Bus
DEAS	Defensie Enterprise Applicaties Store
DEASS	Defensie Enterprise Applicaties Store Services
DevOps	Development/Operations
DML	Definitive Media Library
DMO	Defensie Materieel Organisatie
HLO	High Level Ontwerp
IDA	Integrale Defensie Architectuur
JIVC	Joint IV Commando
MDM	Master Data Management
MUT-domein	Mobiel, Uitgestegen en Te voet-domein
OMUT	Ontplooid, Mobiel, Uitgestegen en Te voet
Qos	Quality of Service
SMC	Service Management & Control
SOA	Service Oriented Architecture
SPM	Strategisch Portfolio Management
TBM	Tactisch Besluitvormings Model

Bijlage 7: Informatie inzake de reviewsessies

Bijlage wordt als separaat document bijgevoegd.