> Retouradres Postbus 90004 3509 AA Utrecht

Defensie Materieel Organisatie
Programma
Grensverleggende IT

Herculeslaan 1
3584 AB Utrecht
MPC 58 A
Postbus 90004
3509 AA Utrecht
Nederland
www.defensie.nl/dmo

Contactpersoon
Lex van der Loo
Programmasecretaris
Grensverleggende IT

M +31 (0)6 553 802 42
am.vd.loo@mindef.nl

Datum 17 augustus 2015
Onderwerp Verslagen Boardroomsessies 11 en 12 augustus 2015

Op 11 en 12 augustus zijn in Camp New Amsterdam vier electronic boardroom sessies georganiseerd in het kader van de technische marktconsultatie (zie Tenderned # 74808):

1. IT-Infrastructuur;
2. IT-Beveiliging;
3. IT-Toepassingen;
4. IT-Management inclusief businesscase.

Deelname aan die bijeenkomsten stond open voor iedereen die zich vooraf heeft aangemeld. In totaal zijn 51 personen aangemeld voor de bijeenkomsten.

In de vier bijeenkomsten is aan de deelnemers gevraagd om een serie vragen te beantwoorden die betrekking hebben op de nieuwe IT van Defensie.

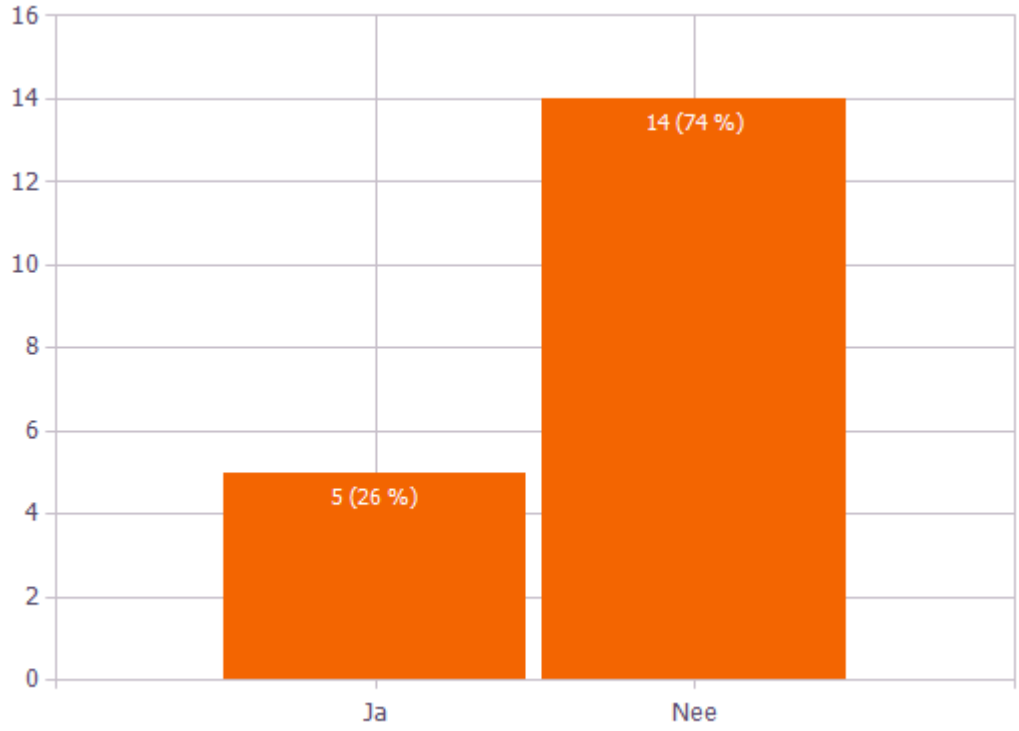
Bijgaand zijn de - nagenoeg - letterlijke verslagen van de vier bijeenkomsten opgenomen met dien verstande dat spelfouten zijn gecorrigeerd.

IT Infrastructuur

Inhoudsopgave

1 Feedback op DoIT

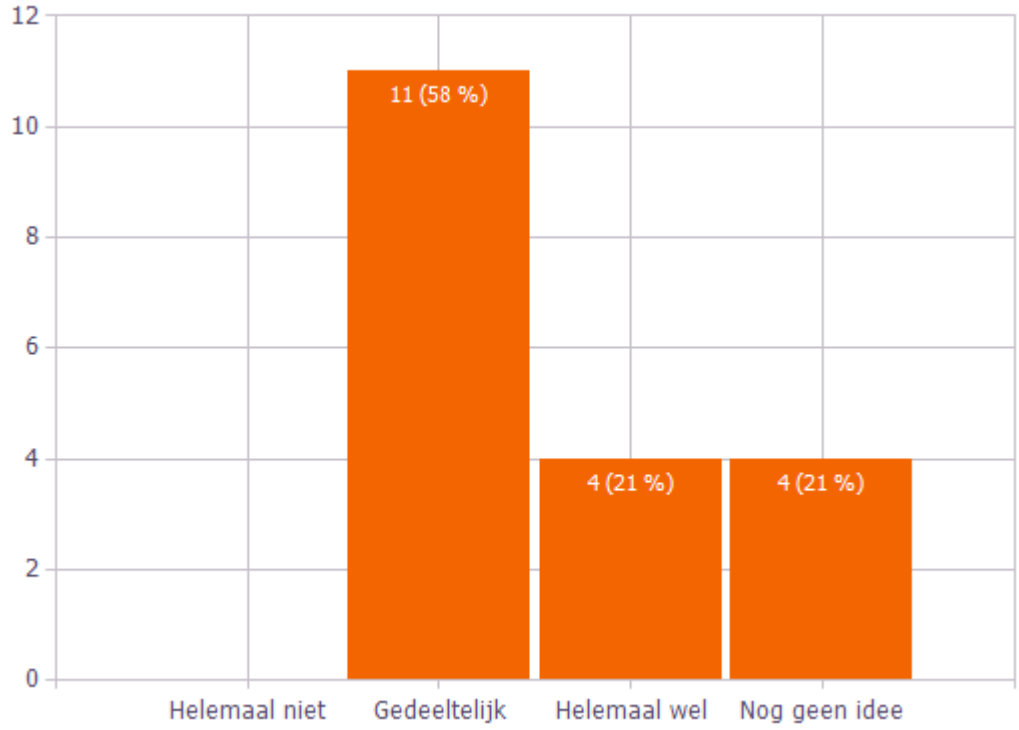
1.1 Vindt u dat DoIT 0.7 op het gebied van IT Infrastructuur de definitieve versie mag worden? (dus geen aanpassingen meer)



Antw.	Nummer	Percentage
Ja	5	26%
Nee	14	74%

1.2 In hoeverre acht u de ambitie van Defensie haalbaar voor de 1ste oplevering van de groeikern?

Denk hierbij onder andere aan de beschikbare tijd, de omvang van de werkzaamheden, één uniforme werkplek, Alles als een service aanbieden, de Defensie Appstore of de doelstelling dat binnen 5 jaar uit huidige realisatiedomein opgeheven kan worden.



Meerkeuze optie: Helemaal niet

Antwoord

Meerkeuze optie: Gedeeltelijk

Antwoord
Realisatie Infra is 1, de daarmee samenhangende cultuurwijziging kan mogelijk belemmerend werken.
Vanuit het infrastructuur-gedeelte vanwaar wij opereren kan ik alleen deze vraag beantwoorden. Het Datacenter-gedeelte dus. De daar beschreven ambitie vind ik realistisch en kan mijnsinziens gehaald worden.
De Scope is breed en er bestaan binnen de groeikern afhankelijkheden. Onduidelijk zijn de "reverse critical paths" binnen deze ambitie.
Geheel afhankelijk van: - In hoeverre men in staat is aan te sluiten bij marktstandaarden/standaardproducten. - Of de regie/governance goed is ingeregeld --> kunnen alle gebruikers/stakeholders "gedwongen" worden om mee te werken of staat men toe, dat zij een Eigen koers varen.
Ervaringen uit het verleden bieden hier de garantie voor de toekomst. Oftewel, snelheid van acteren door de IT-organisatie/Inkoop is altijd al een probleem geweest. De omvang van het traject legt hier nog een extra moeilijkheid op. Regelgeving is vaak beknellend gebleken en veroorzaakt vertraging in de procedures. Uiteraard hoop ik dat het wel haalbaar is.
Ambitie (net als de visie) is absoluut haalbaar maar hoeft niet in 1 keer haalbaar te zijn. Wederom “Think big, act small” is in onze beleving een goede benadering en de plateauplanning goed. Op sommige punten is nog wel een verdiepingsslag nodig, hier komen wij in de schriftelijke RFI-beantwoording op terug. Maturity model: groei nodig in verschillende aspecten om uit te groeien tot shared service organisatie en High Performance Organisatie, met name relevant voor de "mode 2" organisatie. Blijft als vanzelfsprekend cruciaal

Antwoord
om oog te houden voor de "mode 1" organisatie met het oog op de continuïteit van de huidige IT en de daarbij benodigde expertise en kennisbehoud.
Beperkte tijdspanne tussen gunning en IOC.
Het opleiden van de gebruikers meenemen in de transitie.
Aantal fundamentele ontwerpkeuzes over werkplek moeten nog worden gemaakt
Een hybride / public cloud oplossing met complexe koppelvlakken met bestaande iT zal meer tijd vragen
Het venijn zit 'm in de staart. Als Rationalisatie stokt, zal meer tijd nodig zijn.

Meerkeuze optie: Helemaal wel

Antwoord
Wij zijn van mening dat dit haalbaar is. Gezien ervaring met andere projecten. Het deel groeikern is in deze ook goed afgebakend.
Current Defensie Ontwerp IT is mogelijk met todays technology.
Gefaseerde realisatie reduceert het overall risico.
Verwachting moet wel gebaseerd zijn op beschikbare fondsen.
Tijdsbestek van vijf jaar moet realistisch zijn. Ontwerp (HLO) is nog erg globaal; een verfijningsslag naar detailontwerp is bepalend.

Meerkeuze optie: Nog geen idee

Antwoord
Helemaal afhankelijk van de inzet van de defensiemedewerkers/-specialisten, met name voor de specifiek militaire omstandigheden
Dit is alleen mogelijk als de top van Defensie ook werkelijk deze stappen durft te zetten. Cultuur en doorzettingsmacht zijn hierbij essentieel en niet de techniek. Mogelijkheden van Kill en applicatierationalisatie (en de werkelijke wil) zijn hierbij essentieel.
Afhankelijk van wat off the shelve beschikbaar is, mate van samenwerking met de markt, readyness van IT-organisatie en die van de te servicen afdeling (eerste projecten). Uit de huidige stukken is dat nog niet duidelijk.

1.3 Kunt u uw feedback geven op het gedeelte IT Infrastructuur in DoIT

Inleiding

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Aanleiding en doelstelling zijn helder. Raakvlak tussen figuur 21 en 22 mag uitgelegd worden. Belangrijk is dat de gestelde eisen toetsbaar zijn. Zo niet , dan heeft het geen nut deze als zodanig mee te nemen.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Is voldoende duidelijk.
In grote lijnen is het duidelijk. T.a.v. koppelvlakken, eisen, richtlijnen en afbakening is verdieping nodig.
Lijkt me duidelijk genoeg, de politieke speerpunten naar werkelijke prioriteiten en hoe hier mee omgegaan moet worden, lijkt me belangrijk bij de ambitieuze doelstelling. Zeker gezien de planning.

Meerkeuze optie: Is nog niet beschreven

Antwoord
Hoe gaat DO-IT gehanteerd worden. Dit moet volgens mij in het document beschreven worden. DO-IT is/lijkt nu een toetsingskader voor de nieuwe omgeving. Hoe gaat dit gehanteerd worden in de volgende fases RFP/RFI?

Defensie medewerkers

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Is nog niet volledig. Waar ligt de grens bij Services, wie doet wat. De raakvlakken zijn belangrijk.
Management of Change is in onze beleving onderbelicht. Deels bepalend voor het succes voor Defensie en de marktpartijen, want “als je doet wat je altijd deed dan moet je niet verbaasd zijn dat je krijgt wat je altijd kreeg” (vrij naar Einstein).
IT blijkt telkens weer een complex vraagstuk, zodra eindgebruikers er mee moeten gaan werken. Grote stappen (en soms ook kleine, zie de marktreactie om het startmenu van W8...) zijn lastig te managen. Bovendien is de grote groep erg divers van samenstelling en zijn er veel te ondersteunen software producten. Cruciaal is dus dat een goede afvaardiging van de gebruikers wordt opgeschakeld en dat er een positief marketing beleid wordt gevoerd.
Wat wordt de rol van de defensie medewerkers in de volledige life cycle van de diensten?
Eisen zouden nog toelichting kunnen krijgen (waarom van belang). Is wel weer extra werk, maar kan straks een "voldoet niet" van een leverancier in context plaatsen. Mogelijke aanvulling voor wat betreft verantwoordelijkheden.
Een duidelijke uitspraak over de combinatie van de medewerkers "stop" en de up or out strategie is een gedurfde uitspraak, hierdoor is het veel duidelijker welke toekomstige medewerkers (niveau) mogelijk is en hoe dit gehandhaafd kan blijven voor die medewerkers die in dienst zijn/blijven.
Wat zijn de competenties om samen met de markt te ontwikkelen, maar ook wat zijn de competenties en vereiste skills om in de ontplooide omgeving bv Mali het te kunnen beheren?

Meerkeuze optie: Is nog niet beschreven

Antwoord
Afhankelijk van keuze in- of outsourcen zal dit verder uitgewerkt moeten worden (tussen Defensie en markt). Met name voor de Defensie (IT)-medewerker is dit momenteel een grote onzekerheid.

Software as a Service (SaaS)

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Het lijkt of er een volledig "eind" document gemaakt moet worden, echter is het essentieel te weten dat dit een levend document zou moeten blijven. Defensie zou de reis moeten aanvangen met de vele plannen die er nu zijn. Aanscherpen en starten lijkt belangrijker dan nog vollediger te zijn.
Is essentieel om in stappen te kunnen blijven werken. Een 1.0 versie kan natuurlijk ook gevolgd worden door een 1.1. Starten met de werkelijke plannen is wellicht belangrijker dan het verder ontwikkelen van plannen, deze zullen blijven veranderen door marktomstandigheden en politieke keuzes.
Ik denk dat het vooral belangrijk is dat er op termijn werkelijk gestart kan worden. Het is essentieel om in stappen te kunnen blijven werken. Eeen 1.0 versie kan natuurlijk ook gevolgd worden door een 1.1. Starten met de werkelijke plannen is wellicht belangrijker dan het verder ontwikkelen van plannen, deze zullen blijven veranderen door marktomstandigheden en politieke keuzes.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Verantwoordelijkheid van de leverancier(s) voor de life cycle van de SaaS diensten?
Is essentieel om in stappen te kunnen blijven werken. Een 1.0 versie kan natuurlijk ook gevolgd worden door een 1.1. Starten met de werkelijke plannen is wellicht belangrijker dan het verder ontwikkelen van plannen, deze zullen blijven veranderen door marktomstandigheden en politieke keuzes.
SaaS wordt nu nog veelal als publiek gezien. Veel hangt af van in hoeverre - over het algemeen generieke software - kan voldoen aan defensie-standaarden, vooral ten aanzien van beschikbaarheid en beveiliging. Indien het architectuurmodel SaaS gecombineerd kan worden met een private cloud (mag dat nog SaaS heten?), dan zijn er natuurlijk meer mogelijkheden.

Platform as a Service (PaaS)

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Geen commentaar

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Verdieping op de loosely coupled legacy. Van wezenlijk belang bij het uitfaseren hiervan.
Wrapper service is een belangrijke voor toekomstig slagen voor koppeling migratiedomein met innovatiedomein. Mogelijk kan hier iets op worden verdiept.

Infrastructure as a Service (IaaS)

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Grafische weergave verduidelijkt de samenhang en daarmee de wens van Defensie.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Houdt in de IAAS-laag rekening met het feit dat zowel compute als network als storage abstract kan worden. Denk ook aan netwerkvirtualisatie.
Uitwerking van hybride scenario's in relatie tot potentiële workloads.

Antwoord
Belangrijk deel voor Do IT. Zal zeker op een andere wijze aangekocht moeten worden. Hoe sluit dit aan bij enovatie deel (standaarden (IaaS) vs geen standaarden(enovatie))

Housing Services

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Er is een aantal housingaspecten genoemd, welke beïnvloed worden door de te ondersteunen services. Deze opsomming is zeker niet compleet. Mogelijk kunnen er ook nog andere aspecten van de housing services worden gedefinieerd, welke vanuit andere aspecten belangrijk zijn voor Defensie. De basis indeling van de te leveren housing services is overzichtelijk en zeker werkbaar.
Niet geheel duidelijk hoe en waar deze housing gaat plaatsvinden. Brick-and-morter of flexibeler containers Nieuw of bestand. PUE waarden?

Beheer Services

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Hybride integratie platform om incrementele fases te testen, voordat het gebruikt wordt in het operationele system, is een goede keuze.
De structuur/opzet is helder.
Bevat een paar dubbelingen in eisen.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Hoe moet een gezamenlijk beheer eruit gaan zien bij speciale operaties? Screening en geheimhouding, beveiliging?

Security Services

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Security model is stevig en analoog aan USG.

Meerkeuze optie: Is nog niet beschreven

Antwoord
Wordt verwezen naar ander hoofdstuk.

Gehele hoofdstuk (irt) document

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Service Oriented Architecture is gelijk aan US government (USG) IT-systeem.
Hoofdstuk is duidelijk. Wel zal verder moeten worden nagedacht over de functionaliteit, die belangrijk is voor Defensie en niet gemakkelijk kan landen in het innovatie domein, omdat zelfbouw een te grote wissel zou leggen op de Defensie organisatie.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Regie en orchestratie moeten nader worden ingevuld. Framework, waarbinnen marktpartijen kunnen opereren.
Afkadering en interfaces van de "kavels" moeten of duidelijker gespecificeerd worden of gezamenlijk met de te selecteren partners worden bepaald. Bijvoorbeeld koppeling van XaaS/ MwO met de IAM oplossing, manier van ontsluiten van applicaties uit de "oude" omgeving, etc. Vanwege de beschreven manier van werken in gezamenlijke teams lijkt de laatste de voorkeur te hebben, ook vanwege de geschetste tijdslijnen.
Het zou helpen als de figuren (blokken) ergens worden toegelicht, danwel een verwijzing naar de standaarden waar ze op gebaseerd zijn.
alg . Als zaken aangekocht worden in de vorm van ...Service dan is het belangrijk en zal er nog verduidelijkt moeten worden hoe de verschillende delen op elkaar aansluiten.
Document is prima als leidraad om als partners gezamenlijk de nieuwe infrastructuur te realiseren. Is echter niet dusdanig uitgespecificeerd dat het op deze manier in de markt kan worden gezet als RFP, waarop men kant en klare oplossingen kan aanbieden.
De invulling van het governance model mag meer body krijgen, maar wij verwachten dat de toekomstige regie partner samen met Defensie (en de marktpartijen) meer invulling aan dit model zal geven. Wij adviseren Defensie echter wel hier hoge prioriteit aan te geven en snelheid te maken.
Zoveel mogelijk openheid inzake de omstandigheden (zowel LGI als HGI) wat wel of niet verwacht mag worden in de soms extreme omstandigheden, waarmee rekening moet worden gehouden binnen een militaire context (bijvoorbeeld op netwerk gebied, autonomie of koppeling?) of m.b.t. interoperabiliteit vraagstukken in de NATO context. Uiteraard is hier reeds veel kennis over opgebouwd en zijn zaken herbruikbaar, maar geen enkele (Defensie) organisatie is eenduidig.

2 Logische stappen

2.1 Is het op het gebied van IT Infrastructuur mogelijk om "act small" te doen, irt "Think Big"?

Motiveer uw antwoord alstublieft op de volgende wijze;
Ja: Kunt u voorbeelden geven van (kleine) stappen die we kunnen doen.
Nee: Wat zijn belemmeringen en hoe kunnen deze weggehaald worden?

Meerkeuze optie: Ja

Antwoord
Vermits het ontwerp staat kunnen er natuurlijk kleine stappen genomen worden. De samenhang bij een dergelijk project is toch complex, dus er zullen concessies gedaan moeten worden. Ook de wil om samen de schouders er onder te zetten is cruciaal.
Innovatieboard inrichten, waarmee Defensie en vaste partners aan derde partijen de ruimte bieden om innovatieve ideeën in te brengen, welke op basis van gezamenlijke BC worden beoordeeld (finale stem voor Defensie).
De markt vragen wat zij nu al kunnen leveren t.b.v. de gestelde eisen.
Het is hier van belang hier of defensie vasthoudt aan een toekomstvaste infrastructuur, die op kleine schaal is op te bouwen en integreert in het geheel. Standaardisatie, schaalbare technologie.
Assess de gaps en beoordeel het high level design op inefficiënties en/of andere issues met de marktpartijen.
Mits in juiste volgorde wordt uitgevoerd...(van laag niveau diensten naar hogere).
Duidelijke architectuur definiëren waarbij de koppelvlakken gespecificeerd zijn zodat per onderdeel gewerkt kan worden.
Begin met LGI/statisch domein.
Architectuur uitwerken voor eerste behoefte (agile), niet in detail voor eindplaat
Opsplitsen in modules waarbij de modules naadloos op elkaar moeten aansluiten. Hierdoor krijgen de kleinere partijen de kans om hoogwaardige (lees niche) technieken aan te bieden aan Defensie en is Defensie niet veroordeeld tot een totaaloplossing van "de grote jongens". Door het toepassen van "open standaarden" is dit zeer goed te realiseren.
Graduele groei.
De groeikern kan stap voor stap opgebouwd worden. Data centraal "plaatsen" met als eind the Think Big.
Zorg dat People, Process en Technology getest kunnen worden.
'Lessons learned' en 'best practices' blijvend terugkoppelen richting Defensie, zowel de positieve als de negatieve aspecten. Zowel m.b.t. de lopende operatie (plan, design, run fase) als voor innovatieve beproevingen (ook binnen een militaire- en inlichtingen context).
Kantoor applicaties.
Op basis van de basisinfrastructuur gezamenlijk met Defensie en eventueel andere partners in sprints de gewenste toevoegingen/ aanpassingen doorvoeren (interfaces, ontsluiting, beveiliging, etc.).
Small roll out.
Begin met "eenvoudig" project, waarbij de benodigde services uit de infra-laag minimaal zijn.
Small concept.
Zoveel mogelijk openheid inzake de omstandigheden (zowel LGI als HGI). Wat wel of niet verwacht mag worden in de soms extreme omstandigheden, waarmee rekening moet worden gehouden binnen een militaire context, bijvoorbeeld op netwerkgebied, autonomie of koppeling? Of m.b.t. interoperabiliteit vraagstukken in de NATO context. Uiteraard is hier reeds veel kennis over opgebouwd en zijn zaken herbruikbaar, maar geen enkele (Defensie) organisatie is eenduidig.
Bepaal de afhankelijkheden tussen de verschillende infrastructuur componenten.
Over de technische as met de volgende fasen: architectuur voltooien “Just In Time”, Project Start Architectuur (PSA) hanteren voor deelprojecten, bouw en migratie.
Logische scheiding in hardwarecomponenten.
Infrastructuur neerzetten op basis van standaard diensten partner.
Ja, mits de sturing op de invoering "Think BIG" als doelstelling heeft.

Antwoord
Een duidelijke organisatorische en governance model invulling.
Big architectuur.
Kleine testgroepen per Defensieonderdeel maken.
Selecteren partners op basis van generieke RFP (basis portfolio/capaciteiten/etc.).

Meerkeuze optie: Nee

Antwoord
Continuïteit in besturing en besluitvorming in de toekomst is niet stevig genoeg.
Agile werken vraagt een enorme culltuuromslag.
Kennis van THE big picture moet beter op Governance-overleg landen.

2.2 Feedback op de genoemde kleine stappen

Meerkeuze optie: Verrijking

Big architectuur

Antwoord
De architectuur moet op highlevel niveau het framework voor de kleine stappen geven.

Een duidelijke organisatorische en governance model invulling.

Antwoord
Durf afhankelijkheden ook te verminderen als dat mogelijk is.
Die gedragen wordt door de hele organisatie, maak klanten verantwoordelijk voor de sturing op hun diensten (devops), waardoor ze ook verantwoording moeten nemen op de afgesproken governance.
Testgroepen koppelen aan klanten, direct resultaat daar waar dat mogelijk is (devops benadering), directe impact op klant en uitvoering.

Ja, mits de sturing op de invoering "Think BIG" als doelstelling heeft

Antwoord
Mee eens zie antwoorden op nee.

Zoveel mogelijk openheid inzake de omstandigheden (zowel LGI als HGI) wat wel of niet verwacht mag worden in de soms extreme omstandigheden, waarmee rekening moet worden gehouden binnen een militaire context, bijvoorbeeld op netwerk gebied, autonomie of koppeling? Of mbt interoperabiliteit vraagstukken in de NATO context. Uiteraard is hier reeds veel kennis over opgebouwd en zijn zaken herbruikbaar, maar geen enkele (Defensie) organisatie is eenduidig.

Antwoord
Welke openheid wordt hier gevraagd? Moeten leveranciers mee naar Mali?

Op basis van de basisinfrastructuur gezamelijk met defensie en eventueel andere partners in sprints de gewenste toevoegingen/ aanpassingen doorvoeren (interfaces, ontsluiting, beveiliging, etc.)

Antwoord

Goede Agile Methode. Wel extrapoleren naar Project/Programma level.

Kantoor applicaties

Antwoord

Het faciliteren in een virtuele KA-omgeving voor de medewerkers, waarbij geleidelijk nieuwe apps worden toegevoegd, zal het draagvlak (cultuursverandering) vergroten en daarmee faciliteren in het in kleine stukjes opleveren van de infra.

'Lessons learned' en 'best practices' blijvend terugkoppelen richting Defensie, zowel de positieve als de negatieve aspecten. Zowel mbt de lopende operatie (plan, design, run fase) als voor innovatieve beproevingen (ook binnen een militaire- en inlichtingen context).

Antwoord

Ervaringen en leveranciersonafhankelijke inzichten zijn nodig om tot de best practise te komen. Voorkomen van preken voor eigen parochie.

Opsplitsen in modules waarbij de modules naadloos op elkaar moeten aansluiten. Hierdoor krijgen de kleinere partijen de kans om hoogwaardige (lees niche) technieken aan te bieden aan Defensie en is Defensie niet veroordeeld tot een totaaloplossing van "de grote jongens". Door het toepassen van "open standaarden" is dit zeer goed te realiseren.

Antwoord

Op deze manier krijgen de kleinere marktpartijen ook een kans om zich te bewijzen, anders zijn ze afhankelijk van een grote partij die hun oplossing wel of niet in de aanbieding wil meenemen.

Deze aanpak werkt kwaliteit verhogend en zo wordt de benodigde kennis optimaal benut.

Duidelijke architectuur definiëren waarbij de koppelvlakken gespecificeerd zijn zodat per onderdeel gewerkt kan worden.

Antwoord

Van belang om interoperabel te zijn en open binnen de architectuur.

Van belang hier is of defensie vasthoud aan een toekomstvaste infrastructuur die op kleine schaal is op te bouwen en integreert in het geheel. Standaardisatie, schaalbare technologie.

Antwoord

Mee eens en in hoeverre kan en wil Defensie (op deelvlakken) een early adopter zijn.

Markt vragen wat zij nu al kunnen leveren tbv de gestelde eisen

Antwoord

Belangrijk zijn goede referenties.

Dit zal toch blijken uit de beantwoording van de RFP ?

Innovatieboard inrichten waarmee Defensie en vaste partners de ruimte bieden aan derde partijen om innovatieve ideeen in te brengen welke op basis van gezamenlijke BC worden beoordeeld (finale stem voor Defensie)

Antwoord
Mee eens. Als innovatie 1 van de kernpunten is, zal een innovatieboard van toegevoegde waarde zijn in het stapsgewijs uitrollen.

Meerkeuze optie: Feedback

Selecteren partners op basis van generieke RFP (basis portfolio/capaciteiten/etc.)

Antwoord
Ja, goed plan, middels verdere verdieping komen tot raamcontracten voor de diverse onderdelen van de infra.

Kleine testgroepen per defensie maken

Antwoord
Wat wordt hier bedoeld?
Zorg wel dat de groepen afdekkend zijn.
Als het onderdeel is van een groter geheel.

Big architectuur

Antwoord
Wat wordt hiermee bedoeld?
toelichting
Klinkt afschrikwekkend en langdurig. Wel voor de grote lijn (maar die tekent zich nu al af), voor meer concete stappen een JIT architectuur en PSA

Een duidelijke organisatorische en governance modelinvulling.

Antwoord
Defensie zal de regie in eigen hand moeten houden.
Belangrijk is dat de "impact" wel groot is, voor de cultuuromslag bij de "klant" is het essentieel dat er voordelen voor staken-holders moeten zijn, te klein acteren heeft vaak geen duidelijke voorbeeld functie en is nodig voor succes!

Ja, mits de sturing op de invoering "Think BIG" als doelstelling heeft.

Antwoord
Mee eens.
Eens, risico is te verzanden in kleinere initiatieve en "BIG" nooit te bereiken.

Infrastructuur neerzetten op basis van standaard diensten partner

Antwoord
Dit kan haaks op enovatie komen te staan.

Logische scheiding in hardwarecomponenten

Antwoord

Aanvulling op deze stap is, dat zoveel mogelijk voor generieke hardware wordt gekozen vanuit een Software Defined Datacenter optiek en software-matig wordt gescheiden.

Bepaal de afhankelijkheden tussen de verschillende infrastructuur componenten

Antwoord

Fundamenteel voor de architectuur van de omgeving.

Small concept

Antwoord

Onduidelijk, toelichting nodig.

Begin met "eenvoudig" project, waarbij de benodigde services uit de infra-laag minimaal zijn.

Antwoord

Helemaal mee eens; werken in sprints is ook hier noodzakelijk. Tenzij het nu helemaal uitgespecificeerd kan worden. Dit laatste lijkt niet verstandig, omdat je juist wilt dat de omgeving in de toekomst ook blijft ontwikkelen/ meegroeien --> hanteer dan vanaf het begin deze aanpak gedachte.

Kantoorapplicaties

Antwoord

Zou het wat ruimer definieren.

Is een van de eerste stappen: is vaak onderdeel van de standaard werkplekken op de markt.

Is een grote stap.

Opsplitsen in modules waarbij de modules naadloos op elkaar moeten aansluiten. Hierdoor krijgen de kleinere partijen de kans om hoogwaardige (lees niche) technieken aan te bieden aan Defensie en is Defensie niet veroordeeld tot een totaaloplossing van "de grote jongens". Door het toepassen van "open standaarden" is dit zeer goed te realiseren.

Antwoord

Goed idee.

Opsplitsen in modules in deze fase betekent, dat je het nu dicht moet specificeren. Is dat mogelijk? Zijn alle variablelen nu al bekend?

Architectuur uitwerken voor eerste behoefte (agile), niet in detail voor eindplaat

Antwoord

Mee eens!

Begin met LGI/statisch domein

Antwoord

Mee eens: dit sluit het beste aan bij de standaard producten en diensten op de markt. Op die manier kun je zeker stellen, dat je snel een eerste resultaat bereikt. Op basis van de keuzes, die voor LGI/statisch worden gemaakt, kun je daarna de andere combinaites oppakken waarbij je dezelfde architectuur principes/ tooling/ etc. gaat hanteren als voor LGI/statisch.

Duidelijke architectuur definiëren, waarbij de koppelvlakken gespecificeerd zijn, zodat per onderdeel gewerkt kan worden.

Antwoord
Pas op voor te veel detailuitwerking.

2.3 Feedback op de genoemde belemmeringen

Meerkeuze optie: Feedback

Kennis van THE big picture moet beter op governance-overleg landen.

Antwoord
Aanvullend, verantwoordelijkheden duidelijk maken en procedures hoe met elkaar om te gaan als niet eens.

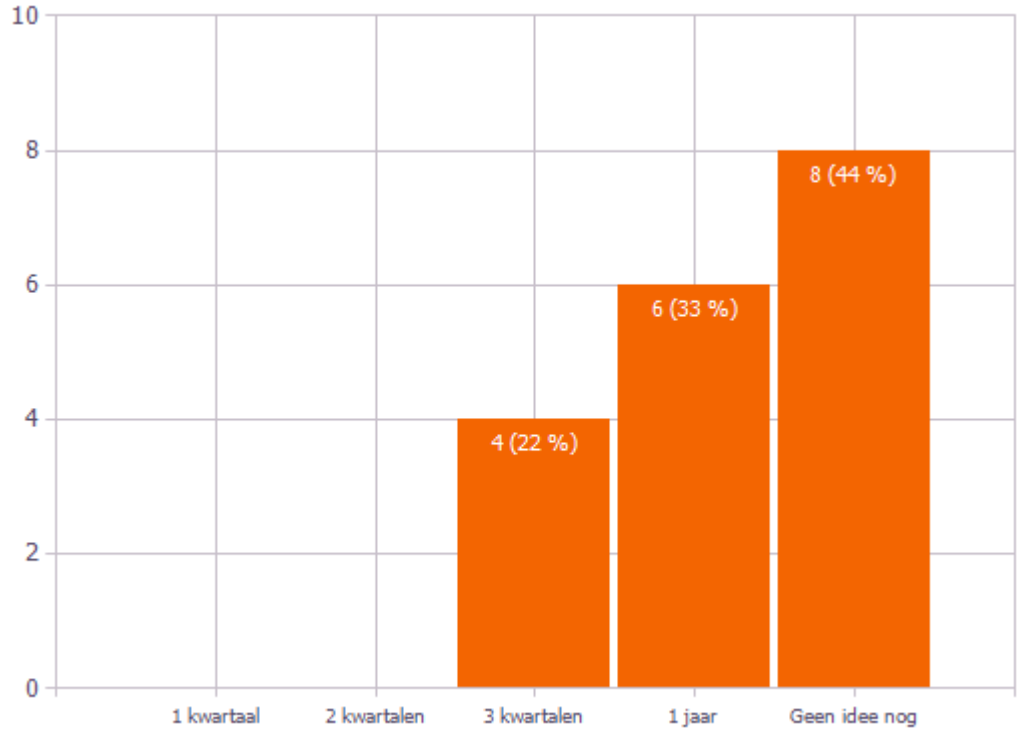
Agile werken vraagt een enorme culltuuromslag.

Antwoord
Mee eens. Defensie en Markt hanteren nu andere relatie. Van vecht naar Hecht relatie.
Draagvlak is key.
Mee eens. Groen is Aguilera per definitie, maar de andere kleur moet dit in ondersteunende vorm ook zijn
Ambitie is realistisch met today's technology, maar procedures en policy moeten daar wel op aangepast zijn. Vanuit IT-invalshoek moet policy gesynchroniseerd worden en consistent zijn met technologie.
Zowel bij Defensie als bij (een aantal) leveranciers. De Techniek staat het niet altijd toe.
Kleinschalig beginnen.

3 Plan van Aanpak

3.1 Hoeveel tijd schat u in om de IT-Infrastructuur van de gewenste groeikern te realiseren?

Kunt u uw antwoord toelichten?



Meerkeuze optie: 3 kwartalen

Antwoord
Is gebaseerd op voorgaande architectuur slagen (LAN2000, MULAN).
Levering van IOC voor statisch/LGI op basis van standaard Componenten.
Infrastructuur is niet het probleem. Implementeren, Applicatie finetuning en testen hebben de meeste tijdrisico's.
Gebaseerd op groot aantal aannames t.a.v. de referentie architectuur.

Meerkeuze optie: 1 jaar

Antwoord
Zal wel sterk afhangen van vele factoren: van de afkadering, omvang, aansluiten bij de standaard producten/diensten van de partner (maatwerk gaat meer tijd kosten).
Defensie zal, zoals ook andere overheidsorganisaties, zich moeten houden aan de Europeese regelgeving m.b.t. aanbesteden. De voorbereiding neemt de meeste tijd, omdat eerst de vraag moet worden gesteld; **Wat** wil ik hebben en vervolgens **Hoe** ga ik dit uitvragen, zodat ik krijg wat ik wil (met **Wat** bedoel ik hier natuurlijk **Functionaliteit**). De standaard doorlooptijd voor RFI + RFQ is minimaal 24 weken.
Hangt er vanaf van welk startpunt je rekent. Realisatie van infra sec gaat sneller dan alle voorbereidingen treffen (organisatie, governance, juridisch etc.).
De verwerving in deze is lastig te definiëren, want Defensie zou een ander model kunnen hanteren. De implementatie van een basis groeikern (new) 2-3 kwartalen.
Een reële ambitieuze planning is de enige planning, die gehaald wordt. Gezien de planning, verwerven tot implementeren, is 1 jaar een goede inschatting. Een langere planning zal de klant de mogelijkheid geven om te vernieuwen binnen de vernieuwing, wat zal afleiden van het te implementeren resultaat.

Meerkeuze optie: Geen idee nog

Antwoord
Verdere verdieping detail-ontwerp en keuzes zijn nog nodig, incl. de randvoorwaarden.
Keuzes, invulling, bouw, migratie etc. vergen een enorme doorlooptijd waar nu nog geen uitspraak over gedaan kan worden.
Vergelijkbare projecten hebben binnen de markt vaak langer dan een jaar in beslag genomen. De financiële middelen om dit te realiseren moeten ook geborgd zijn.
M.b.t. Plateau 2: met het juiste model van samenwerking, goede en door alle partijen gedragen scoping en goede inrichting van het governance- en regiemodel is 01-07-2016 haalbaar, mits gunning aan de markt begin januari 2016 plaatsvindt. In de schriftelijke beantwoording van de RFI geven wij een nadere uitwerking m.b.t. de 7 functionaliteiten genoemd in hoofdstuk 4.8. De echte complexiteit zit in Plateau 3. Ook hier gaan wij in een latere fase dieper op in.
Nog te weinig tijd gehad om de volledige scope op mijn netvlies te krijgen. Vooral als roces nog housing vraagstukken zijn kan het lang duren. Besluitvaardig handelen (act small) is cruciaal om meters te maken. Gevoelsmatig moet er in een jaar veel kunnen!
Helemaal afhankelijk van de design keuzes, welke gemaakt worden. Keuze voor standaarden van leveranciers kan het proces versnellen.

3.2 Waar liggen volgens u, op het gebied van de realisatie van de IT Infrastructruur, de drie grootste uitdagingen?

Let op mocht de uitdaging al genoemd staan hoeft u deze niet nogmaals in te voeren.

Antwoord
Gunning aan de markt begin januari 2016 zal plaatsvinden.
Defensie moet zelf ook snel meebewegen in het project. Kan de organisatie dat?
Scope scherper definiëren.
Samenwerkingsmodel dat gehanteerd wordt: selecteer partners waarmee je het samen gaat doen.
Geen beperking opleggen vanuit historie.
Wijzigen processen en procedures.
Goede en door alle partijen gedragen scoping en goede inrichting van het governance- en regiemodel
Don't take it personal Kees.
Haalbare eerste scope met doorgroeimogelijkheden na 1 juli 2016.
Detailuitwerking eisen en wensen.
Een werkende ITSM omgeving.
Voorkomen van maatwerk/beperken van afwijking van standaardproducten.
Scope scherper definiëren.
Implementatie: het aanpassen van procedures en policy aan de technologie.
Met het juiste model van samenwerking tussen marktpartijen en regiehouder.
Keuze virtualisatieplatform.
De kunst van het loslaten, geen bemoeienis van Defensie architecten, adoptie van good practices.
Vraagstelling in- of outsourcen.
Goede governance structuur (verantwoordelijkheden, afspraken).
Er moeten nog detail ontwerpkeuzes worden gemaakt.
Doorlooptijd behoeftestelling - verwerving
Verwerving, mensen/organisatie, service/dienst of traditioneel.
Keuze in uitvraag aan de markt.
De continuïteit van besluitvorming binnen Defensie.
Detailuitwerkingen.
Keuze in techniek.
Scope van de Groeikern.

3.3 Hoe groot schat u de genoemde uitdaging in?

Geef uw mening op een schaal van 1 - 10, waarbij
1 = helemaal geen uitdaging
10 = zeer grote uitdaging

Onderdeel	-	Gemiddelde van de score	St.dev.
De continuïteit van besluitvorming binnen Defensie		7,1	1,8
Goede governance structuur (verantwoordelijkheden, afspraken)		7,1	2,1
Implementatie: het aanpassen van procedures en policy aan de technologie.		6,9	2,3
Vraagstelling in- of out- sorcen		6,7	2,2
Verwerving		6,7	2,2
Wijzigen processen en procedures		6,6	1,9
Voorkomen van maatwerk/ beperken van afwijking van standaard producten		6,5	2,6
Scope scherper definieren		6,4	1,8
Keuze in uitvraag aan de markt		6,1	1,9
Keuze in techniek		4,2	2,2
	1 2 3 4 5 6 7 8 9	6,4	2,3

3.4 Uitdagingen uitwerken

3.4.1 Grootste uitdaging: De continuïteit van besluitvorming binnen Defensie

Meerkeuze optie: Gekozen oplossing

Antwoord
Infrastructuur keuzes niet onderhevig maken aan politiek: geen ruimte geven om technische discussies op politiek niveau te voeren. Richting bestuurders en politiek één iemand verantwoordelijk maken voor besluiten over functionaliteit. Voor de duur van het programma moet er dus één iemand zich committeren aan het leveren van Functionaliteit.
Kom met geloofwaardige snelle en zeer goede werkende oplossingen.

3.4.2 Grootste uitdaging Goede governance structuur (verantwoordelijkheden, afspraken)

Meerkeuze optie: Gekozen oplossing

Antwoord
Samenwerking definiëren met meerdere partijen, inclusief Defensie (moet in RFP bekend zijn). In dit samenwerkingsverband onder regie van Defensie afspraken maken over besluitvorming in architectuurboard, innovatie borgen in innovatieboard/architectuur board, financiële modellen, afspraken over transparantie (auditable). Dit samenwerkingsmodel moet je in stand houden gedurende de levensduur van de infra.

3.4.3 Grootste uitdaging Implementatie: het aanpassen van procedures en policy aan de technologie.

Meerkeuze optie: Gekozen oplossing

Antwoord
- Goeie governance structuur in het project. - Robuust advisory board (snel keuzes maken) . - Voldoende capaciteit en kwaliteit in projectgroep. - Commitment vanuit organisatie. - Rol van kosten.

3.4.4 Grootste uitdaging Vraagstelling in- of out- sorcen

Meerkeuze optie: Gekozen oplossing

Antwoord
Defensie houdt de leiding en regie. Business case moet duidelijk zijn in-/outsourcing. Niet alles bij een partij (Imtech). Duidelijke grenzen / koppelvlak.

3.4.5 Grootste uitdaging Verwerving

Meerkeuze optie: Gekozen oplossing

Antwoord
- Defensie moet actief teamvorming van leveranciers ondersteunen.
- Behoefte beter spiegelen met de marktmogelijkheden (op dat moment). - Zoveel mogelijk standaarden volgen.

3.4.6 Grootste uitdaging: Wijzigen processen en procedures

Meerkeuze optie: Gekozen oplossing

Antwoord
Stevig governance model, duidelijk stakeholders, empowered change agents.

3.4.7 Grootste uitdaging: Voorkomen van maatwerk/ beperken van afwijking van standaard producten

Meerkeuze optie: Gekozen oplossing

Antwoord
Strakke Project Governance met rigide sturing op de Scope. Zoveel benaderen vanuit een business perspectief. Wat is echt nodig.

4 Security

4.1 Waar ziet u nu de grootste beperkingen bij de realisatie van de Infrastructuur die voortkomen uit de gestelde beveiligingseisen.

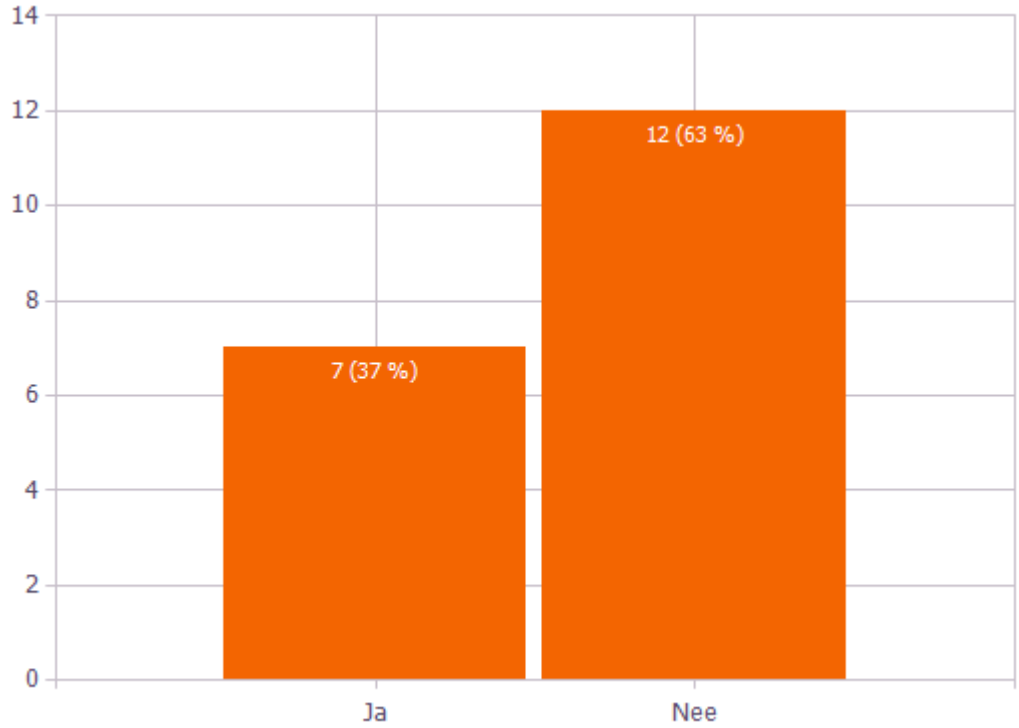
Antwoord
Mogelijke complexiteit voor deployed omgeving, waar ook de beveiligingseisen van belang zijn.
Ontsluiten van data uit meerdere bronnen/databases/systemen naar een veelvoud van applicaties op een beveiligde manier, is op een traditonele manier niet flexibel en agile genoeg in te richten. Overweeg om een Entrerprise Data Layer op te nemen in de infrastructuur als onderdeel van de infrastructuur.
Het IT-landschap rondom beveiliging is momenteel zeer sterk in ontwikkeling, zowel functioneel als technologisch. Vertaalslag van de huidige eisen en wensen levert afhankelijk van de insteek van leverancier een veelheid aan oplossingen. Helemaal lastig wordt het wanneer ook publieke diensten er bij worden betrokken, omdat daarvoor in het algemeen een one-size-fits-all keuze is gemaakt, waarbij de waardering dus andersom gaat: zijn de features van leverancier voldoende voor het afdekken van mijn eisen en wensen.
Garanties voor toegang tot nodige informatie vanwege de strenge veiligheidseisen.
De continue aanpassing op veranderende bedreigingen. De flexibiliteit van de Infrastructuur daarvoor. Hoe agile met relatief kleine aanpassingen?
Extreme RTO/RPO eisen.
De 'verborgen' uitdagingen – zaken, die nu nog niet aan het licht gekomen zijn maar straks als blocking issue opduiken en een maatwerk realisatie vragen. Dit hoeft geen probleem te zijn, maar voor de marktpartijen die alleen kennis hebben van de aangeboden stukken is dat minder stellig te beweren.
De beheergrens tussen LGI en HGI en overgang Statisch/Ontplooit.
Eisen t.a.v. RPO en RTO in combinatie met doorlooptijd en beschikbaar budget. Ontwerpkeuzes t.a.v. realisatie beschikbaarheid.
Geen grote beperking. Security approach is robuust en realistisch.
Het vooraf definiëren van de gewenste rollen, toegangen en verantwoordelijkheden en dit op een goede wijze implementeren en beleggen bij 1 afdeling/organisatie, zodat security geborgd kan worden volgens de geldende eisen.
De producten en diensten van de inschrijver/ leverancier zullen aan moeten sluiten bij de IAM/etc. oplossing, die in een ander kavel wordt gekozen. Hiervoor is in een vroeg stadium (tijdens RFP?) al overleg voor nodig.
Sentiment over de werkelijke security eisen bij bestuurders (risico niet kunnen inschatten). Kiezen voor de 110% oplossing.
Ik zie geen beperkingen, omdat er voldoende, door de Nederlandse overheid goedgekeurde (AIVD/NBV) producten/oplossingen verkrijgbaar zijn, bij voorkeur van Nederlands fabrikaat. Specifieke oplossingen kennen een doorlooptijd tot goedkeuring die vertragend werkt (zeer lang en moeizaam proces, via WBI aangestuurd naar AIVD/NBV).
Koppelvlakken tussen extern Hosted Public Cloud en interne, bestaande IT en Private Clouds stellen zeer hoge eisen om aanvallen van buiten af te slaan.
Continuïteit van de netwerkverbinding en bandbreedte (+latency) ter plaatse waar het nodig is, gegeven de soms extreme omstandigheden waar defensie mee geconfronteerd wordt.
Focus op de data.
Koppeling Hybride platformen (DC/Cloud).

IT Beveiliging

Inhoudsopgave

1 Feedback op DoIT

1.1 Vindt u dat DoIT 0.7 op het gebied van IT Beveiliging de definitieve versie mag worden? (dus geen aanpassingen meer)

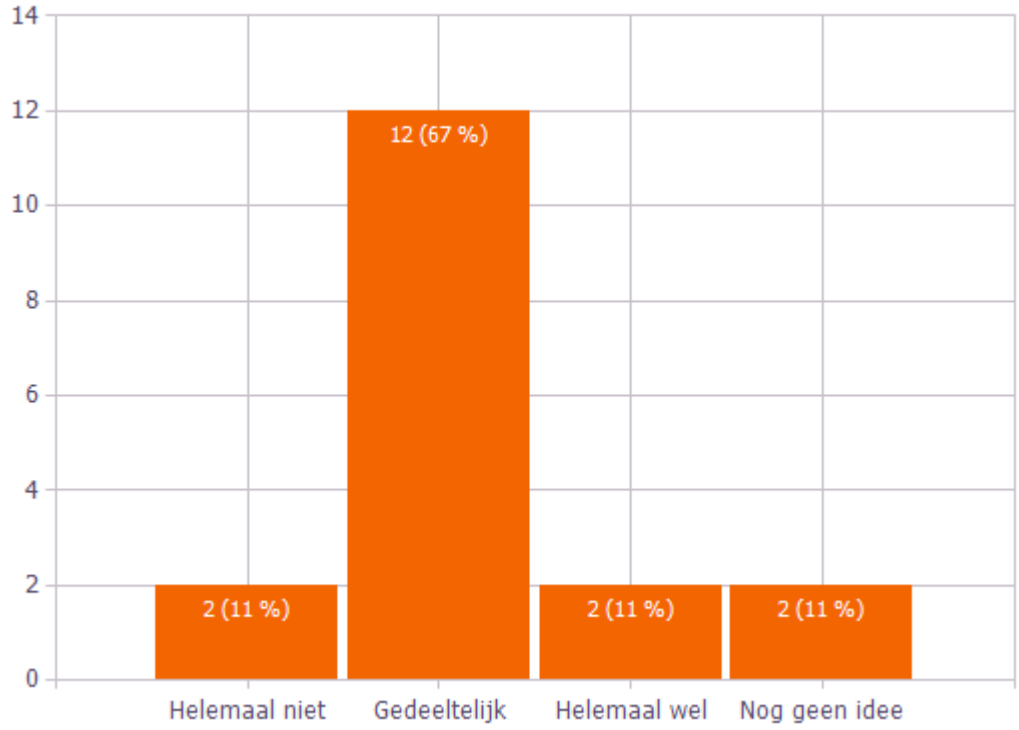


Aantal antwoorden 19

Antw.	Nummer	Percentage
Ja	7	37%
Nee	12	63%

1.2 In hoeverre acht u de ambitie van Defensie haalbaar voor de 1ste oplevering van de groeikern?

Denk hierbij onder andere aan de beschikbare tijd, de omvang van de werkzaamheden, één uniforme werkplek, Alles als een service aanbieden, de Defensie Appstore of de doelstelling dat binnen 5 jaar uit huidige realisatiedomein opgeheven kan worden.



Meerkeuze optie: Helemaal niet

Antwoord
De remmende factor is het meekrijgen van de Defensie-organisatie en daar lezen we weinig over.
Politiek, te log apparaat. Analoge managers. Denkwijze Militair en Burger liggen te ver uit elkaar.

Meerkeuze optie: Gedeeltelijk

Antwoord
In principe is 5 jaar ruim voldoende om een transitie door te voeren. Echter dienen aan aantal zaken aan het begin goed te worden neergezet: mandaat programma, heldere productomschrijvingen, etc.
Tijdslijn is te ambitieus. Een aantal oplossingen zijn nog niet helder genoeg. Bijv.: IAM is essentieel en nog niet in voldoende detail uitgewerkt.
Hangt af van governance en cultuuromslag binnen Defensie.
Nog teveel voor interpretatie vatbaar, te algemeen/theoretisch.
Tegelijkertijd geldt voor beveiliging als voor geen andere discipline de uitspraak “de devil is in the detail”. Principes en ambities zijn noodzakelijk, maar goede, gestructureerde en gecontroleerde aanpak tijdens ontwerp, implementatie, ingereedstelling, gebruik en onderhoud met een hoge mate van bewustzijn van alle betrokkenen zijn minstens zo belangrijk.
Afhankelijkheden richting Budgetten.
De ontvlechting van toepassingen kan lastig zijn. De aanpak van de migratie is geen garantie voor snelle en effectieve oplossingen.
De hele opzet gaat uit van het feit dat Defensie een open en vertrouwde cultuur heft, waarin open over

Antwoord
beveiliging en falen hiervan kan worden gesproken en gehandeld. Onbekend is of deze situatie zich ook daadwerkelijk voordoet. Gezien de sterk hiërarchische opzet is dit maar de vraag.
Veranderingen met deze omvang kosten eenmaal veel tijd binnen de overhead.
Is mogelijk, maar hangt af van meerdere zaken/randvoorwaarden. o.a. scoping, aansluiten bij markt-product standaarden, sterke governance/ besturing/ doorzettingsmacht.
Historie heeft geleerd dat vaak meer tijd nodig is. Binnen een jaar kan wel een groeikern worden neergezet, maar is het de vraag of deze bevat wat Defensie nu voor ogen staat. De eisen zijn nog niet allemaal concreet genoeg voor een aanbesteding.

Meerkeuze optie: Helemaal wel

Antwoord
Current design is haalbaar met huidige stand van technologie. Gefaseerde implementatie. Wel gebaseerd op beschikbare fondsen.
Haalbaar mits een juiste interactie met de markt, wat dus ook afhankelijk is van de methode van verwerving en de regelgeving m.b.t. tenderen.

Meerkeuze optie: Nog geen idee

Antwoord
Hangt af van budget, mogelijkheid tot standaardisatie op te leggen en mandaat die toegekend worden.

1.3 Kunt u uw feedback geven op het gedeelte IT Beveiliging in het DoIT

Inleiding

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Helder
De doelgroep en doelstelling van het document zou nog kunnen worden toegevoegd.
Geen opmerkingen
Ja
OK
Duidelijk

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
In de inleiding zou een toelichting over hoe deze set aan documenten gebruikt gaat worden in de volgende fases een welkome aanvulling zijn. Voorbeeld: de DO-It documenten worden gehanteerd als toetsingskader van de aanbiedingen van de RFP, waarna een selectie van partners gaat plaatsvinden, waarin in een transparante- en open samenwerking (Joined) het geheel verder wordt uitgewerkt.
Ok.
Het is onvoldoende duidelijk voor wie het geschreven is en wat de lezer ermee moet kunnen doen. Hierdoor is een inhoudelijke toetsing lastig.
Is ok.

Basisprincipes informatiebeveiliging nieuwe IT

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Helder.
Helder.
Goed om basisprincipes als basis te hanteren. Basisprincipes moeten altijd goed worden afgewogen ten opzichte van wendbaarheid.
Geen opmerkingen.
Goed beschreven.
Beveiliging model vergelijkbaar met dat van US government.
Als basis ok.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Zijn behoorlijk beschreven. Er is wel wat ongelijksoortigheid in het abstractieniveau. BP25 is bijv. veel concreter dan BP21. Er moeten ook nog wat keuzes gemaakt worden. BP29 lijkt te breed gedefinieerd. Kan niet voor alle devices gelden. Er zijn dilemma's, waarin keuzes moeten worden gemaakt, die niet expliciet worden geadresseerd.
Ok.
In detail uitwerken waar welke beveiligingseisen moeten worden toegepast, waarbij ook uitzonderingen in tijd en lokatie mogelijk kunnen zijn.
Met de basisprincipes kun je het moeilijk oneens zijn, gezien het feit dat deze op een redelijk hoog abstractieniveau gedefinieerd zijn. Wat niet duidelijk is is hoe en onder welke voorwaarde dit gerealiseerd gaat worden. Bijv. Encryptie is essentieel, maar er zijn geen eisen gedefinieerd over Enterprise Key & Certificate management.
Pas als doelgroep en doelstelling van het document en dit deel duidelijk zijn, kan een oordeel gegeven worden over de duidelijkheid van dit deel.
De visie welke Defensie beschrijft, is dermate algemeen, dat deze altijd juist is. De principes en uitgangspunten zijn "tekstbook" principes en daarom zeker niet onjuist. De groeikern maakt het geheel iets concreter, maar nog is de vraag welke verandering Defensie nu daadwerkelijk door wenst te voeren.

De gebruiker centraal

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Door vanuit de gewenste effecten te acteren kan dit worden geborgd. Duidelijk.
Als uitgangspunt duidelijk.
Duidelijk

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Uitwerken soort gebruiker en omstandigheden.
Goed streven. Praktijk kan uitdagend zijn, met de vele mensen en smaken. Daarbij kan met name voor HGI de kans bestaan dat hier vanuit Security perspectief enkele concessies gedaan dienen te worden. Goed om hier verwachtingsmanagement te doen.
Pas als doelgroep en doelstelling van het document en dit deel duidelijk zijn, kan een oordeel gegeven worden over de duidelijkheid van dit deel.
Vanuit de visie is niet duidelijk omschreven welke typen gebruikers er zijn en welke rubricering van toepassing is. Informatie staat centraal, dus integriteit moet zijn geborgd.

Antwoord
De visie welke Defensie beschrijft, is dermate algemeen, dat deze altijd juist is. De principes en uitgangspunten zijn "tekstbook" principes en daarom zeker niet onjuist. De groeikern maakt het geheel iets concreter, maar nog is de vraag welke verandering Defensie nu daadwerkelijk door wenst te voeren.

De business centraal

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Goed beschreven.
Zeer goed beschreven.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Zijn goede uitgangspunten, maar het zou goed zijn om een aantal dilemma's te pakken en hierop keuzes te maken. Sommige zaken conflicteren.
Welke omstandigheden kennen we en wat zijn de beveiligingseisen daarvoor?
Goed beschreven! Wat de business wil en wat de gebruiker wil kan mogelijk uit elkaar liggen. Hoe worden deze twee werelden zo goed mogelijk bij elkaar gebracht?
Is slechts op hoofdlijnen aangegeven, bedrijfsvoering en operatie. Ik kan me hier wel wat bij voorstellen, maar het zijn 2 volledig andere grootheden met andere relaties en afhankelijkheden, dus ook informatie integriteit. Opmerking: de visie zou meer moeten zeggen over informative-integriteit.
Pas als doelgroep en doelstelling van het document en dit deel duidelijk zijn, kan een oordeel gegeven worden over de duidelijkheid van dit deel.
De visie welke Defensie beschrijft, is dermate algemeen, dat deze altijd juist is. De principes en uitgangspunten zijn "tekstbook" principes en daarom zeker niet onjuist. De groeikern maakt het geheel iets concreter, maar nog is de vraag welke verandering Defensie nu daadwerkelijk door wenst te voeren.

Gehele hoofdstuk irt document

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Helder.
Geen opmerkingen.
Beveiliging architecture is goed. Multiple enclaves en cross domail guards in place to limit access to applications and data.
Als Defensie ontwerp beveiliging voldoende toegelicht. Ook omdat er wordt verwezen naar deelrapport A. Echter dient er een concrete vertaalslag te worden gemaakt van doelstellingen naar tastbare resultaten die meetbaar, acceptabel en tijdgebonden zijn.
Het opheffen van onderscheid tussen groene en witte IT is een goed uitgangspunt.
Goed.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Behoeft detailuitwerking op het gebied van politiestaat (IAM).
Het ontwerp dient voldoende te worden vertaald naar specifieke, meetbare en tijdgebonden beschrijvingen van het eindresultaat om een goede vertaalslag naar een programmaplan te kunnen maken.
Het Jericho principe kan verder worden uitgewerkt door pro-actieve segmentering toe te voegen.
De principes en uitgangspunten zijn vaak zo beschreven dat ze bijna altijd zijn in te vullen. Of dit dan tot een

Antwoord
werkende oplossing gaat leiden is nog niet geheel duidelijk.
Defensie is uniek in haar eisen voor het operationele domein. Een dergelijke omgeving die onder andere gekenmerkt wordt door het “disadvantaged information grid” met lage netwerkcapaciteit en beperkte bereikbaarheid, legt bijvoorbeeld zijn beperking op aan monitoring- en detectieoplossingen die in netwerken met een vaste infrastructuur soms al uitdagend genoeg zijn. Het evenwicht tussen preventieve en detectieve maatregelen zal hier meer moeten hellen naar preventieve maatregelen en monitoring en detectie zal lokaal op endpoints moeten worden ingericht en met vertraging centraal beschikbaar worden gesteld voor eventuele analyse.
Uit ervaring weten wij dat beschikbaarheid vaak weinig aandacht krijgt door beveiligingsfunctionarissen. Vaak staat DDOS-bescherming nog wel op het netvlies, maar een geïntegreerd plan om de beschikbaarheid en herstel bij calamiteiten te garanderen laat soms te wensen over. Uiteraard is beschikbaarheid minstens zo belangrijk is als exclusiviteit en integriteit, zeker vanuit het defensie-oogpunt waarbij de eisen nog hoger zijn dan bij andere enterprises. Honderd procent beschikbaarheid over de volle breedte toepassen is echter niet altijd realiseerbaar en duur. Een gedifferentieerde aanpak in relatie met een goed business continuity plan en een disaster recovery plan is dan ook noodzakelijk om tot een realistische aanpak te komen. Per service moet bekeken worden welke eisen er gelden voor beschikbaarheid en recovery.
Pas als doelgroep en doelstelling van het document en dit deel duidelijk zijn, kan een oordeel gegeven worden over de duidelijkheid van dit deel.
De visie welke Defensie beschrijft, is dermate algemeen, dat deze altijd juist is. De principes en uitgangspunten zijn "tekstbook" principes en daarom zeker niet onjuist. De groeikern maakt het geheel iets concreter, maar nog is de vraag welke verandering Defensie nu daadwerkelijk door wenst te voeren.
Bijzondere aandacht vraagt ook het werken met data van verschillende classificatieniveaus in dezelfde omgeving. Ook hier geldt weer dat encryptie belangrijk is, maar ook het categoriseren, het labelen en het volgen van informatie door de gehele keten is van belang. onze organisatie adviseert hier een uitgebalanceerde moderne DLP oplossing, die geïntegreerd is met de SIEM functionaliteit.

2 Logische stappen

2.1 Is het op het gebied van IT Beveiliging mogelijk om "Act small" te doen, irt "Think Big"?

Motiveer uw antwoord alstublieft op de volgende wijze;
Ja: Kunt u voorbeelden geven van (kleine) stappen die we kunnen doen.
Nee: Wat zijn belemmeringen en hoe kunnen deze weggehaald worden?

Meerkeuze optie: Ja

Antwoord
Definiëren van strategie en rules.
SOC inrichting, monitoring uitbrein, thead intelligence verbreden.
Directe contracten met kleine gespecialiseerde (niche) marktpartijen.
Voorbeeld van Act Small met big impact: in patch management, focus op 10 meest bekende vulnerabilities (verantwoordelijk voor 90% van Exploits (DBIR rapport 2015). Zorg dat patches binnen 6 maanden na publicatie worden uitgevoerd (Microsoft geeft aan dat na eerste 6 maanden van een nieuwe release, de eerste exploits verschijnen)
Big: bepalen beveiligingsstandaarden, wijze koppelingen van netwerken, Centrale deployment naar zowel statisch als uitgestegen. Eisen aan apparatuur. Tijdslijnen van leveren van apparatuur in lijn met Defensie tijdslijn. Small: bij elke oplevering van applicatie pentesten en hertesten, SOC monitoring eerst meest kritische onderdelen. Wel kunnen acteren bij dreiging. Dit moet vanaf het begin ten volle werken.
Eerst aansluiten waar NCIA/MIVD en AIVD mee bezig zijn en waar grootste nadruk en dreiging op ligt. Welke innovatieve partijen en oplossingen gebruiken zij al. En maak kerngroepjes van hoog innovatieve bedrijven, die een snelle en gezamenlijke oplossing kunnen brengen. Geef ook de ruimte om te kunnen testen en te laten fallen.
Zorg in een vroeg stadium voor voldoende test opties op basis van Use Cases.
Allereerst moet de infrastructuur van de groeikern goed gedefinieerd zijn. Vervolgens keuze maken voor een type ESB.
De leverancier of projectleider empowerment verandering op te leggen en flexibiliteit gebruiker beperken om zo te standaardiseren.
Bij een uitvraag aan martkpartijen zorgen dat beveiliging er integraal onderdeel van uitmaakt. Dit kan ook bij een kleine/gespecialiseerde uitvraag.
Vaststellen van de principes (think big) en in stappen cq. gelaagdheid implementeren/doorvoeren (act small), bijvoorbeeld data centrische benadering, zonering, beschikbaarheid, etc.
De verschillende aspecten van de nieuwe IT Beveiliging kunnen per applicatie in verschillende fases worden geïmplementeerd, bv. beschikbaarheid kan in een ander release verhoogd worden dan continuiteits- of security verbeteringen.
Werk zo snel mogelijk met abstractie van de infratructuur, zodat hardware afhankelijkheden wegvallen.
Ownership duidelijk definiëren binnen Defensie.
Bij voorkeur toepassen van Nederlands fabrikaat crypto, dit ook vanwege de reeds aanwezige goedgekeurde producten. Zorg voor modulaire opbouw, voorkom een verdor lock-in, maak de modules niet te groot, zorg voor comptabiliteit door het zoveel mogelijk toepassen van open standaarden.
Beveiliging alleen voor dat deel van de IT te regelen, die op dat moment wordt neergezet (bijv de groeikern).
Beginnen met de kantoorautomatisering (virtuele werkplekken).
Blijvende vernieuwing vormgeven door samenwerking in stand te laten tijdens levernsduur platform en middels innovatieboard ruimte te bieden voor innovatie/ start-ups (op basis van Business Case).
Specifieke security services inrichten, zoals Identity management, Authenticatie diensten, certificaatbeheer.
Binnen de groeikern starten met subcomponenten.
Think big moet in de voorbereidingen gedaan worden. Beveiliging moet in de breedte ontworpen worden. Implementatie en uitrol moet op basis van act small uitgevoerd worden om risico's te managen.
Voorkomen van maatwerk.

Antwoord
Scoping en fasering definieren in de samenwerking, zoals gedefinieerd (basisproducten, sprints, etc.)
Concreet zou ik adviseren te beginnen met een, volledig door een marktpartij geleverde en beheerde, Generatie 4 DC container, waar IaaS, PaaS en bovengenoemde SaaS services kunnen worden afgenomen. De "klanten" van IaaS en PaaS krijgen de beschikking over een volledig door de markt beheert portaal, waardoor de inkoop, de ITSM processen en andere ondersteunende diensten (F&C) van Defensie geen belemmeringen meer vormen. Nieuwe ontwikkelde diensten zoals Sharepoint, UC en BPM kunnen vanuit deze Cloud worden afgenomen. Door het beheer (tijdelijk) bij een marktpartij te beleggen kan de beheerlast optimaal worden gebenchmarkt en de nieuwe beheerorganisatie worden gevormd.
Indien het Defensie leiderschap de mensen kan opleggen flexibel te zijn en zich aan te passen, kan IT grootste dingen verwezenlijken met kleine stappen.
Samenwerking definieren tussen Defensie en geselecteerder partners.
Leverancier-/partnerselectie op basis van standard portfolio/Dienstverlening.

Meerkeuze optie: Nee

Antwoord
Een voorbeeld van deze service architectuur is "positiebepaling vijandig doel" (gewoon een verzonnen situatie, die middels informatie moet worden aangegeven aan de gebruiker "soldaat in het veld"). Dit kan als los object worden geprogrammeerd en in de nieuwe DoIT worden opgenomen. Zo kun je Big denken en snel en efficient een resultaat bereiken. De ontsluiting is dan initieel middels de "oude" IT en kan later over worden geheveld naar de "nieuwe" IT.
Digitale weerbaarheid kan alleen gerealiseerd worden wanneer er over de volle breedte van een organisatie maatregel en waarborgen getroffen worden. het gaat dus om het samenspel van activiteiten. Act small brengt het risico met zich mee dat er slechts op deelgebieden maatregelen genomen worden en er dus schijnzekerheid ontstaat.
IT beveiliging kan men niet een "beetje" doen. Een kleinere kern in het begin betekent niet dat er minder beveiliging nodig is.
Beveiliging is net als andere niet-functionele aspecten van IT (performance, schaalbaarheid, etc) een fundamentele eigenschap van een IT-oplossing die "mee moet worden ontworpen". Doorgaans is dit slechts achteraf toe te voeren of aan te scherpen.
De huidige migratie aanpak zorgt niet voor voldoende duidelijke en "losse stukjes". Ik zou een service architectuur adviseren, waar middels object georiënteerde aanpak functies worden overgezet naar DoIT. Nu is er geen service architectuur, maar zijn er traditionele services benoemd.

2.2 Feedback op de genoemde kleine stappen

Meerkeuze optie: Verrijking

Voorkomen van maatwerk

Antwoord
Het maximaliseren van standaardisatie brengt het grootste positieve effect met zich mee, snelle migratie, grote stap voor de gebruikers van Defensie, kleine stap qua inspanning en IT migratie.

Think big moet in de voorbereidingen gedaan worden. Beveiliging moet in de breedte ontworpen worden. Implementatie en uitrol moet op basis van act small uitgevoerd worden om risico's te managen.

Antwoord
Er zal eerst een compleet fundament neergezet moeten worden, dat alle aspecten benoemd, voordat er op een Agile methode verder gewerkt kan worden. Gezien de tijdslijnen zal dit fundament zo dicht mogelijk bij een marktconforme oplossing moeten liggen. Dit maakt dat een (beperkt) aantal eisen niet in de eerste fase kunnen worden geïmplementeerd.
Wij vinden de omvang van de nieuwe werkplek initieel vrij groot. Maak dit kleiner waar het kan.

Beginnen met de kantoorautomatisering (virtuele werkplekken)

Antwoord

Opbreken in kleinere iteraties (eerst LGI, dan HGI).

Bij voorkeur toepassen van Nederlands fabrikaat crypto, dit ook vanwege de reeds aanwezige goedgekeurde producten. Zorg voor modulaire opbouw, voorkom een verdor lock-in, maak de modules niet te groot, zorg voor comptabiliteit door zoveel mogelijk toepassen van open standaarden.

Antwoord

Inzet van de crypto zo breed mogelijk, waarbij dezelfde apparatuur zowel in NL als ook in coalitieverband kan worden ingezet en waarbij de exclusiveitswaarden zoveel mogelijk bewaakt blijven. Voorbeelden hierin zijn concepten die bij NCIA worden inzet, zoals Protected Core Networking.

Zorg in een vroeg stadium voor voldoende test opties op basis van Use Cases

Antwoord

Testen vanuit business needs, niet vanuit systeemspecs.

Directe contracten met kleine gespecialiseerde (niche) mmarktpartijen

Antwoord

Top. Onderstrepen wij. Juist de kleine Niche partijen kunnen dat extra brengen. Geef deze de ruimte om in contact te komen. Worden vaak door de Mastodonten weggedrukt. Regie wordt dan vaak ondermijnt ten koste van de Niche!

Meerkeuze optie: Feedback

Specifieke security services inrichten zoals Identity management, Authenticatie diensten, Certificaatbeheer.

Antwoord

Prima voorbeeld van act small, dit is de basis.

Beginnen met de kantoorautomatisering (virtuele werkplekken)

Antwoord

Onbelangrijk. Het laatst toepassen.

Allereerst moet de infrastructuur van de groeikern goed gedefinieerd zijn.
Vervolgens keuze maken voor een type ESB.

Antwoord

Zorg dat het wiel zo min mogelijk opnieuw wordt uitgevonden en dat er gebruik wordt gemaakt van intl standaarden om de definitiefase te versnellen.

2.3 Feedback op de genoemde belemmeringen

Meerkeuze optie: Feedback

IT beveiliging kan men niet een "beetje" doen. Een kleinere kern in het begin betekent niet dat er minder beveiliging nodig is.

Antwoord
Meer nog, beveiligen begint met kennis op doen over wat er bestaat en wie interesse heeft in Nederlandse MOD, hoe beter je je tegenstander kent/begrijpt/bestudeert, hoe meer/beter je je kan beschermen.
Act small kan, wanneer de impact van een risico helder is (wat in het beveiligingstuk staat). Act small kan dan, het is immers inzichtelijk wat er aan maatregelen wordt geïmplementeerd en welke risico's er overblijven (beheerst veranderen).
Verschillende IT heeft verschillende niveau's van beveiliging nodig. Het kan niet een beetje, maar er is wel een verschil tussen zware en lichtere beveiliging. Er moeten keuzes worden gemaakt (zo veel mogelijk beveiliging voor een euro).
Klopt, maar je kan de scope waar je het op toepast wel klein maken.
Er zal eerst een compleet fundament neergezet moeten worden wat alle apecten benoemd voordat er op een Agile methode verder gewerkt kan worden. Gezien de tijdsijnen zal dit fundament zo dicht mogelijk bij een marktconforme oplossing moeten liggen. Dit maakt dat een (beperkt) aantal eisen niet in de eerste fase kunnen worden geimpementeerd.
Je kunt wel de attack servers verkleinen (act small).

3 Governance

3.1 Hoe ziet u de verdeling van verantwoordelijkheden van de IT-Beveiliging in de exploitatiefase

Meerkeuze optie: Verantwoordelijkheid Defensie

Antwoord
Opmerking: U heeft aangegeven voor een "Best of Breed" aanpak te gaan met leveranciers. Dit resulteert in de noodzaak voor een integrator rol, integratie van deze Best of Breed. Die regie lees ik nu als Defensie verantwoordelijkheid, het is de vraag of deze expertise altijd aanwezig zal zijn. Defensie zit met een uitdaging in deze.
Het kunnen bemensen van het SOC dient door goed getraind defensiepersoneel te worden uitgevoerd, die continue met nieuwe kennis worden gevoed en scherp blijven door ze ook op andere cyber onderdelen in te zetten.
Bij de markt kan sprake zijn van potentiële overnames, waardoor het landschap kan veranderen. Beveiliging wordt lastig als een marktpartij opeens wordt gekocht door een bedrijf vanuit een land/gebied waar wij minder of geen militaire relatie onderhouden. Bij een keuze voor de markt kan moeilijk governance worden ingespoeld. Wat hier ook een rol speelt is het eigenaarschap van de data die beveiligd moet worden.
Migratie is verantwoordelijkheid van Defensie met Markt in een advisory capacity. Ook d.m.v. van een steering comité voorgezeten door defensie.
Het accepteren van restrisico's.
Vaststellen aanpassingen IT Beveiligingsbeleid.
De eindverantwoordelijkheid voor de productiefase zal bij defensie moeten liggen. Defensie wordt ook geacht op het vlak van beveiliging de eigen broek op te houden. Echter voor specialistische taken zal de kennis niet altijd aanwezig zijn en zal Defensie marktpartijen moeten kunnen betrekken. Voor die individuele deelgebieden zijn de marktpartijen dan verantwoordelijk. Daar waar het uitbestede en/cloud diensten zijn, is defensie verantwoordelijk voor kaderstelling en toezichthouden. De marktpartijen zullen binnen de door defensie gestelde kaders de beveiligingskosten moeten invullen.
Innovatie van huidige diensten (verbeteren wat er wordt ingezet).
HGI defensie met Modern regie (SPOT) LGI Markt met regie Defensie (SPOT) (BOP).
Penetratietesten (initiatie hiervan).
Binnen laaggerubiceerd valt ook Stg. Confidentieel. Dit zou voor beheer eerder bij defensie behoren te liggen dan bij de markt. Dep. vertrouwelijk kan in principe door de markt worden beheerd.
Controleert de markt (op basis van beveiligingseisen).
In beginsel kun je als Defensie taken delegeren naar andere partijen, maar Defensie blijft eindverantwoordelijk. Een goed governancemodel benoemt de mate van over te dragen verantwoordelijkheid, maar dan ook inclusief stuurmiddelen om die taak uit te voeren.
Audit functie.
ICT voor operaties (veld).
Defensie zal de regie moeten houden, waarbij ze gebruik maken van kennis uit de markt om te verrnieuwen.
Defensie vraagt functioneel uit; de markt levert en moet aantonen aan de gestelde eisen en richtlijnen te voldoen.
Maakt risico-inschattingen
Beveiligingsbeheer t.b.v. geleverde diensten uitvoeren.
Integrale beheer (dit omdat HGI beheer altijd bij Defensie ligt en LGI mogelijk bij de markt).
Controle op naleving. Onderhouden beleid. Regie op onderhoud tijdens exploitative. Eigenlijk de meeste Planning- / en controlverantwoordelijkheden.
Verantwoordelijk voor publicatie en onderhoud beveiligingseisen.
Hooggerubriceerd dient vanwege gevoeligheid bij Defensie te liggen, ongeacht statisch of uitgestegen.
Regie functie.

Antwoord
Business owner en coördinatie regiefunctie.
Cyber crisis management uitvoeren/regie voeren.
Indien HGI-systemen geheel door Defensie beheert dienen te worden, zal Defensie het SOC moeten doen.
Opstellen rollen/profielen.
Beveiligingsbeleid vaststellen/bijgestellen.
Impact analyse/ vaststelling van onderkende veiligheids risico's.
Strategische regie (integrator role) over de verschillende partijen.
Business beveiligingseisen vaststellen.
Is kerntaak van Defensie.
Gebruikersbeheer.
Regie met andere kavels/onderdelen.

Meerkeuze optie: Verantwoordelijkheid Markt

Antwoord
Rapporteert over beveiligingsincidenten.
Markt is verantwoordelijk voor kennisoverdracht /kennisdeling en geeft gevraagd en ongevraagd advies, Defensie beslist op basis van deskundig advies over de in te zetten oplossing.
Is voorbereidt op migratie van beveiligingsincidenten.
Actueel houden (technische) risicoanalyse.
Productie is verantwoordelijkheid van Markt met 'Government oversight'. Dus d.m.v. een steering comité voorgezeten door defensie.
Er kan voor veel zaken gesproken worden over het delegeren van verantwoordelijkheden richting de markt (met name voor LGI), mits de business impact en regels maar bepaald worden door Defensie.
Ondersteunt bij risicobeslissingen door het leveren van technische expertise en waarschijnlijkheidsanalyse.
Voorstellen aanpassingen IT Beveiligingsbeleid.
Informeert over dreigingen.
Innovatie (nieuwe technologie) toekomst gericht denken als advies.
Beveiligingsupdates realiseren en uitrollen voor zover deze betrekking hebben op de afgesproken IT-diensten.
Aandragen innovatie/vernieuwingsvoorstellen.
Ontwikkeling van de applicaties.
Defensie vraagt functioneel uit; de markt levert en moet aantonen aan de gestelde eisen en richtlijnen te voldoen.
Beveiligingsincidenten managen en Defensie informeren.
Functioneel beheer (deel-)oplossingen.
ICT voor bedrijfsvoering beheren (outsourcing).
Uitvoering, monitoring en rapportage.
Beheer en exploitatie.
Technisch beheer geboden (deel-)oplossing.
Technisch beheer van de systemen (operations, patching, deployment etc.).
Product specialismen.
Producten/diensten met passende beveiliging leveren.
Operationele regie (integrator role) over de verschillende partijen.
Technologische Innovatie.
Security in IAAS laag.

4 Realisatie IT Beveiliging

4.1 Waar liggen volgens u, op het gebied van de realisatie van de IT Beveiliging, de drie grootste uitdagingen?

Antwoord
Opzetten ISO 27001.
De beveiliging raakt alle organisatorische geledingen, principes en systemen. Dit vereist een governance en effectiviteit die defensie niet gewoon is in vredestijd.
Kunnen testen in context van het gehele ecosystem, inclusief partners.
Aansluiting missies op statisch domein
De hoofdaandacht zal de komende tijd uitgaan naar de Groeikern. Deze oude omgeving zal logischerwijs steeds meer kwetsbaarheden gaan vertonen. Door de Security & Information Assurance Services primair op de groeikern te richten, bestaat het risico dat de oude omgeving minder wordt bewaakt, terwijl deze juist het beste zou moeten worden bewaakt.
Het vertalen van een groot aantal, op zich zinnige, eisen in pakketten zodat ze kunnen worden meegenomen in de aanbestedingen.
Het vinden van kwalitatief hoogwaardige security experts, in een markt waarbij de industrie betere arbeidsvoorwaarden kan bieden.
Het aantrekken en behouden van beveiligingsexperts.
Can do mentaliteit militairen.
Het werken met data van verschillende classificatieniveaus in dezelfde omgeving. Ook hier geldt weer dat encryptie belangrijk is, maar ook het categoriseren, het labelen en het volgen van informatie door de gehele keten is van belang
Aanpassen van procedures en policy met technology. Procedures en policy consistent across de Defensie-organisatie.
Aansluiting security infra bij joined missies in het buitenland bij samenwerking andere krijgsmachten.
Het samenkomen van HGI en LGI op de werkplek.
Defensieinformatie adequaat beveiligen in de transitieperiode. De groeikern en de oude wereld. Hoe blijft configuratie management actueel?
Kerncomponenten, die voor de first line of defence zorgen en een hoog innovatief karakter hebben, om deze te kunnen meenemen in de groeikern
Governance/samenwerking: er zal een open en transparante samenwerking tot stand moeten komen tussen de te selecteren partijen en Defensie, waarbij op basis van gelijkheid tot werkende oplossingen wordt gekomen. Dit is een andere manier van samenwerking dan tot nu toe.
Keuzes maken ten aanzien van welke IT via welk sourcing model geleverd kan worden op basis van beveiligingsoverwegingen. Bijvoorbeeld welke services uit de groeikern kunnnen/mogen uit de cloud worden afgenomen?
Beveiliging tijdens de migratie (veilig tijdens de verbouwing).
Beperken van toegang tot informatie t.o.v. een stijgende vraag naar meer toegang van de gebruikers.
Adoptieve organisatie open voor verandering.
Inregelen van een goede en onafhankelijke Quality Assurance-rol van een partij, die over de volle breedte van het onderwerp expertise heeft.
Agility is dus niet alleen van belang bij het ontwerpproces, maar noodzakelijk voor de gehele beveiligingsfunctie. Belangrijk is hierbij om nauwkeurig te formuleren wanneer de beveiliging van een service succesvol is (KPI's), en ervoor te zorgen dat er voldoende aandacht is voor het lerende vermogen.
Overgang beheer bij inzet van appratuur op missie.
Samenwerking met andere mogendheden (informatie delen, eigenaarschap).
Kennis.
HGI en LGI binnen hetzelfe ecosysteem (netwerk, werkplek, etc).
Actueel houden van het gewenste niveau van beveiliging.
Interfacing Hybrid Cloud/DC.
Gebruikersbewustzijn (phishing is voorlopig grootste veroorzaker van beveiligingsincidenten).

Antwoord
De tijdige realisatie van een single werkplek waar je zowel hooggerubriceerde als laaggerubricceerde gegevens kan benaderen.
De ambitie is volledig, maar de implementatiestrategie en volgorde bepaald het succes.
Uiteindelijk objectief, timing en budget verenigen in een realistisch plaatje.
Integriteit van informatie is de kern van DoIT en daarmee van IT beveiliging (juiste informatie tijdig voor de juiste gebruiker).
Principes en ambities zijn noodzakelijk, maar goede, gestructureerde en gecontroleerde aanpak tijdens ontwerp, implementatie, ingereedstelling, gebruik en onderhoud met een hoge mate van bewustzijn van alle betrokkenen, zijn minstens zo belangrijk.
LGI, HGI, statisch en deployed in 1 keer realiseren.
Het behalen van de ambities zal vooral in de mens en proceskant zitten. Zolang Defensie zich zorgen maakt over het inhuren van schaarse capaciteit of de kostendekking van resources op het gebied van Beveiliging, wordt op input gestuurd en niet op het resultaat. Door deze sturing zullen de ambities, hoe realistisch deze ook zijn, niet worden behaald.
Interfacing naar de Infrastructuur/Cloud olpossingen. Deze moeten op elkaar worden afgestemd (in RFP fase of direct daarna).
Agile Governance.
Verkrijgen en behouden van voldoende goede eigen specialisten.
Budget.
Voortschrijdende technologie t.a.v. cybercrime.
Samenwerking irt Open Innovatie.
Keuze van de oplossingen.
Snelheid, kennis, adoptieve organisatie open voor verandering.
IAM.
Zorgen voor een integrale benadering op cyber security.
Vaststellen migratie van huidg naar nieuw.
Sterke authenticatie.
Juiste uitvraag aan de markt.
Innovatie.

4.2 Hoe groot schat u de genoemde uitdaging in?

Geef uw mening op een schaal van 1 - 10, waarbij
1 = helemaal geen uitdaging
10 = zeer grote uitdaging

Onderdeel	-	Gemiddelde van de score	St.dev.
Het aantrekken en behouden van beveiligingsexperts.		8,0	2,0
Snelheid, kennis, adoptieve organisatie open voor verandering.		7,6	1,8
Het behalen van de ambities zal vooral in de mens en proceskant zitten. Zolang Defensie zich zorgen maakt over het inhuren van schaarse capaciteit of de kostendekking van resources op het gebied van Beveiliging, wordt op input gestuurd en niet op het resultaat. Door deze sturing zullen de ambities, hoe realistisch deze ook zijn, niet worden behaald.		7,4	1,7
Voortschrijdende technologie t.a.v. cybercrime.		7,4	1,6
Governance/samenwerking: er zal een open en transparante samenwerking tot stand moeten komen tussen de te selecteren partijen en Defensie, waarbij op basis van gelijkheid tot werkende oplossingen wordt gekomen. Dit is een andere manier van samenwerking dan tot nu toe.		7,3	1,6
LGI, HGI, statisch en deployed in 1 keer realiseren.		7,1	1,6
juiste uitvraag aan de markt.		7,0	1,9
Uiteindelijk objectief, timing en budget verenigen in een realistisch plaatje		6,9	1,9
Inregelen van een goede en onafhankelijke Quality Assurance-rol van een partij die over de volle breedte van het onderwerp expertise heeft.		6,8	1,9
Budget.		6,7	2,1
De ambitie is volledig, maar de implementatiestrategie en volgorde bepaald het success.		6,5	1,9
De hoofdaandacht zal de komende tijd uitgaan naar de Groeikern. Deze oude omgeving zal logischerwijs steeds meer kwetsbaarheden gaan vertonen. Door de Security & Information Assurance Services primair op de groeikern te richten, bestaat het risico dat de oude omgeving minder wordt bewaakt, terwijl deze juist het beste zou moeten worden bewaakt.		6,5	2,1
Zorgen voor een integrale benadering op cyber security.		6,4	2,2

Onderdeel	-	Gemiddelde van de score	St.dev.
Kunnen testen in context van het gehele ecosystem, inclusief partners.		6,3	1,7
IAM		6,3	2,2
Beperken van toegang tot informatie t.o.v. een stijgende vraag naar meer toegang van de gebruikers		5,9	1,4
Aanpassen van procedures en policy met technology. procedures en policy consistent across de Defensie-organisatie.		5,9	1,6
Integriteit van informatie is de kern van DoIT en daarmee van IT beveiliging (juiste informatie tijdig voor de juiste gebruiker).		5,8	2,3
Interfacing naar de Infrastructuur/Cloud oplossingen. Deze moeten op elkaar worden afgestemd (in RFP fase of direct daarna).		5,4	1,8
Interfacing Hybrid Cloud/DC.		5,2	2,4
Sterke authenticatie.		5,2	1,6
	1 2 3 4 5 6 7 8 9	6,6	2,0

4.3 Uitdagingen uitwerken

4.3.1 Grootste uitdaging Het aantrekken en behouden van beveiligingsexperts

Meerkeuze optie: Gekozen oplossing

Antwoord
Expert boeien met unieke kenmerken van het werken van Defensie (bijzonder threat model, bijzondere bevoegdheden, intl context). Aantrekkelijk maken door veel te investeren in opleiding, carrièreperspectief. Creëren van omgeving, waarin beveiligingsexperts zich thuisvoelen (subcultuur). Extern inhuren van experts voor specifieke kennis.
Als voortijdig duidelijk wordt afgesproken hoe men van start gaat in een project en vervolgens Advisory Board vaststelt onder voorzitterschap van Defensie.
Aantrekkelijk maken door veel te investeren in opleiding, carrièreperspectief.

4.3.2 Grootste uitdaging Snelheid, Kennis, adoptieve organisatie open voor verandering.

Meerkeuze optie: Gekozen oplossing

Antwoord
Verandermanagement: - Bewustzijn. - Kennis nieuwe technologisische oplossingen - leren omgaan met. - Open staan voor innovaties (vermijdt not-invented-by-me) Proces inrichten, waarmee je innovatie een plaats geeft: innovatieboard - op basis van BC innovatie doorvoeren. Voor snelheid is het belangrijk dat er in kleine stappen innovaties worden toegevoegd (dan snel de eerste business effecten). Security bewustzijn doorvoeren tot de laatste man.

4.3.3 Grootste uitdaging Het behalen van de ambities zal vooral in de mens en proceskant zitten. Zolang Defensie zich zorgen maakt over het inhuren van schaarse capaciteit of de kostendekking van resources op het gebied van Beveiliging, wordt op input gestuurd en niet op het resultaat. Door deze sturing zullen de ambities, hoe realistisch deze ook zijn, niet worden behaald.

.

Meerkeuze optie: Gekozen oplossing

Antwoord
Draag zorg voor voldoende budget en resources en pas de sturing aan naar output. Dit vergt wel een sterke Quality Assurance rol.

Meerkeuze optie: Voordelen
Aantal antwoorden 0

Antwoord

4.3.4 Grootste uitdaging Voortschrijdende technologie t.a.v. cybercrime

Meerkeuze optie: Gekozen oplossing

Antwoord
Defensie heeft mogelijk moeite om cyber kennis in huis te houden, wat belangrijk is voor keuze en adoptie van nieuwe technologie. Veel samenwerking met de Certs, kennisinstituten en industrie. Betrokkenheid bij hackers collectieven. Een goede balans van preventie, detectie, response en Intell. Zorgen dat alles wat via Intell binnenkomt terugleidt naar de response en beschermende systemen.

4.3.5 Grootste uitdaging LGI, HGI, statisch en deployed in 1 keer realiseren.

Meerkeuze optie: Gekozen oplossing

Antwoord
Alhoewel technisch mogelijk is het risico/impact bij een menselijke fout veel groter (verkeerde User rights).
Koppel de beveiliging aan de rol van de defensiemedewerker, niet aan de werkplek of de toepassing.

4.3.6 Grootste uitdaging juiste uitvraag aan de markt

Meerkeuze optie: Gekozen oplossing

Antwoord
Veel aandacht voor interoperabiliteit en standaardisatie, met name op het gebied van koppelvlakken en interfaces.
Requirements management goed opzetten met als resultaat SMART requirements.
Aandacht besteden aan modulariteit en wendbaarheid van oplossingen.

4.3.7 Grootste uitdaging Uiteindelijk Objectief,Timing en budget verenigen in een realistisch plaatje

Meerkeuze optie: Gekozen oplossing

Antwoord
Eerste groeikern opsplitsen in kleinere segmenten. Deze groeikern is op dit moment te groot en daardoor niet realistisch.
Niet uitrollen over de hele organisatie maar per organisatie-onderdeel.

4.3.8 Grootste uitdaging inregelen van een goede en onafhankelijke quality assurance rol van een partij die over de volle breedte van het onderwerp expertise heeft.

Meerkeuze optie: Gekozen oplossing

Antwoord
QA Advies vanuit juist alle partners toevoegen, onafhankelijke partij laten beoordelen.
Vooraf afspraken met de partners ten behoeve van het Quality Assurance proces.

5 Business case

5.1 Met welke kostencomponenten voor de IT beveiliging moeten wij rekening houden tbv de businesscase?

Antwoord
Aanpassen legacy systemen cq. afstoten daarvan.
Kosten/budget voor innovatie (conform agile).
Verhouding statiisch vs OMUT.
Beveilgiing is een integraal aspect van alle IT. Het gaat dus om applicatie, infra, proces, personele kosten.
Cyber defensie onderzoek en ontwikkeling (cyber lab uitbreidingen).
Hardware onderzoek.
Kosten basisoplossing (in zijn geheel).
Instandhouding. Legacy.
Projectkosten en ondersteunende diensten, dienstverlening en services.
Conformeren met frameworks.
Hoeveelheid HGI vs LGI.
Uitbreiding SOC en SIEM functionaliteit.
Innovatie & ontwikkeling.
Aantal interfaces.
Blue en red teaming.
Testing.
Arbeid en kennis; eigen personeel en externen. Hardware zoals HSM, Cryptodevices, Software etc.. Aanpalende diensten en services, o.a. Ohgv Cyberresilliance.
Kosten voor validatie van oplossingen.
Unexpected threats.
Accreditatie kosten.
Opleidingskosten van letterlijk iedereen (bewustzijn creëren/vergroten).
Architectuurkosten voor de voorbereiding.
Hardware, software, specifieke klantontwikkelingskosten, installatie, configuratie, projectmanagement, eindaudit, training personeel, contractkosten, verwervingskosten, licentiekosten (eenmalig en jaarlijks terugkerend).
Integratie (herhalend) door aanpak middels "Best of Breed", dit zal zich herhalen.
Personele kosten, incl. verwerving.
Afvloeingskosten.
Opleiding.
Projectkosten.
Hangt af van de hoeveelheid kennis die jullie nu intern willen opdoen en behouden.
Reorganisatiekosten.
Totale beveiliging zou niet meer moeten kosten dan 30% van de Expected Loss (Gordon & Loeb Return on security investment).
Organisatie changekosten.
De verwachtte schade indien onvoldoende beveiligd wordt.
Opleidings- en trainingskosten.
Licenties.
Quality Assurance.
Codereview.
Training.
Onderhoudskosten hardware en software.

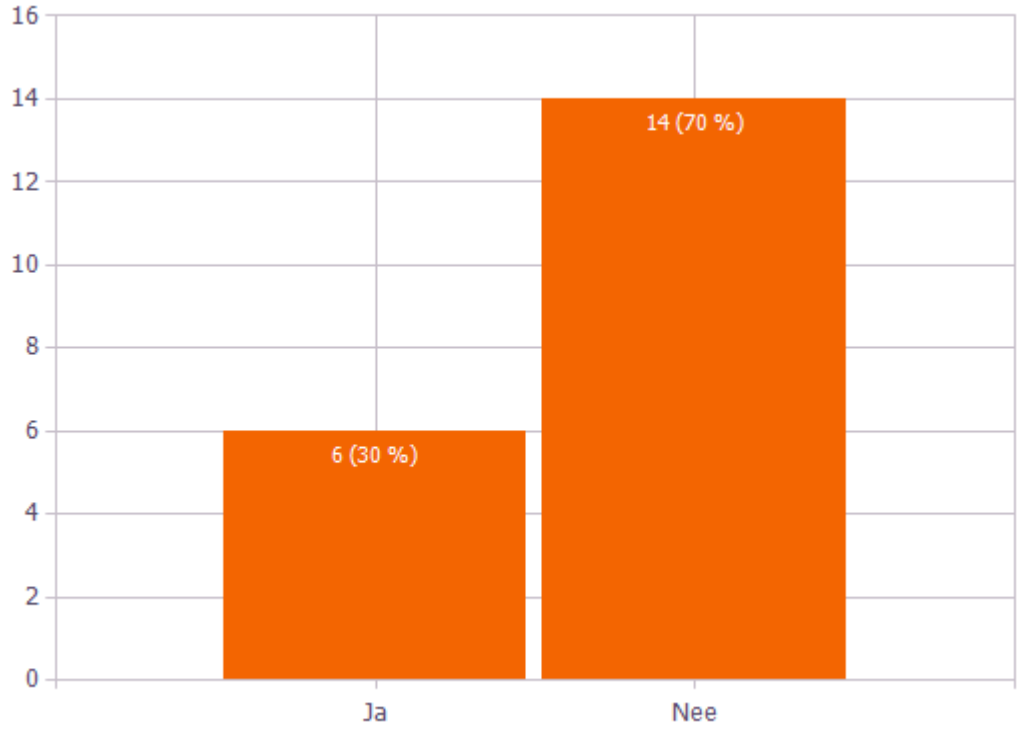
Antwoord
Inhuur van kennis en expertise.
De grootste kostencomponent zal gaan zitten in de organisatorisch transformatie.
Innovatie cycli.
Vereiste beschikbaarheid per keten.
Cultuurveranderingen.
Netwerkinvesteringen
Facilitiesinvesteringen.
Omvang Infra.
Hardware investeringen.
Innovatie.
Software investeringen.
Hoeveelheid applicaties.
Audits en penetratietesten.

IT Toepassingen

Inhoudsopgave

1 Feedback op DoIT

1.1 Vindt u dat DoIT 0.7 op het gebied van IT Toepassingen de definitieve versie mag worden? (dus geen aanpassingen meer)

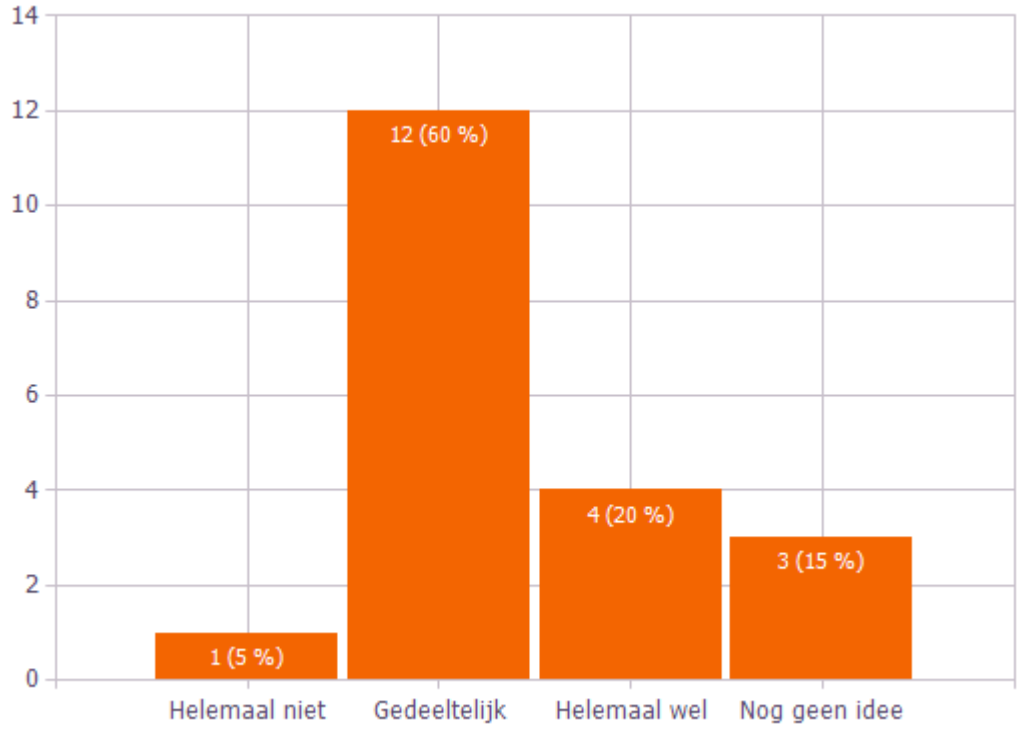


Aantal antwoorden 20

Antw.	Nummer	Percentage
Ja	6	30%
Nee	14	70%

1.2 In hoeverre acht u de ambitie van Defensie haalbaar voor de 1ste oplevering van de groeikern?

Denk hierbij onder andere aan de beschikbare tijd, de omvang van de werkzaamheden, één uniforme werkplek, Alles als een service aanbieden, de Defensie Appstore of de doelstelling dat binnen 5 jaar uit huidige realisatiedomein opgeheven kan worden.



Aantal antwoorden 20
Aantal antwoorden 1

Meerkeuze optie: Gedeeltelijk

Antwoord
Op deelgebieden prima hanteerbaar, bijvoorbeeld uniforme werkplek of de Appstore. Alles als een service is volstrekt onhaalbaar ,gezien het complexe applicatielandschap. Dit is echter niet belemmerend, er moet nu maar gewoon eens gestart worden met wat doen.
Het onderdeel van de uniforme werkplek op het gebied van de User applicaties is haalbaar voor wat betreft de office automation en de communicatiemiddel/collaboration onderdelen. Voor de coi applicaties is te weinig info. Appstore is te doen.
Op dit moment nog geen uitspraak mogelijk over de 5 jaar termijn voor het opheffen.
Het is zeker een haalbare ambitie van Defensie. Alleen of dit binnen 5 jaar te realiseren is, is mij de vraag. De app store is zeker wel haalbaar, indien de governance goed wordt ingericht en persoons-/functiegebonden en agendagestuurd apps aangeboden gaan worden. Maar de complexiteit van de infrastructuur met de rationalisatie is lastig binnen de gestelde 5 jaar.
Afhankelijk van budget en politieke wil/ondersteuning van Defensie top.
ik verwacht vertraging als gevolg van de cultuur van de MinDef organisatie. Verder verwacht ik dat op dit moment niet alles in beeld is, dus gaandeweg ontstaat ander beeld. Ook denk ik dat er eerder van een proces dan van een afgebakende time frame uitgegaan moet worden. IT/IV gaan komende tijd steeds sneller en sterker veranderen.
Inzichten zullen de komende 5 jaar veranderen. DoIT zal navenant moeten worden bijgesteld.
Dit is sterk afhankelijk van de wil om te veranderen binnen Defensie.
Complexe business.

Antwoord
Afhankelijkheid van reorganisatie. Nog geen zicht op kosten van o.a. transitie. Nieuwe governance.
Te hoge ambitie: half jaar doorlooptijd voor realiseren eerste oplevering. Belemmerende factoren: verandering van werkwijzes, cultuur, besturing en inzet van bleeding edge technologie met name voor security.
Nog wel wat detaillering en afstemming nodig.

Meerkeuze optie: Helemaal wel

Antwoord
Technisch zeker mogelijk; process is meer beperkend.
Andere organisaties hebben het gedaan, dus waarom niet hier? Maar alleen indien het Operating Model aangepast wordt om de snelheid en wendbaarheid mogelijk te maken. En als de financieringsaspecten geadresseerd worden.
Technisch haalbaar. Gefaseerde aanpak. Afhankelijk van beschikbare fondsen.
Als de juiste resources beschikbaar gesteld worden en leveranciers niet alleen voor hun 'eigen hachje' gaan, is dit volgens mij prima realiseerbaar. Wel zal er ruimte moeten blijven om tussentijds bij te sturen indien noodzakelijk.

Meerkeuze optie: Nog geen idee

Antwoord
Hangt af van commitment, regievoering, beschikbare middelen en vooral de snelheid/flexibiliteit, waarmee bedrijven (flexibel) gecontracteerd kunnen worden.
Gezien het feit dat er nog aspecten verder uitgewerkt moeten worden in 0.7.
Er zijn veel afhankelijkheden, zowel binnen IT (bv. gereedstelling infrastructuur) als daarnaast (veranderkundig, sturing, financiën).

1.3 Kunt u uw feedback geven op het gedeelte IT Toepassingen in het DoIT

Inleiding

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Ok.
Is voor de inleiding voldoende duidelijk. Op voorwaarde dat er meer detailinformatie beschikbaar komt in de vervolghoofdstukken.
Geen opmerkingen.
Goed uitgewerkt voor deze fase. Oppassen dat blokjes in schema ook voor iedereen helder zijn. Voor niet IT’ers extra uitleg nodig.
Is heel summier.
Ok.
Ok.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Communication services ontbreken in figuur 9
Kaderzetting is prima
Focus lijkt te liggen op het ontwikkelen van services (SGA). Een verduidelijking/nuancering is nodig om aan te geven dat er ook legacy is en blijft. Ook zullen standaard oplossingen (bijvoorbeeld wapensystemen) hun eigen architectuur kennen.
De scope van DOIT is onduidelijk. De nadruk lijkt vooral op de bedrijfsvoering te liggen. De toepassingen voor operaties zijn onderbelicht.
ok

User-Facing capabilities

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Ok.
Er zijn mijn inziens een paar standaardoplossingen, die hier prima aan voldoen. Ik mis hier wel het aspect beveiliging bij lokale opslag.
Ok.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Gericht wordt persoonlijke, taakgerichte werkomgevingen. In een flexibele, maar robuuste context. Ik wil meer verheldering over hoe autorisaties gegarandeerd gaan worden. Aangeboden services dienen 100% gekoppeld te zijn aan vastgestelde autorisatie en authenticatiemodellen. Hetzelfde geldt voor data access. dit is uit ervaring de grootste uitdaging bij geïntegreerde oplossingen.
Hier spreekt uit dat er een portal functionaliteit wordt geambieerd. Vanuit hier moet de gebruiker in staat zijn, afhankelijk van de rol, de relevante info beschikbaar te hebben. Wel te weinig diepgang om hier een verdere uitspraak over te kunnen doen.
Duidelijk verwoord. Alleen belangrijk dat de governance goed wordt ingericht bij de user-facing capabilities. Wie mag welke informatie zien en welke informatie heeft welke rol/functie binnen Defensie nodig om zijn of haar werkzaamheden uit te voeren. Met de gedachte, dat iedereen met "dezelfde business" bezig is --> Connected Management.
Een zeer belangrijk aandachtsgebied is gebruikersacceptatie. Zonder deze acceptatie zullen de mooiste technische toepassingen niet (voldoende) gebruikt worden met als risico dat ICT-projecten falen. De balans tussen security en gebruiksgemak moet in balans zijn per doelgroep. Er wordt in de documenten veel over security en over connectivity/beschikbaarheid gesproken, echter wordt er geen combinatie van deze twee onderdelen aangegeven. En juist daar kan de balans in gevonden worden.
Misschien iets meer aandacht voor begrippenmanagement en dataproblematiek.
Alles web-based is een mooi streven maar brengt ook risico's met zich mee. Wordt bedoeld alles, zonder uitzondering?
Ok.

Community of Interest (COI) en Core Services

Meerkeuze optie: Is voldoende duidelijk

Antwoord
In combinatie met uitleg bijlage is het helder.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Hoe denkt Defensie bronnen als (gekwalificeerde) middelen en personen te gaan ontsluiten? Zijn personen met ervaring en competenties niet juist de verrijkers van vooraf geanalyseerde, geïntegreerde, aangeboden informatie? Brains & tools!
Belangrijk dat de juiste innovatieve applicaties worden gevonden/ontwikkelt voor Defensie. Uitproberen, inzetten en eventueel laten falen, maar vooral leren van wat wel en niet werkt in een app. De apps zo inrichten dat deze agendagestuurd gaan worden voor elke specifieke werknemer/rol. Zorgen dat de benodigde informatiebronnen (apps) voor de agenda van de defensiemedewerker naar voren komen op het juiste moment voor snelheid.
Duidelijke en zeer (te) ambitieus. De wens om alles als een service aan te bieden is logisch. Het gevolg is echter dat alle, dus ook de standaard toepassingen, hierop moeten worden aangepast. kostbaar, en zorgt ervoor dat de ambitie om zo veel mogelijk gebruik te maken van standaard overboord kan. Advies is om alleen die domeinen waar meerdere applicaties/oplossingen gebruik maken van de services, daadwerkelijk als service aan te bieden.
De organisatie van de Col's en de governance van hun eigen ontwikkel- en innovatiebehoeften en roadmaps is niet geadresseerd. De kortcyclische aspecten van de visie - kritische succesfactoren - zijn sterk afhankelijk van een succesvolle organisatie en Operating Model op dit gebied. Ook is het verband met het gebruik van NATO capabilities aan de ene hand en verregaande verservicing van de eigen omgevingen nog niet zichtbaar: wat zijn de duurzame patterns van organisatie/consultatie en sturing/waardeketens in het run model? Kortom, hoe gaat men het 'doen' (niet technisch)?
Blokken zijn erg summier toegelicht en kunnen hier voor meerdere uitleg vatbaar zijn. Hoe is de indeling tot stand gekomen? Zijn landservices heel anders dan airservices? Hoe wordt integratie en afbakening gehanteerd?
Ok.
Met name de afhankelijkheid van het basis innovatieplatform zou uitgediept kunnen worden.
Is defensie voornemens om voor ISR de MAJIIC standaarden te omarmen, inclusief de volledige service stack van enterprise en COI specific services.
Ok.
Ok.

Meerkeuze optie: Is nog niet beschreven

Antwoord
Er staat nauwelijks in, behalve een ambitie. Of deze überhaupt haalbaar is vraag ik mij wel sterk af, want dit neigt wel heel sterk naar grote hoeveelheden maatwerk/customisation, en daar ben ik geen voorstander van. Er wordt hier feitelijk een oplossing beschreven en niet een doel!

Defensie eigen sensoren

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Ok.
Duidelijk.
Ok.
Ok.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Geen mening. Lijkt onvolledig.
Het is belangrijk dat er een overkoepelende laag komt over alle verschillende bronnen van Defensie, waarbij de patronen, algoritmes etc. herkent en zichtbaar maakt. De informatie die te meten is door bijv. sensoren: welke systemen vangen nu deze informatie op? Bij een punt als predictive maintenance is het belangrijk dat alle beschikbare informatie wordt verzameld en per assest wordt getoond aan de verantwoordelijke. Hoe gaat Defensie nu om met de informatie uit sensoren.
Zwalkt wat in zijn keuzes; er staat nu 'alles moet overal kunnen'. Ik heb liever een eenduidige keuze, dit klinkt mooi maar werkt in de praktijk niet.
Aanvullende uitleg op altijd beschikbaar: er dient altijd voldoende reken- en opslagcapaciteit beschikbaar te zijn, logisch. Met het uitvallen van netwerk dient dat ook het geval te zijn. Hoe wil Defensie hier mee omgaan?
(eisen aan) koppelvlakken/interfaces moeten in meer detail beschreven worden. Denk hierbij aan het noemen van toepasselijke standaarden (bijv. uit het NATO MAJIIC programma). Waar ligt de verantwoordelijkheid voor de interface, aan de infrastructuurzijde, sensorzijde, of beiden? Vallen aanpassingen aan de de sensor stations binnen de scope van dit programma? Om zinvol big data analytics te kunnen toepassen vormen veel standaarden voor data en services een rem op het uitnutten van het volledige potentieel aan informative.

Bestaande Defensie toepassingen

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Duidelijk omschreven, de keuze is wat mij betreft wel dubieus. Er wordt wat teveel openheid gegeven in oplossing; kies liever ('we faseren alles dat niet SGA is uit, TENZIJ' dan wel 'alles wordt tot SGA omgebouwd'). Dit maakt het te complex.
Procesmatig voldoende duidelijk. Zal de nodige aandacht vergen bij ontwerp en implementatie.
Ok.
Ok.
Ok.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Dit gaat veel geld kosten. Daarnaast wordt er wel erg makkelijk gedacht over het omzetten van de applicaties.
Evenals bij User Facing capabilities is hier de balans tussen security en gebruiksgemak van groot belang. Zowel bij centric- als bij cloud based toepassingen dient een dataverbinding beschikbaar te zijn als er nieuwe informatie geraadpleegd en/of gemuteerd moet worden. Deze verbinding moet uiteraard veilig zijn, maar in onze ogen moet de gebruiker geen extra handelingen uit dienen te voeren om de verbinding (weer) tot stand te brengen of telkens opnieuw in te loggen in de betreffende omgeving en/of applicatie.
Met name dataproblematiek verdient wat extra aandacht. Procesmatig is het wel helder.

Hybride Integration Platform en externe services

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Ok.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Ok.
Is erg technisch benaderd. Iets meer aandacht aan de functionele integratie en tijdelijk gebroken ketens om continuïteit te garanderen. Prima dat wordt aangesloten op open standaards!
Blijft nog erg algemeen.
Opnemen van voorbeeld helpt om te verduidelijken wat Defensie hiermee wil bereiken.
Ok.

De te bereiken eindsituatie

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Ok.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
"Het volledige IT-infrastructuurplatform" Wat wordt hier mee bedoeld? De volledige Defensie infrastructuur voor alle IT (groen+wit), waarbij de bestaande infrastructuur is gemigreerd/vervangen?
2020 voor het beschikbaar hebben van alle services is zeer ambitieus. Ambitie is goed, maar de verwachtingen kunnen door deze uitspraak ook onrealistisch worden. Een PoC of eerste project helpt om een betere inschatting te maken. Een dergelijke toelichting helpt mogelijk het verwachtingenmanagement.
Veel is op dit moment niet bekend. Mist een beschrijving van hoe men het gat/white space gaat dichten.
De te bereiken eindsituatie is duidelijk verwoord door Defensie. Het is een innovatieve visie, alleen zorgen voor een overzicht van al deze applicaties en al de toepassingen die bij Defensie worden ingebracht is dan belangrijk. Waar komt welke informatie vandaan en wat zegt het over de "Business". Er moet een duidelijke overkoepelende laag komen die dit zichtbaar maakt. SPOT, Single Point Of Truth. De visie hierop moet verduidelijkt worden voor de te bereiken eindsituatie. Als je van te voren zichtbaar maakt wat de essentiële te behalen managementdoelstellingen zijn, kan er op een efficiëntere wijze gekeken worden naar de inrichting van de toepassingen daaronder.
Tijdslijn, roles en responsabilities.

Meerkeuze optie: Is nog niet beschreven

Antwoord
Ik begrijp deze niet, de SOLL beperkt zich hier tot infra?

Algemeen geldende ontwerpprincipes voor IT-toepassingen

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Voldoende voor nu.
Prima en voldoende generiek.
Ziet er goed overdacht uit. Wel omvangrijk.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Ook hier dient aandacht te zijn voor de security/gebruiksgemak balans. Mensen 'in het veld' verliezen enorm veel tijd door opnieuw inloggen, verbindingen proberen te maken, etc. Dit levert ook onnodig veel frustratie op. Security en data connectivity kunnen met de juiste oplossing prima gecombineerd worden, zodat de gebruiker door kan werken.

De roadmap

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Voldoende en generiek omschreven, prima.
Het Innovatie Domein en de geschetste ontwikkelrichtingen zijn voor ons een uiterst logische, goede en begrijpelijke aanvliegroute. De bijbehorende roadmap in tijd is zeker haalbaar, mits er aan bepaalde randvoorwaarden ten aanzien van governance en regievoering wordt voldaan. Hier komen wij later op terug. Bovendien zijn alle beschreven sets aan management services een vereiste om verandering en vernieuwing binnen Defensie te kunnen realiseren. Dit vereist aan Defensiekant het versnelt uitbouwen en/of opbouwen van kennis op deze kennisgebieden, al dan niet met behulp van de nog te benoemen regiepartner. De marktpartijen moeten reeds deze kennis paraat hebben om als volwaardig partner van Defensie te kunnen optreden en lessons learned en best practices te kunnen delen. Een meer fundamenteel en inhoudelijk oordeel beschrijven wij in het RFI document.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Goed dat roadmap wordt gehanteerd. Misschien afstemmen met algemene roadmap Defensie.
De 4 projecten lijken ambitieus. Mogelijk is een relatief klein project met weinig complexiteit handiger om inzicht te krijgen in de haalbaarheid van de gewenste eindsituatie.
Toepassingen van (recente) standaarden is een manier om op korte termijn te komen tot eerste resultaten m.b.t. geintegreerde IT-toepassingen, tevens interoperabel met coalitie partners. op middellange termijn is dit niet (volledig) te handhaven. In hoeverre kan/mag in deelsystemen afgeweken worden van (open) standaarden als dit leidt tot waardevolle/zinvolle verbetering van performance en/of capability?

Gehele hoofdstuk (irt) document

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Vraag onduidelijk.
Door de gehele documentatie blijkt dat Defensie twee, schijnbaar tegenstrijdige, zaken wil bereiken, t.w. continuïteit en innovatie. Om dit te bereiken is er ons inziens een mix nodig van grote en van kleinere ICT spelers. Momenteel is niet duidelijk hoe Defensie wil bereiken dat deze mix gaat ontstaan. Het huidige proces lijkt wat meer geënt en toepasbaar op juist grotere, strategische, partners. Ons beeld is dat er explicieter richting de mix van groot en klein moet worden gestuurd en dat dit bereikt kan worden door dit te verankeren. Allereerst in de Sourcing strategie en daarna in het Control Framework richting de leveranciers.

Meerkeuze optie: Is nog niet beschreven

Antwoord
Wat wij missen is hoe Defensie het control framework wil gaan inrichten irt applicaties in het bijzonder en DoIT in het algemeen. Het beeld hoe je de control wilt gaan uitoefenen is van wezenlijk belang voor de keuzes die je nu maakt in de voortgang van DoIT. Hierbij denken wij aan de volgende stappen m.b.t. het Control Framework: (0) Visie, en vertaling in "harde" doelstellingen. (1) Inrichting control mbt het totale programma, obv (bijvoorbeeld) benefit management. (2) Opstellen sourcing strategie. (3) Definieren ICT control (regie) voor het uiteindelijke opgeleverde resultaat. Belangrijk aspect hierbij is, waar de huidige organisatie staat m.b.t. haar control framework (startniveau) en wat er met name bij de medewerkers mogelijk is cq. moet veranderen om het uiteindelijke gewenste niveau van ICT control te bereiken.

Bijlage: Eindrapport DoIT Deel B

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Wel heel breed, volwassenheid van delen wisselt sterk
Top down approach met het juiste mandaat, governance en regie is in onze beleving de juiste marsroute.
De mens centraal, IT volgt. Volledig mee eens en zo moet het zijn. De IT moet in alle 5 omstandigheden naadloos kunnen volgen.
Ok.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Nadruk op de bedrijfsvoering. De toepassingen voor operatie lijken te ontbreken.
Het document is redelijk ver. Het mist een aantal aspecten over 'hoe het gaat runnen' (niet technisch), hoe het anders is dan tot vandaag. Hoe gaan Defensie en het ecosysteem zich beter organiseren voor succes?
Vooral ten behoeve van Analytics Service is het belangrijk de mogelijkheid te hebben tot het ontsluiten van alle databronnen, zowel gestructureerd als ongestructureerd (traditioneel en nieuw/big data). Door het blenden van al deze databronnen kunnen diepgaande inzichten worden verkregen.
Nog veel onduidelijk over hoeveel data/systemen nu precies gemigreerd moeten worden. Hoeveel verschillende datasoorten zijn er, bijv. ook paspoorten/biografisch/biometrisch?
Op sommige punten is nog wel een verdiepingsslag nodig, hier komen wij in de schriftelijke RFI-beantwoording op terug.
Om zoveel mogelijk tegemoet te kunnen komen aan de eisen die worden gesteld aan, en ambities rondom zowel het LGI als HGI domein (en een steeds verdergaande vorm van convergentie van deze twee rubriceringsniveau's door bijvoorbeeld voortschrijdende technologische security oplossingen, concepten en

Antwoord

processen) en het feit dat 3 van de 4 use cases van de Defensie onderdelen, en het NOIS domein in het bijzonder, in onze beleving een aanbestedingsvorm vergt die de marktpartijen in staat stellen zo open en transparant mogelijk tot beantwoording in een RFP fase over te kunnen gaan. Kortom, een vorm waarbij ABDO geaccrediteerde marktpartijen Defensie kunnen adviseren en met Defensie kunnen 'sparren' tot en met het niveau Staatsgeheim Geheim en Staatsgeheim Zeer Geheim.

De “Think big, act small” aanpak spreekt ons zeer aan, daarbij komen de aanpak en doelstellingen ons haalbaar over binnen de gestelde termijnen, met kanttekeningen.

Meerkeuze optie: Is nog niet beschreven

Antwoord

Self-service data-preparatie voor analytics is een belangrijk onderdeel, waaraan Analytics zou moeten voldoen. Dit is vooral belangrijk bij het efficient analyseren van Big Data.

2 Logische stappen

2.1 Is het op het gebied van IT Toepassingen mogelijk om "act small" te doen, irt "Think Big"?

Motiveer uw antwoord alstublieft op de volgende wijze;
Ja: Kunt u voorbeelden geven van (kleine) stappen die we kunnen doen.
Nee: Wat zijn belemmeringen en hoe kunnen deze weggehaald worden?

Meerkeuze optie: Ja

Antwoord
Opdelen in veel kleine projecten/domeinen.
Aanvulling op vorige. De users en rollen is de allereerste stap.
Focus.
Geef z.s.m. aan wat de definitieve pilaren zijn waarop gebouwd zal worden, dat bepaald de scope en voorkomt onnodig veel aannames.
Let op randvoorwaarden: tijd, geld, capaciteit en commitment vanuit leiding en bedrijfsvoering niet-IT.
Wat voor een andere partij goed genoeg is, is ook goed genoeg voor Defensie. Vermijd customisation! Het kost altijd 2 x meer dan je wilt uitgeven, het duurt 2 x langer dan geschat, en je krijg de helft van wat je nodig hebt.
Voldoende aandacht voor changemanagement, ook bij leveranciers.
Combinatie tussen faseaanpak en agile. Voor wat betreft agile: werken middels POCs. Zorg ervoor dat de organisatie getraind is om echt agile te werken, niet alleen in intentie.
Testen per onderdeel: Definieer de oplossingen en ga deze testen binnen een duidelijke en niet aanpasbare scope. Ervaar dat de oplossing werkt en verzand niet in roadmap verhalen. Beperkte set onderdelen samen testen: zoek de koppelvlakken op en test deze binnen een niet aan te passen scope. Maak het geen 'ICT feestje': ga samen met de gebruikers(groepen) op pad en ervaar waar deze mensen in de praktijk tegenaan lopen rondom ICT. Lijst gecertificeerde oplossingen: als er oplossingen commercieel beschikbaar zijn die voldoen aan de eisen/wensen van DoIT, maak dan het certificeringstraject stukken eenvoudiger.
1. Begin met alle verwachtingen hetzelfde te krijgen bij iedereen (cultuur & adoptie). 2. Start met de generieke office automation/.collaboration applicaties. 3. Creëer een portal Bepaal wat je wilt ontsluiten via de portal 4. Faciliteer het samenwerkingsplatform. 5. Creëer daar de services voor, indien nodig. Een en ander hangt nauw samen met het infrastructuur project. Met name als we het hebben over de public cloud.
Federatief zoeken is een duidelijk voorbeeld van iets dat stapsgewijs kan worden gedaan.
Regel een duidelijk intake, design, testproces in. Maar doe dat wel snel.
1 Breng infrastructuur en werkplek op orde. 2 Start met nieuwe toepassingen met kleine impact en niet gekoppeld aan reorganisatie of grote cultuur verandering. 3 Pak de iets complexere problemen met toepassingen met meer impact. 4 Werk aan opschaling vanuit pilots.
Hou vast aan fundamentele keuzes in HLO, bijv.beveiliging, beschikbaarheid etc.
Kortcyclisch => gemandateerde user in het team.
Durf in deze aanpak ook te stoppen op het moment dat resultaat niet gaat leveren wat verwacht is.
Bepalen wat de projecten aan informatie hebben opgeleverd, en wat zegt deze informatie over onze "Business"? Wat gaan wij doen met deze informatie: zorgen voor continue stroom van resultaten vanuit de afgeronde sprints.
Definieer de grenzen van de extreme use cases vroeg, zodat voor leveranciers duidelijk is wat het speelveld is

Antwoord
en waarvoor de standard moet gelden. Dit voorkomt te veel maatwerk oplossingen achteraf.
9. Accepteer dat je in een permanente staat van vernieuwing zit.
Architectuur is hierbij belangrijk, maar dan als referentiekader, niet als wet!
Indien procurement/contractmanagement ook kortcyclisch en agile zijn (voorwaarde voor succes van benadering).
Zorg voor een closed feedback loop waarbij de evaluatie van ieder stapje tot een herijking van de doelen kan en mag leiden
Kleine stapjes, maar koersvastheid op doelen die je wilt bereiken.
Maak een overzicht van het bestaande landschap. Leg fitheid, businesswaarde en overlappen tussen applicaties daarin vast.
Indien bevoegde integrated teams (agile) ontwikkeling oppakken (end2end).
Assess de 'gaps' en review het HLO op inefficiencies, zoals beschreven in het DoIT plan.
8. Gooi waar mogelijk weg. Weggooien is geen desinvestering maar een besparing.
Laaghangend fruit: eerste onderdelen oppakken, die makkelijk te realiseren zijn.
Via POC's bepalen of er mogelijkheden zijn, dus denk in mogelijkheden.
The 'big picture' dient z.s.m. te worden vastgesteld m.b.t. het nemen van de kleine stappen.
7. Accepteer tijdelijke onvolkomenheden (afwijkingen van architectuur bijv.).
Indien een snelle lifecycle model voor services (met meerdere versies coexisterend) als basis wordt gekozen, is loskoppeling van ontwikkelgebieden (suppliers/consumers) gaat flexibilitieit omhoog (Patterns voor SOA succes).
Na het afronden van verschillende sprints, steeds meer het grote behaalde plaatje samenvatten, verantwoordelijke aanstellen, en doorgaan met volgende kleine stap.
Lange termijn doelstellingen zijn aan verandering onderhevig. Durf regelmatig te herijken om in sinc te blijven met de behoefte van de organisatie.
Ja, is zeker mogelijk. N.B. Houd er rekening mee dat echter de context, waarbinnen Defensie acteert (stakeholdrveld), niet ingericht is om 'Act small' (met meer agility) te kunnen werken. Het is dus zeker niet alleen een kwestie van logische kleine stappen of een meer agile aanpak voor Defensie zelf, maar er zal tevens stuur op de omgeving noodzakelijk zijn!
6. Focus op echte issues, op basis van de BC.
5. Wijs duidelijke probleemeigenaren aan. Geen traject zonder owner.
Begin met het organisatieonderdeel dat graag wil, zodat er meer 'tijd' is voor technische issues.
Bepaal heel duidelijk de verschillende rollen en verantwoordleijkheden.
Overstappen ov web applicaties of web enabled applicaties, zodra dat kan - actief beleid voeren, inmengen in nieuwe aanschaf.
Fouten maken mag, leer van deze fouten en neem dit mee naar volgende Sprints.
Ga voor de 80% oplossing (tegen 20% van de moeite).
Blijf bij je korte termijn doelstelling. Ga niet afwijken tijdens uitvoering.
Patronen voor herbruikbare services eerst bepalen (leest voor alle services).
Vooraf goede afspraken maken over verantwoordelijkheden en verwachtigingen (governance), zowel binnen Defensie als met de leveranciers.
Pilots voor afzonderlijke bedrijfsonderdelen. Let op afhankelijkheden. Niet koppelen aan enorme cultuurveranderingen en reorganisaties.
Zorg er voor dat IT is aangehaakt als enabler, niet als bepaler van de functionele doelen.
4. Deel deze op in kort-cyclische trajecten met maximale doorlooptijd.
Uitvoeren, tevreden met het behaalde resultaat? Nee -> nieuwe doelstellingen definiëren en mee nemen in de volgende sprint.
Kleine stappen met Agile/Scrum methodiek. Politieke wil!
Bestaande "legacy" systemen kunnen één voor één worden ontsloten met een en dezelfde user interface. Dit hoeft niet in 1 grote migratieslag.

Antwoord
3. Focus op nu haalbare doelen.
App batches definieren, die gevirtualiseerd gaan worden, en daarmee beginnen.
Zorg er voor dat zowel lange termijn scope als logische korte termijn stappen/doelen 100% functioneel zijn, afgestemd met eindgebruiker.
2. Instellen van actieve en dedicated leiding, die bestaande patronen doorbreekt.
Per use case een stappenplan voor implementatie maken, kort cyclisch itereren, beoordelen, bijsturen, herprioriteren.
Uitvoeren, resultaat bespreken, tevreden, Ja? -> volgende sprint.
Portfolio management inrichten (services, toepassingen).
Applicatie rationalisatie onmiddellijk starten, teneinde complexiteit en hoeveelheid te migreren apps te verlagen.
Sprints definieren met de te behalen doelstellingen.
Begin met klein project waar het aantal services minimaal is om aan te tonen. Dat het platform haalbaar is.
Zoek laaghangend fruit.
1. Inrichten en activeren van een nieuwe besturingsmethodiek.
Knip lange termijn scope op in logische blokken, die concrete resultaten gaan opleveren.
1. Korte projecten definiëren voor alle grotere projecten.
Maak een lijst van uitgewerkte use cases, stel prioriteiten.
Definieer je lange termijn scope per domein.
Toepassen van agile/scrum method.
Kleine stappen maken gewenning aan iT-verandering mogelijk.

Meerkeuze optie: Nee

Antwoord
Precondition: Kanteling naar services => business information services, niet alleen technisch. DIe hebben een Service Owner nodig (en governance org), niet alleen een Service Delivery org.
Architectuur kan initiatief dood knuffelen. Ook architectuurvisie moet mee kunnen bewegen zonder out of control te raken.
Niet voor alles. Toepassingen die meekomen met bijvoorbeeld J35 kunnen niet als act small opgepakt worden. Bepaal op basis van een enterprise architectuur wat wel/niet als small aangepakt kan worden.
Think big kan vertragend werken. Je weet nu nog niet wat straks nodig is. Duidt vooraf waar je vooraf wel iets over moet zeggen. Denk aan services die een cruciale rol gaan spleen, waarbij quick & dirty voor desinvestering gaat zorgen.
(2) Goed ingericht control framework voor de uiteindelijk te leveren dienstverlening door leveranciers: kern hierin is een juist ingerichte informatievoorziening op de dienstverlening. Vanuit onderaf moet de juiste operationele informatie beschikbaar zijn, om te kunnen sturen op de uiteindelijke doelen die Defensie hiermee wil realiseren. Het control framework en de bijbehorende informatievoorziening moet op alle lagen van de betrokken organisatie worden ingericht.
IT/IV betrekt eindgebruiker niet of te laat bij de lange termijn planning, korte termijn aanpak. Verwachting en resultaat dreigen dan uiteen te lopen.
De organisatie cultuur is hiervoor een realistische bedreiging, Vooringenomen standpunten.
Ontbreken van overall kaders (architectuur - IDA, startarchitecturen) leidt tot suboptimale oplossingen. Eén werkplek voor HGI/LGI plus SOMUT kan niet op agile wijze tot stand komen.
Cultuur binnen defensie! Een agenda.
Tenzij er een groot aantal commodity zaken worden uitbesteed.
Service fabric/security platform(s) moeten eerst komen, voordat bijvoorbeeld IGO kan.
Kleine stappen leiden tot groter belang van een goed ingericht control framework. Stap (1): inrichten van control op het totale programma, op basis van (bijvoorbeeld) benefit management.
Enkele onderdelen van het programma dienen als enabler voor kortcyclisch kunnen werken. Die moeten stevig (en snel) als een platform neergezet worden.

2.2 Feedback op de genoemde belemmeringen

Meerkeuze optie: Feedback

Enkele onderdelen van het programma dienen als enabler voor kortcyclisch kunnen werken. Die moeten stevig (en snel) als een platform neergezet worden.

Antwoord
Is geen belemmering.

Door hele programma in samenhang uit te voeren in plaats van vernieuwing en organisatie gescheiden door te voeren

Antwoord
Besteed voldoende aandacht aan de ontwikkeling van de competenties van de business en IT.
Eén geïntegreerde planning en afstemming werkpakketten.
De stromen ontwikkelen en personeel/organisatie onder een besturing brengen.
Door de business de lead te geven. Benoem business owners voor de toepassingen.

kleine stappen leidt tot grotere belang van een goed ingericht control framework.
Stap (1): inrichten van control op het totale programma, obv (bijvoorbeeld) benefit management

Antwoord
Oplossing staat verwerkt in de belemmering.

Service fabric / security platform(s) moeten eerst komen voordat bijvoorbeeld IGO kan.

Antwoord
Ook hier klein beginnen en zorgen dat voorzieningen voldoende zijn voor IGO en passen binnen architectuur. Pragmatisch benaderen en oppassen voor alles hangt met alles samen. Eventueel op zoek gaan naar tijdelijke workarounds. Oplossen binnen 'het werk'. Proof of concepts gebruiken om toepasbaarheid en werking aan te tonen.

Tenzij er een groot aantal commodity dingen worden uitbesteed

Antwoord
Al ingevuld.
Strikte naleving van buy i.p.v. make. En consumeren i.p.v. buy (abonnementen op capabilities) (eigendom brengt vele verantwoordelijkheden en investeringen met zich mee).

cultuur binnen defensie!
een agenda

Antwoord
Wij zien problemen in de nieuwe werkwijze; men is gewend aan grote, logge projecten die jarenlang duren. De werkwijze moet nu kostencyclisch en iteratief worden. Dit vraagt om: - Formuleren van korte termijn doelstellingen. - Bijstellen in denken; een sprint die niet oplevert wat verwacht is, is niet 'mislukt' maar is de basis voor de

Antwoord

volgende spring.

- men moet leren denken als een incubator. Binnen een innovatiegerichte cultuur is falen goed; daar leer je van. Dit denken moet gestimuleerd worden.
- Grote doelen bewegen continu, die bereik je dus ook nooit. Deel een groot doel op in haalbare elementen en ga daar voor aan de slag.
- Inzien, accepteren en doorvoeren van veranderingen; bij Defensie zit het probleem met name op het gebied van acceptatie. Hier moet aan gewerkt worden. Dit vraagt andere keuzes (personeelsbeleid, opleidingen) en sfeer (bedrijfscultuur, goede voorbeelden vanuit de top).
- Wijs ECHTE probleemeigenaren aan. Geen project zonder probleemeigenaar. Geen owner = stoppen.

Ontbreken van overall kaders (architectuur - IDA, startarchitecturen) leidt tot suboptimale oplossingen. Eén werkplek voor HGI/LGI plus SOMUT kan niet op agile wijze tot stand komen.

Antwoord

Einddoel in zicht houden.

Richt een permanente proeftuin (CDTE) in.

Tijdens iteratieve ontwikkeling doorlopend testen en verifieren of een oplossing doet wat hij moet doen binnen de gestelde scope, en potentie heeft om op termijn volledig compliant te worden.

Koppeling tussen verschillende systemen testen en verifiëren.

IT/IV betrekt eindgebruiker niet of te laat bij de lange termijn planning, korte termijn aanpak. Verwachting en resultaat dreigen dan uiteen te lopen

Antwoord

Gebruiker te laat betrokken bij lange termijn planning: verandermanagement integraal opnemen binnen het programma. Bijvoorbeeld d.m.v. business champions/ambassadeurs. Deze vroegtijdig betrekken.

Klankbordgroepen.

User ambassadeurs.

Gefaseerde uitrol met tussentijdse evaluaties.

(2) Goed ingericht control framework voor de uiteindelijk te leveren dienstverlening door leveranciers: kern hierin is een juist ingerichte informatie voorziening op de dienstverlening. Vanuit onderaf moet de juiste operationele informatie beschikbaar zijn, om te kunnen sturen op de uiteindelijke doelen die Defensie hiermee wil realiseren. Het control framework en de bijbehorende informatievoorziening moet op alle lagen van de betrokken organisatie worden ingericht.

Antwoord

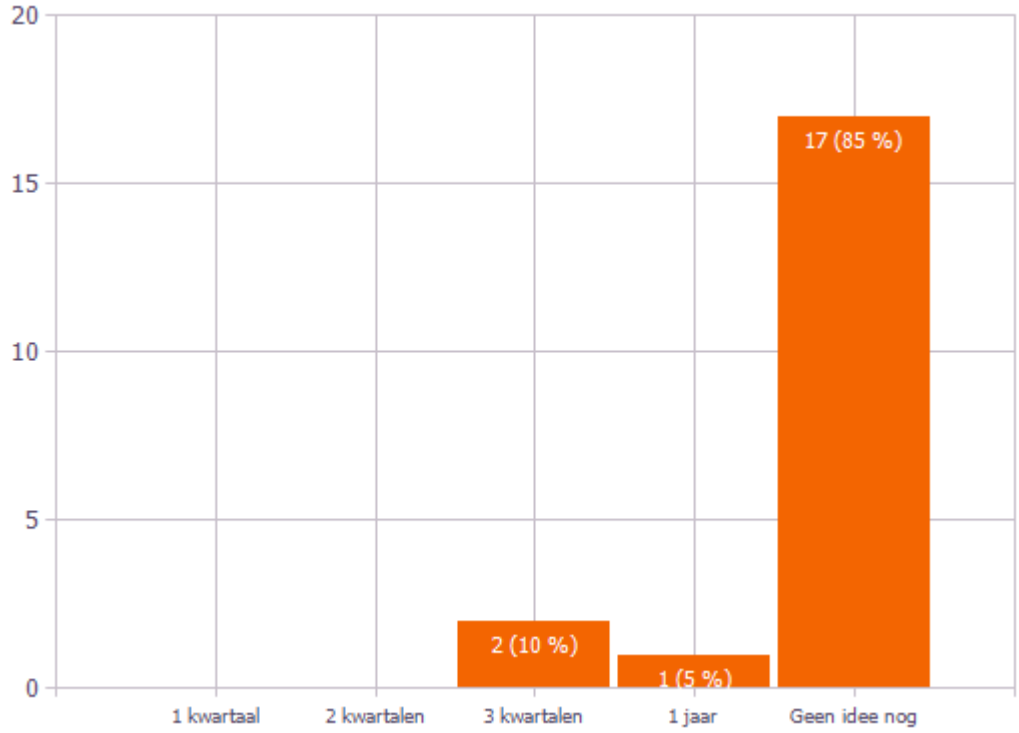
Niet helemaal duidelijk welk probleem hier wordt geduid.

- Goed ingericht opdrachtgeverschap.
- Middelen beschikbaar stellen voor leveranciers.
- Duidelijkheid hoe onderscheid te maken in leveranciersmanagement voor exploratie en voor realisatie.

3 Plan van Aanpak

3.1 Hoeveel tijd schat u in om de IT Toepassingen van de gewenste groeikern te realiseren?

Kunt u uw antwoord toelichten?



Meerkeuze optie: 3 kwartalen

Antwoord
Met testen, falen, leren en uiteindelijke keuzes maken en doorvoeren.
M.b.t. Plateau 2: met het juiste model van samenwerking, goede en door alle partijen gedragen scoping en goede inrichting van het governance en regie model is 01-07-2016 haalbaar, mits gunning aan de markt begin januari 2016 plaatsvindt. In de schriftelijke beantwoording van de RFI geven wij een nadere uitwerking m.b.t. de 7 functionaliteiten genoemd in hoofdstuk 4.8. De echte complexiteit zit in Plateau 3. Ook hier gaan wij in een latere fase dieper op in.

Meerkeuze optie: 1 jaar

Antwoord
Mits goed begeleid (governance goed ingericht en gebruik makend van een projectteam) en met de juiste prioriteit.

Meerkeuze optie: Geen idee nog

Antwoord
IT-Toepassingen is nooit "klaar". Ook in het kader van "act small" is het niet persé duidelijk wanneer de realisatie een feit is.
Maar meer dan een jaar. Ik stel een proof of concept voor. Dat geeft een gevoel bij wat er aan tijd nodig is voor de rest.
De volledige inhoud van de nu gedefinieerde groeikern (voor LGI/HGI plus SOMUT) is niet binnen een jaar gereed. Onderdelen zijn wel mogelijk. Onduidelijk is of er nog EU aanbestedingen voor technologie noodzakelijk zijn, of er al (op onderdelen) bruikbare resultaten zijn voor de toepassingen in de groeikern en of

Antwoord
de business en IT-medewerkers op tijd klaar zijn voor de verandering.
Veel langer dan 1 jaar. De randvoorwaarden voor succes moeten eerst ingevuld worden.
Het zal zeker meer dan een jaar zijn, maar zonder keuzes en specificaties valt hier niets zinnigs over te zeggen.
Business innovatie moet, uitgaande van big think, act small, relatief snel haalbaar zijn. Vraag die bij mij leeft is hoe snel de standaard IT om dit mogelijk te maken beschikbaar komt. Tweede vraag is of Defensie in staat is om de business daadwerkelijk ruimte te geven om te komen tot innovatieve oplossingen. En hoe snel kan IT (OPS) e.e.a. in beheer nemen (flexibiliteit infra, autorisaties, schaalbaarheid, etc.). En de derde vraag is hoe dit contractueel/juridisch naar de markt gebracht gaat worden. Een complexe aanbesteding duurt al snel een ¾ jaar. Tot slot, hoe gaat Defensie alle specifiek benodigde kennis om te komen tot innovatieve oplossingen bij elkaar krijgen, ontwikkelen, inhuren?
Veel is afhankelijk van wat buiten mijn kennis-domein ligt.
Invullen van de randvoorwaarden voor succes zijn essentieel.
Hangt af van wat het percentage 'defensiespecifiek' zal worden.
Hoeveel tegenwerking verwachten jullie van de gebruikers en hoeveel aanpassingen kunnen we verwachten?
Hangt deels af van de manier van organiseren van het traject.
Er zijn nog vele afhankelijkheden.
Langer dan 1 jaar!
Veel afhankelijkheden van geld en beschikbaarheid van de mensen uit de bedrijfsvoering.
Nois, Icommand en IGO zijn erg groot en gekoppeld aan grote organisatieveranderingen.
Snelheid wordt niet bepaald door techniek maar door governance en besluitvorming.

3.2 Waar liggen volgens u, op het gebied van de realisatie van de IT Toepassingen, de drie grootste uitdagingen?

Antwoord
Omgang met “ can do” mentaliteit en onbeperkte ambities.
Aanpassen van procedures en policies aan technologie.
Hoeveelheid datastromen.
De winkel moet open blijven; dus ontsluiten van legacy systemen vereist veel aandacht.
Beschikbaar budget, benodigde capaciteit en verandering werkwijze IT-personeel en transitie van oud naar nieuw.
De wijze van invulling geven aan partnerships met externe partijen.
Probleemeigenaren aanwijzen /verantwoordelijken.
Financiereingsvormen (cashflow/uitgave vs. investering).
De eerder besproken security eisen die gestalte moeten krijgen op de werkplek (in brede zin des woords).
Verandermanagement, ten behoeve van de medewerkers van Defensie.
Koppelingen/interfaces
De interne Defensie organisatie, politiek, cultuur, versnippering.
Cultuur - doelgericht, acceptatie van een aanpak met inherent (bewuste) imperfecties en incompleetheid in opgeleverde systemen - omdat het resultaat iteratief/incrementeel/convergerend is in zijn aard.
Te veel tegelijk. Onderlinge afhankelijlkheden.
Cultuur omslag goed vooraf kenbaar maken.
Testen en bewijzen toepassingen binnen een vaststaande scope. Roadmap ontwikkelingen moeten binnen een bepaalde tijd klaar zijn en werken.
Afhankelijkheden die buiten perspectief 'IT-Toepassingen' vallen, zoals infrastructuur, datacenter voorzieningen, cloud koppelingen, etc.
De inrichting van een control framework op het traject, in het bijzonder benefit management.
Combineren oude en nieuwe techniek.

Antwoord
Vrijmaken van voldoende kundige Defensiegebruikers voor begeleiding/toetsing in iteratief ontwikkelproces.
Cultuurverschillen, onderling vertrouwen, ambitie niveau.
Budget.
Totale doorlooptijd.
Goede regie op gehele traject.
Cultuur, agility,creativiteit, prioritizering, budget.
De Defensieorganisatie.
Te veel met grote organisaties in zee gaan i.p.v. innovatief en flexibel MKB.
Procurement/inkoop.
Verandervermogen van de organisatie en de omgeving.
Rules engine aanpassen op de applicaties (advies: niet doen).
Aanbestedingen voor het verwerven van technologie, met name infrastructuur en security.
Innovatie mechanisme a la broedkamers Belastingdienst ontbreekt.
Culture.
Beschikbaar budget.
Juiste organisatie van het traject, in het bijzonder de verwerving.
Onderlinge afhankelijkheid (infra-netwerk-toepassingen) van de deelprojecten zorgt al heel snel voor vertragingen.
Gebruikersacceptatie van toepassingen.
Governance.
Organiseren voor succes. Het gehele traject inclusief aanbesteding, contract management, besluitvorming moet ook kortcyclisch en wendwaar zijn.
Resources.
(inzicht in) Connectivity eisen en beschikbaarheid.
Cultuur/gemeenschappelijke verwachting.
Tijdig inrichten van een proeftuin (CDTE.)
Afstappen van bestaande oplossingen op de gecertificeerde productlijst.
Splits innovatie van het moderniseren en standaardiseren van de basis infra. Dit leidt op korte termijn tot resultaat zonder lange termijn te frustreren.
Budget.
Onduidelijkheid over contractuele vorm voor (flexibel) inschakelen industrie.
De verandering op het gebied van cultuur, besturing en competenties, zowel bij business als IT-medewerkers.
Tijdige beschikbaarheid infrastructuur.
Te complexe eisen, architectuur, besturing maakt slagvaardig opereren onmogelijk.
Nieuwe infrastructuur.
Infrastructuur.

3.3 Hoe groot schat u de genoemde uitdaging in?

Geef uw mening op een schaal van 1 - 10, waarbij
1 = helemaal geen uitdaging
10 = zeer grote uitdaging

Onderdeel	-	Gemiddelde van de score	St.dev.
Governance		8,4	1,8
Totale doorlooptijd		8,3	1,7
Vrijmaken van voldoende kundige Defensie gebruikers voor begeleiding/toetsing in iteratief ontwikkel proces		7,6	1,9
Resources		7,4	1,9
procurement / inkoop		7,4	2,3
Onderlinge afhankelijkheid (infra-netwerk-toepassingen) van de deelprojecten zorgt al heel snel voor vertragingen		7,2	1,6
Budget		7,1	2,0
De eerder besproken security eisen die gestalte moeten krijgen op de werkplek (in brede zin des woords)		6,9	1,7
Infrastructuur		6,8	2,6
Onduidelijkheid over contractuele vorm voor (flexibel) inschakelen industrie		6,8	2,2
De winkel moet open blijven; dus ontsluiten van legacy systemen vereist veel aandacht		6,6	1,9
De inrichting van een control framework op het traject, in het bijzonder benefit management		6,5	2,7
Testen en bewijzen toepassingen binnen een vaststaande scope. Roadmap ontwikkelingen moeten binnen een bepaalde tijd klaar zijn en werken		6,1	2,3
Innovatie mechanisme a la broedkamers Belastingdienst ontbreekt		5,8	2,7
Afstappen van bestaande oplossingen op de gecertificeerde productlijst		5,8	2,0
Rules engine aanpassen op de applicaties (advies: niet doen)		3,6	2,6
	1 2 3 4 5 6 7 8 9	6,8	2,4

3.4 Uitdagingen uitwerken

3.4.1 Uiitdaging: Onderlinge afhankelijkheid (infra-netwerk-toepassingen) van de deelprojecten zorgt al heel snel voor vertragingen

Meerkeuze optie: Gekozen oplossing

Antwoord

Defensie focussed op de unieke Nederlandse behoeften, de infra- netwerk toepassing zouden uitbesteed moeten worden onder een services bases contract.

3.4.2 Uitdaging: de eerder besproken security eisen die gestalte moeten krijgen op de werkplek (in brede zin des woords)

Meerkeuze optie: Gekozen oplossing

Antwoord

Zoek naar pragmatische oplossingen. Probeer niet 1 alomvattende IT-oplossing; los ook niet alles in IT op; zoek naar differentiatie en andere maatregelen, zoals afschermen/beveiligen van data (dus niet alleen leunen op infrastructuur). Accepteer bijv. ook verschillende werkplekken om aan de eisen tegemoet te komen als dat echt noodzakelijk is. Meer risico's managen i.p.v. 100% mijden.

Meerkeuze optie: Voordelen

Antwoord

Haalbaar in termen van tijd en geld; en werkbaar!

3.4.3 Uitdaging: onduidelijkheid over contractuele vorm voor (flexibel) inschakelen industrie

Meerkeuze optie: Gekozen oplossing

Antwoord

Je moet Agile Contract management in gaan richten. Dit houdt onder andere in:

- Werk op basis van MoSCoW.
- Werk op basis van Time/Moneybox.
- Hou rekening met/stel je in op continue bijstelling en herprioriteren.
- Stel Must-haves alleen globaal en high-level vast en laat leverancier zich daar op commiteren.

Je contracteert een major increment, daarbinnen heb je releases die in meerdere sprints opgeleverd worden. MoSCoW moet je door dit hele framework heen inrichten en hanteren. Alleen detaillering wordt steeds fijner; je werkt op elk entry/exit point met wederzijds commitment.

De bijbehorende skillset/professie moet opgebouwd worden. Het denken in opdrachtgever/nemer schap moet losgelaten worden, er moet gedacht worden in een partnermodel.

Meerkeuze optie: Voordelen

Antwoord

1. Je bent samen verantwoordelijk voor de oplossing.
2. Je kan tijdig en tussentijds bijsturen. Ruimte voor voortschrijdend inzicht en invloed van buitenaf.
3. Commitment is kleinschalig, haalbaar en beheersbaar.
4. Budget is beheerst. Binnen het budget krijg je altijd de echt belangrijke zaken, die prioriteer je zelf.

3.4.4 Uitdaging: Innovatie mechanisme a la broedkamers Belastingdienst ontbreekt

Meerkeuze optie: Gekozen oplossing

Antwoord

Een innovatie Stormbaan (Broedkas) opzetten.

De behoeften van de eindgebruiker met hun problemen in kaart brengen. Hier kleine scopebepaling voor maken en vanuit de marktorganisaties uitnodigen en samen in de innovatie Stormbaan zetten. Voorleggen: dit is ons probleem en onze eindgebruiker heeft aangegeven dat hij dit wil: Ontwikkel maar. Hierbij het falen stimuleren, want daar leer je van. Iedereen vrij laten en samen laten werken om binnen de scope tot een innovatieve oplossing te komen. Dit aan de eindgebruiker presenteren: Zo goed? Zo opgelost? Ja of nee en door.

3.4.5 Uitdaging: procurement / inkoop

Meerkeuze optie: Gekozen oplossing

Antwoord

Issue: verschil in visie t.a.v. omgang met en contractering van leveranciers, tussen wat het programma voorstaat (samenwerking, agile, flexibel) versus hoe inkoop traditioneel werkt.

Oplossing: Inkoop moet gaan acteren in lijn met het programma. Inkoop moet beter, sneller, directer aanhaken op het programma. Grotere betrokkenheid nodig vanuit Inkoop.

Dit programma vergt flexibiliteit in Inkoop, c.q. nieuwe manieren van inkoop. Inkoop zal dit moeten faciliteren.

Mogelijk ook capaciteitsprobleem. Hier kan ook nu al op voorgesorteerd worden.

3.4.6 Uitdaging: Infrastructuur

Meerkeuze optie: Gekozen oplossing

Antwoord

Dit gaat vooral om de technische implementatie van de infrastructuur. Maak de infrastructuur architectuur ondergeschikt aan de eisen van het informatiedomein. Ook in het infradomein zijn flexibele oplossingen als (local) cloud, PAAS, software defined storage en software defined networking etc..

Meerkeuze optie: Voordelen

Antwoord

Wendbare infrastructuur, die zich aanpast aan de informatiebehoefte.

4 Governance

4.1 Hoe ziet u de verdeling van verantwoordelijkheden van de IT Toepassingen in de exploitatiefase?

Meerkeuze optie: Verantwoordelijkheid Defensie

Antwoord
Wensen eind gebruiker duidelijk in kaart.
Acceptatie nieuwe werkwijze (Sprints).
Afsluiten beheercontract met beheerpartij.
Benefit Management.
Beschikbaarstellen resources vanuit gebruikersperspectief bij sprints.
Beslissen over nieuw te realiseren wensen.
Bewaken roadmap.
Bewaking gebruik/adoptie.
Blijvend stimuleren van innovatie; we zijn nooit klaar.
Business alignment.
Business Lifecyclemanagement.
Defensie durven spiegelen op efficientie en effectiviteit.
Defensie zal te allen tijde de regie in de beheer fase zelf moeten uitvoeren.
Dependency Management.
Duidelijk doorontwikkelplan.
Duidelijke verantwoordelijken/probleemeigenaren.
Duidelijke verantwoordelijkheden en bevoegdheden.
Durf innovatie intern te motiveren.
Eerste (en tweede-?) lijns gebruikersondersteuning.
Functionele vraag blijven definieren.
Geen belemmeringen voor continu updaten van applicaties, ook al zijn nieuwere versies geïniteerd door andere klanten dan Defensie.
Interne gebruikers stroomlijnen naar en gestandaardiseerde omgeving.
Life cycle management.
Managen van afhankelijkheden tussen services en toepassingen
Ook in exploitatie fase zal zeker in de beginfase een Advisory Committee actief moeten zijn. Voorzitterschap bij defensie. Marktpartijen hebben een adviserende rol.
Opdrachtgeverschap.
Opstellen van SLA: functionele specificatie van minimale performance.
Partner betrekken in besluitvorming over releaseplanning.
Primair dagelijks beheer ligt bij Defensie. Updates/Upgrades/SLA/Support/etc. ligt bij de contractpartij. Bij onderlinge afhankelijkheden tussen systemen kunnen Defensie en verschillende leveranciers van deze systemen samenhangende SLA's/support constructies opzetten om de continuïteit van de omgeving te borgen.
Productowner.
QoS (esp. voor business informatieservices).
Regie houden.
Regie op continue doorontwikkeling.
Regievoering.
Ruimte aan de markt om mee te denken.

Antwoord
Ruimte voor innovatie.
Service Delivery Manager.
Service owner.
Strategisch Beheer.
Strategisch management.
Structurele innovatie.
Taken kunnen gedelegeerd worden, maar verantwordelijkheid berust bij Defensie. Dat gezegd hebbende vallen in een goed governance model wel afspraken te maken en bijbehorende middelen (niet alleen budget, maar ook mandaat) beschikbaar te stellen.
Uitbesteden of zelf beheren.
Zorgt voor discipline bij het gebruik van de toepassingen.

Meerkeuze optie: Verantwoordelijkheid Markt

Antwoord
Aandragen vernieuwingen.
Actief aandragen mogelijkheden voor verbetering.
Adviseer m.b.t. optimaal gebruik van oplossingen.
Applicatie Onderhoud/Adaptief in weer nieuwe sprints.
Applicatieonderhoud.
Bereid zijn om kort cyclische trajecten te lopen.
Bijhouden roadmap leveranciers van IT-oplossingen: signaleren nieuwe mogelijkheden, upgrades.
Continue stroom van opgeleverde resultaten aan Defensie.
Cyclische Rationalisatie en Consolidatie.
Defensie durven spiegelen op efficiency en effectiviteit.
Het overdraagbaar houden van kennis in geval van noodsituatie.
Het runnen nu de applicatie gebeurt onder verantwoordelijkheid Defensie. In alle gevallen gemengde teams en flexibiliteit in aansturing aan te geven door Defensie. Demand management.
Inbrengen best practices en marktstandaarden.
Insourcen dan wel ondersteunen en onderhouden.
Leveren van cost efficiënte gestandaardiseerde available omgeving.
Levert op tijd en op maat de afgesproken functionaliteit.
Luis in de pels.
Meedenken op gebied van innovatie.
Meedenken over doorontwikkeling/releaseplanning in het kader van goed partnership.
Meeste vormen van support, behalve op wapensystemen.
Naleven beheercontract.
Naleven SLA t.a.v. maintenance, support, trouble shooting, bug solving, maken kleine aanpassingen.
Operationeel beheer.
Opleiden. Grote changes.
Platform innovatie.
Proactief Defensie informeren met kennis, nieuwe toepassingen en mogelijkheden/innovatiemogelijkheden.
Resultaatverantwoordelijkheid op tijdige realisatie binnen betreffende kavel (binnen financieel kader).
Signaleren, rapporteren & acteren ter voorkoming en oplossen van incidenten.
Tactisch Beheer.
Technisch Applicatie Beheer.
Technisch Applicatiebeheer.

Antwoord
Technisch Lifecyclemanagement.
Tweede- of derde lijns gebruikersondersteuning.
Ultvoerende taken.
Zorgen voor een werkende oplossing en geen dikke rapportages met adviezen.

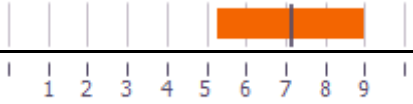
5 Evaluatie

5.1 Wat heeft u in de sessie niet kunnen inbrengen?

Antwoord
Goede sessie. Voor zover niet ingebracht, zal de schriftelijke ronde uitkomst bieden.
Het algemene gevoel over de omvang: erg ambitieus. Ook de groeikern. Advies is om samen met een aantal leveranciers een POC te definiëren. Dan wordt er veel duidelijk.
Voorkom een one-size fits everything aanpak. Niet alle toepassingen kunnen agile/SGA worden gerealiseerd.
Meer detail rondom de Big.
Kort cyclisch betekent andere houding en gedrag van MinDef medewerkers. Fouten maken mag. Dus breng lijn en samenhang in ontwikkeling organisatie en IV/IT doelstellingen.
Spanningsveld tussen 'act small' en intenties hieromtrent versus neiging om e.e.a in meer traditionele (gefaseerde aanpak)
Maak meer expliciet wat de scope is van het ontwerp, c.q. breng meer balans aan tussen bedrijfsvoering en operatie. Focus lijkt nu erg te liggen (ook in de bewoording) op de bedrijfsvoering.
Specifieke kennis en ervaring op expertise gebieden.
Architectuur rol in geheel (dik/dun/agile/...).
Defensie geeft aan kortcyclisch/iteratief te willen gaan werken en dat vraagt een andere aanpak. Je ziet echter in alle aangeleverde documentatie dat dit nog niet doorgevoerd is. Het enige dat er wezenlijk anders lijkt te zijn, is de tijdslijn. Je kan niet werken met volledige architectuurframeworks/specificaties/regiemodellen en d.an verwachten dat je Agile bezig bent. Er zal meer focus op doelen en minder op werkwijze moeten komen
In het kopje governance zijn de cultuuraspecten meegenomen. Mijn inziens niet correct: cultuur is een duidelijk ander onderwerp en zal apart behandeld moeten worden.
Elementen die niet te delen zijn met concurenten.
Details, maar is geen problem.
Programmamanagement good practices vs bad practices.
Mijn ideeën.

5.2 Wat vond u van deze sessie?

Invuladvies: Geef een score tussen 1 en 10, waarbij:
1 = geen goede sessie
10 = hele goede sessie
IT toepassingen

Onderdeel	-	Gemiddelde van de score	St.dev.
IT toepassingen		7,2	1,9
		7,2	1,9

5.3 Welke tips, suggesties of opmerkingen heeft u voor ons of kunt u ons meegeven?

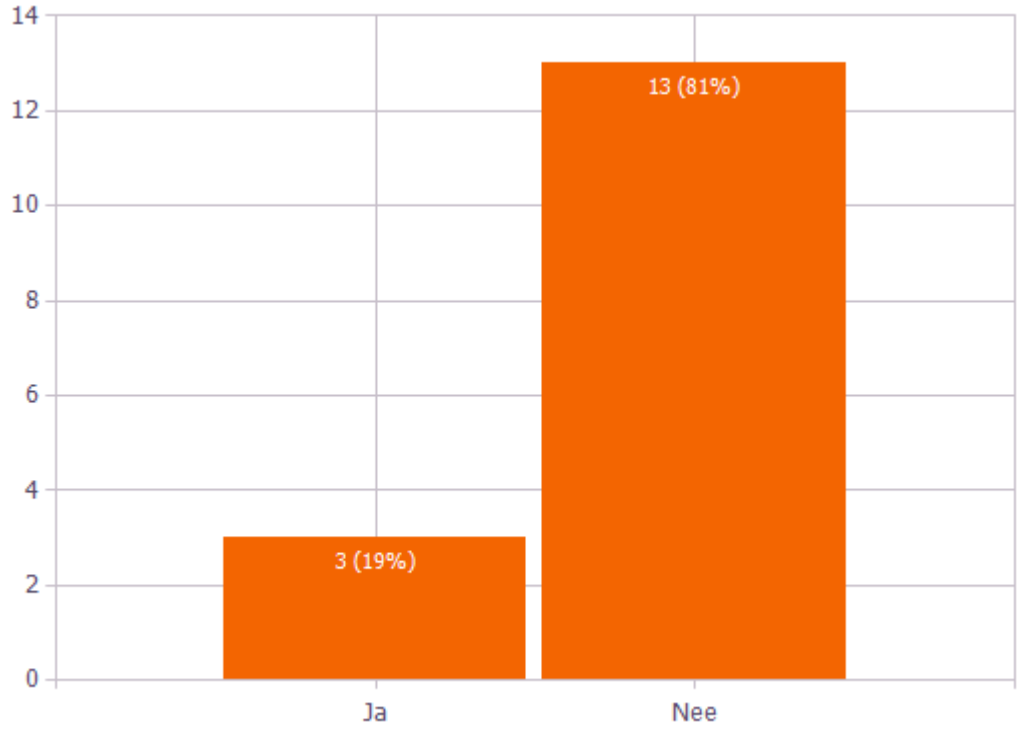
Antwoord
Overweeg het vervolg beter toegankelijk te maken voor Engelstaligen.
Slim gebruik van deze software in toekomstige architectuur sessies kan besluiten inderdaag versnellen.
Vooraf vragen sturen (met beperking in omvang antwoorden) kan helpen in kwaliteit en biedt ruimte voor discussie.
De beantwoordingstijd is wel extreem kort voor de grote hoeveelheid vragen. Dit zal ten kostte gaan van de professionaliteit van de beantwoording.
Alle tips zijn al gegeven.
Er zou beter vooraf gecommuniceerd moeten worden over welke onderwerpen aan bod gaan komen. Voorkoken van antwoorden is niet gewenst dus vragen verspreiden is niet nodig, maar een aanwijzing welke soort vragen er gaan komen zou wel zinvol zijn.
Kortere samenvatting verstrekken met kern van verhaal (elevator pitch).
De sessie is grotendeels gebaseerd op gesloten vragen of beperkte keuzes. Een aantal stellingen en een discussie onder de deelnemers had de mogelijkheid kunnen bieden voor onverwachte inputs.
Risico is dat de antwoorden een hoog Twitter gehalte krijgen: wel heel kort en bondig, zonder ruimte voor nuance.
Leveranciers zouden best kunnen aangeven wat zij van Defensie nodig hebben/verwachten om zo goed mogelijk in te spelen op de vraag.
Meer interactie.
Vakantieperiode is een lastige tijd voor dit soort mooie initiatieven.
Er zijn teveel onderwerpen, waardoor er nauwelijks onderlinge interactie is. Ik heb tijdens de rookpauze invollere standpunten van de deelnemers gehoord dan dat ik in de sessie verwoord heb gezien.
Een globale indicatie van de vragen vooraf zou prettig zijn, zodat we de stukken daar nog eens op kunnen nalezen. Gezien de korte tijd van het proces is het niet doenlijk alles grondig te bestuderen.
Sessies zijn goed, tooling die gebruikt wordt om de sessie te houden staat niet op punt. We hadden feedback op voorhand kunnen in brengen in een survey en dan feedback geven tijdens een interactieve sessie.
Misschien iets meer werken met stellingen en meer interactie.
Zou mooi zijn als er meer ruimte komt voor interactie.
Iets meer tijd voor voorbereiding ten aanzien van de vragen..
Ruimte geven voor visie delen en discussie met de aanwezigen hierover
Volgende keer graag eerder dit soort sessies aankondigen en bij voorkeur niet in vakantieperiode.
Geef aan het begin van de sessie iedereen de ruimte om zich kort te introduceren en om toelichting te geven wat de beweegredenen zijn om deel te nemen aan de sessie.
Andere aanpak met meer ruimte voor interactie en toelichting.
Iets meer de discussie tussen de marktpartijen op gang brengen.

Rapportage
IT Management

Inhoudsopgave

1 Feedback op DoIT

1.1 Vindt u dat DoIT 0.7 op het gebied van IT management de definitieve versie mag worden? (dus geen aanpassingen meer)

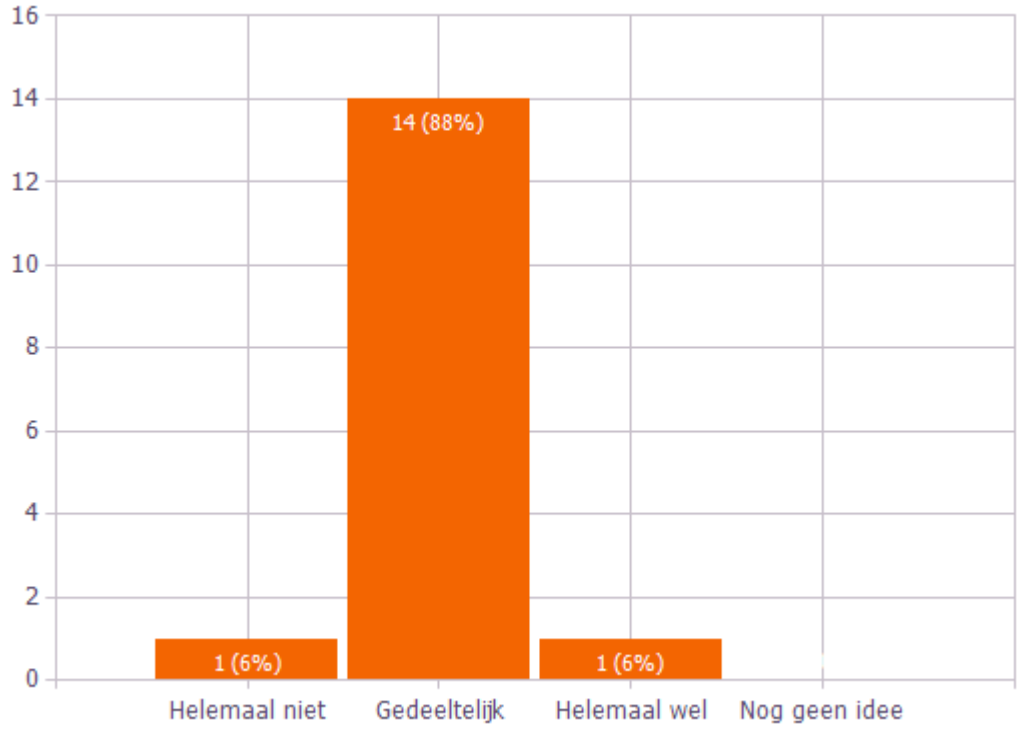


Aantal antwoorden 16

Antw.	Nummer	Percentage
Ja	3	19%
Nee	13	81%

1.2 In hoeverre acht u de ambitie van Defensie haalbaar voor de 1ste oplevering van de groeikern?

Denk hierbij onder andere aan de beschikbare tijd, de omvang van de werkzaamheden, één uniforme werkplek, Alles als een service aanbieden, de Defensie Appstore of de doelstelling dat binnen 5 jaar uit huidige realisatiedomein opgeheven kan worden.



Meerkeuze optie: Helemaal niet

Antwoord
Te omvangrijk voor een volledige realisatie in een half jaar

Meerkeuze optie: Gedeeltelijk

Antwoord
Business commitment voorwaardelijk - impact op functionaliteit en mensen gevalideerd Politiek (intern + Den haag) commitment te valideren - impact op investeringen, mensen en bedrijfsvoering geaccepteerd
Ambitie (net als de visie) is absoluut haalbaar maar hoeft niet in 1 keer haalbaar te zijn, wederom 'Think big,act small' is in onze beleving een goede benadering en de plateauplanning goed. Op sommige punten is nog wel een verdiepingsslag nodig, hier komen wij in de schriftelijke RFI-beantwoording op terug. Maturity model: groei nodig in verschillende aspecten om uit te groeien tot shared service organisatie en High Performance Organisatie, met name relevant voor de "mode 2" organisatie. Blijft als vanzelfsprekend cruciaal om oog te houden voor de "mode 1" organisatie met het oog op de continuïteit van de huidige IT en de daarbij benodigde expertise en kennisbehoud.
Mits organsatie verandert van analoge managers naar digitale managers, politiek een lagere prio krijgt. En de beslissingen sneller worden genomen bij kern beslissers
Implementatie en bepaling van de juiste meetpunten voor de benodigde governance.
Ambitie is groot, vraagt om krachtige besluitvorming aan de kant van defensie
Afhankelijk van politieke wil en de wil om te veranderen en samen te werken binnen de onderdelen

Antwoord
wanneer gewerkt gaat worden volgens think big act small kan MinDef op onderdelen succesvol zijn. Randvoorwaarde is wel dat de basisinfra op orde is, de regiefunctie ingeregeld is en er sprake is van heldere IT-Managementfunctie
Zeker mee starten. Anders gebeurt er niets. Er zal een cultuurverandering moeten plaatsvinden. Daarnaast hangt het af van de ervaring van het team. Dus selecteer een team dat dat al eerder gedaan heeft.
alles lukt niet. te uitgebreid.
Hangt af van de veranderbereidheid intern in defensie en de mate waarin eenvoud en aanpassingen in werkprocessen leidend zijn
De ambitie is alleen haalbaar bij een continuïteit in besluitvorming en een goede sturing hierop door bestuurders en management over de hele organisatie en zijn keten partners
Gunning dit jaar wordt een uitdaging, oplevering van de eerste onderdelen binnen 8 maanden is wel een heel grote uitdaging
Deadline is tijd, requirements flexibel afh van geld, dus gedeeltelijk haalbaar

1.3 Kunt u uw feedback geven op het gedeelte IT Management in het DoIT

Inleiding

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Duidelijk vehaal, mooie ambitie
helder verhaal
goede inleiding, wel wat meer achtergrond over wat de business-doelstellingen zijn

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Nu wat karig benoemd, wellicht handig in het licht van elan en Agile om hier ook wat sturing aan te geven in de vorm van Visual-management-mogelijkheden binnen de benodigde tool-set (anders denken en doen)
Informatiebeveiliging moet een integraal onderdeel van handelen worden (dus ook bij de vraag); deze Security component zoveel mogelijk standaardiseren binnen de sprinters- en de Devops teams, anders zou dit een erg vertragende factor kunnen worden voor de sprints
erg korte inleiding met aantal open deuren. Maak juist de inleiding meer SMART
Toevoeging van de grotere betekenis en belang hiervan voor defensie vergroot inzicht en betrokkenheid
er wordt gesproken over "autonome teams die integrale verantwoordelijkheid hebben". Gaat dit alleen over IT, of over de IV-services die via IT geleverd gaan worden? Kan nogal impact hebben
te summier wat mij betreft, zoek toch iets meer strategie
samenhang met regie en organisatie verduidelijken

Meerkeuze optie: Is nog niet beschreven

Antwoord
IT management is erg operationeel beschreven, gericht op het realiseren van toepassingen. Meer aandacht is nodig voor bijvoorbeeld project portfolio-management, architectuur, het wijzigingsproces etc. IT4IT (Open Group), MoP, BISL en ASL kunnen hiervoor handvatten geven

Devops

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Vraagt wel om een nieuwe manier van werken en met name van verwerven.
Generieke beschrijving voldoet
Dit is een bewezen methode. Ervaring bij andere overheden met DevOps binnen halen.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Toepassing specificatie mist - niet ieder onderdeel van het landschap behoeft DevOps. Waar liggen de grenzen, waar ligt het onderscheid, bij wie zou de verantwoordelijkheid moeten liggen
Niet alles leent zich voor Devops. Denk aan het implementeren van pakketten of infrastructuur migraties
DevOps is een acroniem voor de “agile” werkwijze Development en Operations, een nauwe en kort-cyclische samenwerking in kleine teams van (software) ontwikkeling en systeembeheer. Ik mis hierin, en in de rest van deze paragraaf, de rol en betrokkenheid van de eindgebruiker.
m.n. mogelijke wijze van samenwerking. ruimte die er is
Vraagt ook om een nieuwe manier van werken en met name verwerving binnen defensie
Wat zegt dit over een duurzame DNA-verandering bij defensie en de samenwerking intern en met haar partners?
Definitie van Devops in the document (12.2) stemt niet overeen met de marktdefinitie.
Hoe gaat Dev-Ops zich verhouden tot het voorgestelde Change Management framework. Kortom, hoe wordt een stuwmeer van nieuwe ontwikkelingen voorkomen.
DevOps vraagt om implementatie over de gehele keten tot en met involvement van de feitelijke business, dit komt er nog niet uit
Lijkt netwerk te suggereren terwijl regie nog in ketens denkt
Devops vergt een behoorlijke cultuuromslag (vooral ook aan de klantzijde) daarnaast hebben jullie een aantal ketens beschreven; wellicht ook handig om voor de flexibiliteit ook een onafhankelijk Devopsstream mee te nemen in de planning, gezien de aard van werkzaamheden binnen defensie en de politieke weerbarstigheid van besluitvorming

Devops en Informatiebeveiliging

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Tooling is ondersteunend, er is genoeg tooling beschikbaar in de markt om een goede SecDevOps plan te managen. Zou hier geen problemen in zien.
De SecDevOps aanpak is een goede methode omdat dan ook de secruity autoriteiten onderdeel uitmaken van het DevOps team. Zij moeten echter voldoende kennis en mandaat hebben voor snelle besluitvorming.
Is duidelijk, echter wel vraagtekens of de OTAP-strategie voor een redelijke prijs haalbaar is

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Probeer verdergaand te prioriseren wat de belangen zijn van DevOps ten opzichte van de andere onderdelen in de goeikern. Basis op orde lijkt me een eerste stap alvorens vergaand te automatiseren. Schep die helderheid ook naar de leveranciers en interne stakeholders
Door voor SecDevOps te kiezen zal nog duidelijker moeten worden ingezet op automatisering om de beschreven principes te borgen, maar geen onnodige vertraging te veroorzaken.

Antwoord
waar liggen de toleranties en waar niet
Goed dat het benoemd is, moet wel stevig verankerd worden in het defensiedomein
Maatregelen bij risico's bij open innovatie verduidelijken

Processen en tooling

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Ambitiestekking m.b.t. Management kan duidelijker. Bijv. maximale inzet tooling, maximale inzet standaard procesmodel kan explicieter, maximale transparantie en rapportages. Daar waar IT-management uit verschillende onderdelen en functionele verantwoorelijkheden bestaat, helpt een visie op onderscheidende elementen in management voor interne- en markt partijen
onvoldoende concreet
Moet innovatie direct aan alle security etc eisen voldoen, of kan innovatie in een afgesloten omgeving worden vorm gegeven en pas later worden getoetst aan architectuur, security, etc. Risico bestaat anders dat innovatie wordt doodgeknuffeld door de formele wereld.
Wil je hier echt zoeken naar meer partnership-relaties, dan kan het - ook gezien het belang hiervan voor defensie - wijs zijn te overwegen partners uit te dagen tot herijking van bestaande standaarden te komen
hoe sluit je in een samenwerking processen en tooling op elkaar aan. Beschrijving is nu nog erg algemeen
Besteed ook aandacht aan ontwikkel- en beheerstraten. Het samenstel van processen, tooling, methoden en technieken, competenties om software te realiseren en te beheren.
Erg algemeen zonder keuzes, wat voor een uit-vraag vergelijkingen erg moeilijk zal maken
Processen in een flexibele omgeving is lastig omdat vrijwel alles ad-hoc gebeurt.
Nog weining diepgang in relatie tot DevOps
Meer duidelijkheid nodig hoe de gekozen frameworks op elkaar gaan aansluiten.

Meerkeuze optie: Is nog niet beschreven

Antwoord
Betrek verandermanagement als onderdeel van dit programma, niet als een nevenstaand programma (uit de toelichting begreep ik dat dit nu het geval lijkt)

Gehele hoofdstuk (irt) document

Meerkeuze optie: Is voldoende duidelijk

Antwoord
In algemene zin onze complimenten voor het opgeleverde werk. Het Defensie team heeft de verleiding kunnen weerstaan om te detaillistisch te worden. Functioneel is functioneel gebleven!
op moment van start zal er sowieso moeten worden geanticipeerd op de aanpassingen/veranderingen (org) en aanbod van innovatieve mogelijkheden. De crux zit hem in tijd

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Ambitie is helder, op onderdelen concreter; duidelijke keuzes maken; wijze van samenwerking
Erg algemeen, theoretisch, wat erg veel ruimte geeft voor (niet altijd gewenste) verschillende invullingen. Samenvoeging met Regie en Organisatie lijkt gewenst.

Antwoord
Kaderstelling is goed, op onderdelen mag er verdieping komen, zeker met de input van marktpartijen.
(Organisatie) voor de ketens en de ketenpartners wordt samenwerken essentieel (gezien de continue verbeteringen die gewenst zijn). De regie over deze ketens moet onafhankelijk sturend binnen het team gedaan kunnen worden, de overkoepelende (afhankelijkheden) regie zou scherper benoemd kunnen worden hoe dit te regelen.
Samenvoegen met Regie en Organisatie
Ik vind dit wel een erg veel IT gedreven hoofdstuk. Harde IT wel te verstaan. Ik mis de betrokkenheid van de eindgebruiker als vraagkant die sterk bepalend moet worden voor het vormgeven van de IT/IV services en bijkomende IT-Management consequenties

Meerkeuze optie: Is nog niet beschreven

Antwoord
Welke IP komt mee vanuit de bestaande organisatie die hergebruikt kan worden.

1.4 Kunt u uw feedback geven op het gedeelte Regie in het DoIT

Governance & Regie

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Mooie ambitie

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Het kan werken als de bevoegdheden en mandaat ook aan het DevOps team worden gegeven.
De verdeling van de verantwoordlijkheden tussen marktpartijen en defensie.
Samenwerking met de markt gaat naast regie vooral over het (onder)houden van een Partner Ecosysteem, het werken met kleinschalige en/of strategische partner(s) gericht op Open Innovatie. Ik neem aan dat dit per domein binnen MinDef kan verschillen. Wapensystemen of ondersteunende bedrijfsvoering stellen echt andere eisen.
Onduidelijk hoe een strategische partner wordt geselecteerd. Team zal uit verschillende disciplines bestaan, maar vooral ook uit eindgebruikers vanuit de werkvloer. Kan Operation dit aan? Kunnen zij voldoende eindgebruikers aanleveren met voldoende kennis.
Regie gaat nog sterk uit van een centraal coördinerende rol, terwijl je alle partners uit wil dagen je overhead- en transactiekosten zo laag mogelijk te houden. Bedenk wat je uit kunt vragen m.b.t. regulaties en omstandigheden die partners in kunnen brengen om het voor defensie beter en goedkoper te maken, zonder dat defensie in hoeft te leveren aan grip.
Erg algemeen
Het is mij niet duidelijk hoe aan de ketenregie vorm wordt gegeven, denkt men aan SIAM?
Ik mis informatiebeveiliging als onderdeel van assurance
Als de business leidend is: hernoem IT-governance naar governance. Voorkom dat het te veel beleefd wordt als een IT-feest. Business is in the lead.
Regie vervangen door collaboratie en ketens door netwerken.

Open Innovatie

Meerkeuze optie: Is voldoende duidelijk

Antwoord
t.a.v. ambitie

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Goed platform, maar prioriteiten zijn wel nodig om te voorkomen dat er teveel tijd door defensiepersoneel wordt opgebruikt om de uitvoering met de ketenpartners in te regelen. Op welke wijze ga je uiteindelijk prioriteren, tenzij de innovatie geheel zonder defensie gedaan wordt.
erg theoretisch. Kan ik het niet mee oneens zijn. Maar hoe nu verder?
Co-creatie en innovatie in de groeikern (figuur 34) is minder gelukkig voor de eerste oplevering die in een half jaar moet gebeuren **(i.p.v. worden opgeleverd)**.
Open innovatie in relatie tot IP-eigenaarschap?
Hoe borg je dat dit een continu proces blijft? Vaak blijft het bij mooie beloften van de markt en goede bedoelingen van opdrachtgevers.

Antwoord
Dit moet niet alleen gaan over processen (wat nu vooral het geval is), maar ook over omstandigheden en condities die innovatie bevorderen; bevraag de markt hiernaar, want dit voedt op positieve wijze de DNA-verandering binnen defensie. Zeker als je relatief kleine partijen en nichespelers de kans wilt geven.
Kan defensie als organisatie met deze concepten omgaan in relatie met haar stakeholders?
Meer uitwerken wat er gewenst wordt
Criteria benoemen voor adoptie van open innovatie.

Shared Risk & Reward

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Echter, nog niet veel succesvolle voorbeelden gezien in publiek-private samenwerkingen.
Vraagt wel om een nieuwe manier van inkopen

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Er staat: Het delen daarbij van risico's is een beproefde werkwijze om de balans tussen succes en falen, met de bijbehorende kosten, beheersbaar te houden. Juist in een innovatieperiode moeten risico's genomen kunnen worden om te beoordelen wat voor een impact die hebben. Hier lijkt het alsof risico's de beslissende factor wordt voor wel/niet innovatie. Ik zou graag meerwaarde voor business proces als leidend willen zien
Terechte verwachting waarbij de markt veel meer zou kunnen als dat ze momenteel toont. Echter dit vereist wel een constante open dialoog en flexibiliteit in contractuele invulling. Wat hierbij helpt is een business case en invulling belangrijkste business drivers zodat de regie functie i.s.m. met de markt proactief invulling kan geven aan dit concept.
In het kader van samenwerking in NATO-verband (of kleiner binnen Europa), geef partijen de opening via de NL Defensie in beeld te komen bij andere landen; 'beloon & betaal' met zaken die defensie geen geld kosten
Dit ligt ingewikkelde bij de grote marktpartijen rondom IP
Shared Risk en Reward, is een mooie opzet maar ook lastig uit te voeren, om er voor te zorgen dat iedereen ook mee blijft doen, hoe voorkom je overlap met verschillende aanbieders en een gevecht op innovatie, (ervaringen bij andere klanten) En als je dit oplost hoe voorkom je bij een grote reward dat je toch een impliciete verdor-lock-in krijgt) Dus goed idee maar wellicht iets verder uitwerken qua uitvoering (kan ook in versie 1.5)
ambitie duidelijk. vooral kijken naar mogelijkheden om dit concreet vorm te geven
ambitieus, maar kan haalbaar zijn
Zal per deelgebied/partner verder uitgewerkt dienen te worden
Product Owners zal veelal vanuit de Business worden aangeleverd. Die bepaalt uiteindelijk per sprint of het product tot dusver akkoord is. Dus risico management vindt plaatst door deelopleveringen in sprints. Duidelijk maken over welke risico's er worden gesproken?
Lijkt mij lastig bij publiek-private samenwerking met heel verschillende doelstellingen.

Open Innovatie Strategie

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Hangt nu op goede bedoelingen: 'er moet voldoende vertrouwen zijn', 'er moet een cultuur ontstaan'. In commerciële relaties is het raadzaam hier KPI's op te definiëren
Laat mensen rouleren over de partijen in het eco-systeem heen (dus ook defensie) en creëer open / living labs
Mooie en nodige ambitie hetgeen procedureel en contractueel tussen Defensie en 1 partner prima in te vullen is. Echter met naar verwachting is dat er een eco-systeem aan partners zal ontstaan, waarmee partijen bescherming op IP en investeringen zullen verwachten. Een visie hierop zal helpen voor externe partijen
Dit vraagt om echt partnerschap i.p.v. Het aloude opdrachtgever en opdrachtnemersschap
En hoe nu voor Defensie?
Benadruk ook de verbinding met de business innovatie
Niet concreet genoeg.
Innovatie en de risk-share opzet is een goede maar ook tevens een uitdaging om uit te werken, daarnaast hoe voorkom je dat je door het inrichten van deze ketens (juist) geen verdor-lock-in gaat krijgen) Regie over innovatie moet dan ook onafhankelijk gevoerd kunnen worden. Hoe voorkom je dat er te veel innovatieve producten komen die teveel tijd van de defensie organisatie vergen en hoe stel je daarin prioriteiten?
Zorg dat uitgewerkt wordt hoe specialistische markt partijen een rol krijgen binnen dit domein.

Gehele hoofdstuk (irt) document

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Past prima is de gehele context
Duidelijk. Toelichting is bekent!! en is reeds gedeeld

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Creëer naast innovatie - gericht op het vinden van nieuwe oplossingen voor bekend problemen / behoeften - heel bewust een deel voor co-creatie, waarbinnen je alle partners complexe vraagstukken voorlegt die toekomstbepalend zijn voor defensie
Borgen in de praktijk, ambitie is goed.
vooral wijze van samenwerking. regieorganisatie moet geen eigenstandige besluitvormingsorganisatie worden, maar faciliteren. verdeling verantwoordelijkheden moet duidelijk zijn. hoe bij samenwerking tot besluitvorming wordt gekomen. vooral als er duidelijke verschillen van mening zijn. echter vooral ook beginnen en expliciet lering trekken.
Gedeelde regie principes die minimaal tussen de marktpartijen en defensie aanwezig moeten zijn om tot samenwerking te komen (vanuit Defensie Oogpunt).
niks meer toe te voegen aan onderstaande punten van anderen
Mag nog een verdere uitwerking waarbij er meer naar praktische invulling gekeken mag worden.
Samenvoegen met IT management en Organisatie
Zoals ook voor de devops-teams en de bijbehorende ketens moet er zowel regie binnen de ketens als over de ketens gevoerd worden zonder een nieuwe bureaucratie te introduceren. Hoe borg je dit, hoe borg je de sturing vanuit de klanten, dat deze niet continu over de hiërarchische as gevoerd wordt, (wat ga je doen aan awareness bij de opdrachtgevers en de ketenpartners)

1.5 Kunt u uw feedback geven op het gedeelte organisatie in het DoIT

High Performance IT Domein

Meerkeuze optie: Is voldoende duidelijk

Antwoord
De ambities komen duidelijk naar voren.
Helder
Het einddoel is goed beschreven. Alleen de weg daarnaar toe zal meer tijd kunnen kosten. Advies is om te starten met een niet al te complexe applicatie die meerdere lagen raakt.
Is helder, maar een stevige uitdaging.
Top, maar vergeet niet dat al het personeel (en de ketenpartners) ook mee moet draaien in dit perspectief, dus een duidelijke UP or OUT strategie is nodig op het personele vlak (ook voor Bimodaal model)
ambitie is helder

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Gekoppeld aan DevOps invulling is de definitie van high-performing afhankelijk van de klant en de technologie. Net als bij de data rubricering zou invulling hiervan de regie functie en markt helpen de juiste performance te leveren
Graag meer praktisch, bv met een kwantificatie

Bimodaal & Perspectief

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Bimodaal perspectief van Gartner duidt dat er binnen landschappen een duale wereld ontstaat, klassieke it die procesmatig wordt beheerd, en nieuwe it waarbij wendbaarheid en flexibiliteit aan business wordt geboden door agile/devops visies
Gedurende de transitie en naar verwachting lang erna zal niet een bi-modale maar een multi-modale wereld bestaan. Type technologie (IT versus OT), business specifieke behoefte en veiligheidseisen helpen om dat beeld scherp te stellen. Vraag is of dit al onderdeel van de aanbestedingsinfo moet zijn of samen met de markt vormgegeven dient te worden
toelichten
Onderscheid in bi-modaal is prima, mar liever niet langs de lijnen van oud en nieuw. ook nieuw te verwerven IT kan zich gedragen als een system of record met daarbij passende werkwijzen.
Meer detail nodig
Erg geschreven vanuit het oogpunt van de huidige organisatie. Hoe passen de partners hierin ?
Goed idee is ook binnen de overheid vaker toegepast, vergt wel vaak een dubbele investering qua uitvoering. Hoe zorg je voor de juiste transitie van personeel (wie wil je waar hebben) en hoe hou je personeel vast in dergelijke situaties als dat toch mogelijk is.

Kenmerken Huidige IT versus Nieuwe IT

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Helder
Zeer goed. Een duidelijke visie en hier spreekt vooral de mogelijkheid tot snel kunnen veranderen uit. Zoals eerder gemeld en geldt voor gehele document, dit dient een brede ondersteuning van gehele directie te hebben. Zowel aan de demand als aan de supply kant. ITGB heeft hier een uiterst belangrijke rol in

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Bij de uitvraag zal defensie scherpere aanbiedingen krijgen als heldere doelstellingen worden gesteld bij de verschillende werelden. Bijv. Oude wereld dient z.s.m. uitgefaseerd (overgezet) worden versus flexibiliteit diensten in nieuwe wereld
leg het nog een keer naast Modus 1 en Modus 2 van Gartner
Minder verduidelijking nodig dan eerdere gedeeltes, is meer praktisch. Denk wel aan de culturele aspecten

Meerkeuze optie: Is nog niet beschreven

Antwoord
ik mis sturing op IT domein van wel of niet bereiken van beoogde business doelen. En ik mis anticiperend beleid op toekomstig verwachte services vanuit de business. IT blijft in dit beeld achter de werkelijkheid aanlopen, terwijl er juist veel meer feeling met de toekomstige behoefte moet ontstaan. Banken sturen daar bv actief op. Time to value, time to innovation.

Joint SecDevOps Teams (JST's)

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Dit is een goede uitgangspunt.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Tip: de financiële keten lijkt nu leidend / bovenliggend aan o.a. matlog. Als je wilt bereiken dat defensie echt vernieuwd, dan is geld vanzelfsprekend heel belangrijk, maar zet het dan meer onderaan. Dat kan meteen aantal spelers - ook intern defensie - een groot verschil maken.
In hoeverre is zo'n team dynamisch? m.a.w. kunnen er partijen toegevoegd worden als de innovatie daar om vraagt? En vertrekken?
Ervaring van Defensie in andere gebieden gebruiken?
Niet alles zal via SecDevOps teams geleverd kunnen worden. Denk hierbij aan aanpassingen aan legacy die op een klassieke werkwijze moeten plaatsvinden of het implementeren van een standard toepassing die met een wapensysteem meegeleverd wordt.

Methodieken, Modellen & Frameworks

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Helder
Is duidelijk

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
De voorgestelde ontwikkelstandaarden en frameworks zijn weliswaar marktconform maar deze zullen wel binnen de defensiecontext op elkaar moeten worden afgestemd. Door kritisch te kijken naar de bruikbaarheid en samenhang van de componenten vanuit de gekozen frameworks kan Defensie steeds meer op een Agile/Lean manier acteren. Een zwaar change management proces dat niet geautomatiseerd is middels standard changes werkt averechts binnen een SecDevOps cultuur waar veel afhankelijkheid bestaat van verregaande automatisering.
Er wordt verwezen naar verschillende architectuur modellen. Aangezien defensie in nato verband samenwerkt, is het dan niet verstandiger om het architectuur model van de Nato als standaard te hanteren? Uit de praktijk blijkt dat door teveel vast te houden aan het eigen frameworks, internationale oplossingen vaak worden buitengesloten.
Is een algemeen beschrijvend verhaal, er dienen specifieke keuzes gemaakt te worden, wellicht tijds-afhankelijk. Maar gezien de korte implementatietijd van het geheel mag hier in het eerste jaar geen onduidelijkheid over bestaan wat de weg dan is
Kies naast modellen ook technieken en rapportages en tooling de passen bij de nieuwe organisatie, VM en dergelijke praktische uitwerkingen in combinatie met de genoemde Modellen. Zorg error dat de modellen en technieken geen doel op zich worden (slechte ervaringen bij andere overheids-onderdelen)
Het hoog-over benoemen van de gekozen frameworks (ITIL, Six Sigma, SAFE, etc.) is niet voldoende. Het Bimodale aanpak vereist duidelijkheid over de interfaces tussen de nieuwe manier van werken en de "oude manier van werken".
Methodieken en het gebruik van frameworks dienen een versnelling te bewerkstelligen
Strategisch portfolio management wordt gepositioneerd als alleen voor de JST's en daarmee alleen voor de nieuwe IT. Advies: richt het portfolio management in over de bestaande en nieuwe IT.

Lifecycle Management

Meerkeuze optie: Is voldoende duidelijk

Antwoord
Is wel durf voor nodig om ook de Kill en uitfasering ook werkelijk mogelijk te maken
Helder
Uitdaging begint bij het daadwerkelijk uitzetten van services, in praktijk ontbreken hiervoor de benodigde instrumenten. Advies is om dit bij start te regelen.

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
In een continu veranderende omgeving moet dit zwaar aangezet worden
wat is invloed vanuit de business op lifecycle management van IT/IV services? Hoe gaat IT dat integreren in de lifecycle modellen van de basisfuncties?
Het lijkt er op dat alles via maatwerk zal worden gebouwd. Dat lijk mij niet handig. Hoe om te gaan met complete applicaties waar de IP bij de leverancier zit.
Budget is bij deze een belangrijke voorwaarde

Meerkeuze optie: Is nog niet beschreven

Antwoord
Alleen een basisadministratie voor IT is onvoldoende. Denk aan een geïntegreerde oplossing voor de ondersteuning van alle IT-processen: IT4IT.

Gehele hoofdstuk (irt) document

Meerkeuze optie: Is voldoende duidelijk

Antwoord
voldoende duidelijk voor nu. zal vanzelfsprekend verder moeten worden uitgewerkt, handen en voeten moeten worden gegeven. dat kan echter werkende weg.
Stevige ambitie die om leiderschap vraagt

Meerkeuze optie: Moet nog verduidelijkt worden

Antwoord
Dashboard voor cockpit control?
toch nog erg veel theoretische modellen. Ik verwacht meer vertaling naar de toekomstige aanpak.
Sturing door middel van KPI's

Meerkeuze optie: Is nog niet beschreven

Antwoord
Hoe past datamanagement/het beheer van informatie in dit ontwerp?
Wat heeft Defensie geleerd over samenwerking tijdens internationale missies?

2 Governance

2.1 Uitdagingen

2.1.1 Waar liggen op het gebied van IT management volgens u de grootste uitdagingen?

Meerkeuze optie: Tijdens de realisatie van de groeikern

Antwoord
een strakke regie vorm vrij van politieke ambities. Dit vraagt nieuw en modern BLOED
Inspirerend leiderschap gecombineerd met besluitvorming, niet gehinderd door externe waan van de dag
De juiste balans vinden tussen vernieuwing, beheer en onderhoud.
Focus, Focus, Focus op de werkelijke opdrachten die zijn uitgezet, impact van nieuwe prioriteren (politiek of bestuurders) kunnen beantwoorden met Business-impact i.p.v. IT antwoorden!
De veranderkundige aspecten (business en IT)
de nieuwe business doelen bij schakelen
Gedefinieerde processen, tooling etc. (ontwikkel- en beheerstraten) om voorspelbaar (kwaliteit, tijd, middelen) nieuwe IT te realiseren.
de wijze van samenwerking met de markt realiseren die nodig is om de ambities te realiseren.
Transparantie over gehele keten
Veranderkracht Defensie Organisatie
Constant stimuleren van cultuurverandering richting agile, innovatief, out of the box, gericht op business value in plaats van IT standaard, geen bloedgroepen meer maar logische keuzes
een goede administratie van de goedkeuringen en wensen. Stel bij het begin globaal al vast hoeveel functionaliteit zal worden ontwikkeld. Goed is goed genoeg. Durf ook live te gaan met een 80% versie met alleen de musthaves.
adoptief vermogen om buiten de bestaande IT leveranciers Scope te durven kijken. Kennis en kunde ligt juist in het hoge segment bij MKB. durf deze mee te nemen om juist te kunnen versnellen
Bereid te zijn werkprocessen maximaal aan te passen aan de solution, niet andersom (durf op onderdelen techniek te adopteren als toekomstige asset en zet de mogelijkheden centraal, niet de kenmerken van de huidige omgeving waar het in moet landen)
DevOps vraagt om het ver-agilen van de "gehele" organisatie, deze cultuurverandering is de grootste uitdaging, met name op stakeholders
Het inrichten van de management/beheer tooling tijdens de realisatie dient gereed te zijn voordat de eerste exploitatie een feit is. Of wordt de huidige hiervoor gebruikt (niet benoemd/beschreven)
Het verbinden van de bestaande en nieuwe wereld: migratie en co-existentie. Werelden kennen hun eigen processen, tooling, competenties, normen etc. die sterk kunnen verschillen. Maar alleen een verbinding zorgt (zeker in de eerste plateaus) voor werkende business toepassingen.
IT managementmodel waarin ook de business duidelijk een plaats heeft en behoudt
Hoe voorkom je dat zo'n team niet terugvalt in klassiek gedrag?
Flexibiliteit van de leverende partijen op de business behoefte (noodzaak) van deze bijzondere gebruiker tijdens "werk in uitvoering"
Ontwerpen en realiseren van een IT management model dat echt EN kan meebewegen met de business doelen EN de uitgangspunten van IT/IV bewaakt
De continuïteit van de besluitvorming van bestuurders en Management tijdens de realisatie versus de operationele druk, het bimodaal model kan daar bij helpen mits deze niet virtueel zijn (zelfde resources gebruiken)
hoe vaak gaat u uw ambities aanpassen met acceptatie van meerdere partijen
iedereen meekrijgen (alle stakeholders) in de nieuwe ambitie en vooral cultuur en werkwijze.

Antwoord
Een nieuwe werkwijze vraagt om omscholing en een andere werkwijze. Advies is om het JST team dat samen gaat werken, vlak voor de start van de eerste sprint, gezamenlijk op te leiden. Tussen opleiden en start mag niet te veel tijd zitten.
Zowel infrastructuur als applicaties zullen gelijktijdig ontworpen c.q. uitgerold worden. Het zorgen dat er geen onjuiste aannames van de ene hoofdgroep op de andere zijn zal een grote uitdaging geven.
Is er voldoende kennis in NL beschikbaar?
Hoe selecteer je partners die samen door 1 deur kunnen?
Financiën in alle gevallen als randvoorwaarde neer te zetten en nooit als doel
De wijze van verwerving
Hoe de dynamiek te organiseren dat tijdens realisatie met verschillende partners zal ontstaan
Flexibiliteit van de gebruiker tijdens "werk in uitvoering"
Goed leiderschap
veilige en prikkelende innovatie omgeving met een strakke control op de gedefinieerde meerwaarde
Alleen waar dat echt niet kan afwijken wat de markt als standaard ziet
Bepalen en inrichten IT Service Management (People, Process & Technology) naast de bestaande operatie.
Cultuur omslag en richten van personeel van Defensie en de Ketenpartner en hun onderlinge samen werking, zorg ervoor dat de deadlines niet de samenwerking in de weg komen te zitten
De samenwerking met marktpartijen op basis van echte partnership.
Komen tot de gewenste samenwerking met de markt (model, governance, regie)
Huidige kennis en kunde binnen Defensie
Coördinatie over de keten - service integratie in een multipolaire wereld

Meerkeuze optie: Tijdens exploitatiefase

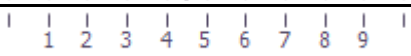
Antwoord
het ecosysteem op juiste wijze in stand houden, waarbij alle partijen recht wordt gedaan
Indien equipment ingezet zal worden (bv op missie) begrijp ik dat het over kan gaan van LGI naar HGI. Dit maakt overgang van beheer noodzakelijk van partners naar Defensie. De samenwerking tussen Defensie en de partners om een naadloze overgang te garanderen vraagt de nodige investeringen en vertrouwen
Het samenwerken met verscheidenheid aan tooling/processen
Als een applicatie stabiel draait en alles er eigenlijk er al inzit. Hoe zorg je dan dat de kennis opbouw aanwezig blijft? De teams zullen veel minder sprints per jaar hebben wanneer de applicatie is productie is. Advies is om te clusteren in productie en te zorgen dat de kennis kan worden behouden.
Effectief veranderen (opgestart tijdens realisatie van de groeikern) want 'als je blijft doen wat je altijd deed, dan zul je krijgen wat je altijd kreeg' - denk met name aan 'de laatste man op de werkvloer bereiken'
de continue afstemming en balans houden tussen vernieuwing en beheer
Geef andere NATO-partners toegang tot solutions, hanteer een open gebruiks-policy en laat hen helpen de producten en diensten beter te maken
Het openstaan voor nieuwe mogelijkheden en initiatieven in de markt
Wanneer is het een succes? Hoe definiëren we succes van IT Management?
Invulling geven aan de gewenste vorm en mate van innovatie met de markt, samenwerking met unieke marktpartijen maar toch standaardiseren of standaarden handhaven
De cultuur om over de machts-as in te grijpen op devops-teams prioriteiten te wijzigen sprints voller te maken dan kan etc. Het dichtdrukken van de nieuwe organisatie (alle lucht er uit) om de vernieuwing ook werkelijk vast te kunnen houden.
Uitbesteden of zelf beheren of wellicht in een combinatie
Change management staat haaks op ad-hoc innovatie
Bij delegeren van taken, 'de kunst van het loslaten' bij het geven van sturingsmiddelen aan partijen die het

Antwoord
support invullen (incl. bijbehorende besturingsmiddelen)
Standaardisatie over de keten

2.1.2 Hoe groot schat u de genoemde uitdaging in?

Geef uw mening op een schaal van 1 - 10, waarbij
1 = helemaal geen uitdaging
10 = zeer grote uitdaging

Onderdeel	-	Gemiddelde van de score	St.dev.
Cultuur omslag en richten van personeel van Defensie en de Ketenpartner en hun onderlinge samen werking, zorg ervoor dat de deadlines niet de samenwerking in de weg komen te zitten		8,8	1,3
Constant stimuleren van cultuurverandering richting agile, innovatief, out of the box, gericht op business value in plaats van IT standaard, geen bloedgroepen meer maar logische keuzes		8,2	1,3
het ecosysteem op juiste wijze in stand houden, waarbij alle partijen recht wordt gedaan		7,9	1,2
Bereid te zijn werkprocessen maximaal aan te passen aan de solution, niet andersom (durf op onderdelen techniek te adopteren als toekomstige asset en zet de mogelijkheden centraal, niet de kenmerken van de huidige omgeving waar het in moet landen)		7,8	1,5
veilige en prikkelende innovatie omgeving met een strakke control op de gedefinieerde meerwaarde		7,6	1,3
Coördinatie over de keten - service integratie in een multipolaire wereld		7,6	2,2
de nieuwe business doelen bij schakelen		7,4	1,5
De samenwerking met marktpartijen op basis van echte partnership.		7,3	2,0
Indien equipment ingezet zal worden (bv op missie) begrijp ik dat het over kan gaan van LGI naar HGI. Dit maakt overgang van beheer noodzakelijk van partners naar Defensie. De samenwerking tussen Defensie en de partners om een naadloze overgang te garanderen vraagt de nodige investeringen en vertrouwen		7,1	1,5
Standaardisatie over de keten		7,1	2,4
Zowel infrastructuur als applicaties zullen gelijktijdig ontworpen c.q. uitgerold		7,1	1,9

Onderdeel	-	Gemiddelde van de score	St.dev.
worden. Het zorgen dat er geen onjuiste aannames van de ene hoofdgroep op de andere zijn zal een grote uitdaging geven.			
Flexibiliteit van de leverende partijen op de business behoefte (noodzaak) van deze bijzondere gebruiker tijdens "werk in uitvoering"		6,9	2,2
De juiste balans vinden tussen vernieuwing, beheer en onderhoud.		6,9	2,4
Bepalen en inrichten IT Service Management (People, Process & Technology) naast de bestaande operatie.		6,8	2,1
De wijze van verwerving		6,3	2,2
Het openstaan voor nieuwe mogelijkheden en initiatieven in de markt		6,3	1,9
Gedefinieerde processen, tooling etc. (ontwikkel- en beheerstraten) om voorspelbaar (kwaliteit, tijd, middelen) nieuwe IT te realiseren.		5,7	2,5
Wanneer is het een succes? Hoe definiëren we succes van IT Management?		5,6	2,2
Uitbesteden of zelf beheren of wellicht in een combinatie		5,5	2,2
Change management staat haaks op ad-hoc innovatie		5,5	2,7
Als een applicatie stabiel draait en alles er eigenlijk er al inzit. Hoe zorg je dan dat de kennis opbouw aanwezig blijft? De teams zullen veel minder sprints per jaar hebben wanneer de applicatie is productie is. Advies is om te clusteren in productie en te zorgen dat de kennis kan worden behouden.		5,0	2,3
Is er voldoende kennis in NL beschikbaar?		4,5	2,7
		6,8	2,3

2.1.3

2.1.4 Uitdagingen uitwerken

2.1.4.1 Uitdaging: Cultuur omslag en richten van personeel van Defensie en de Ketenpartner en hun onderlinge samen werking, zorg ervoor dat de deadlines niet de samenwerking in de weg komen te zitten

Meerkeuze optie: Gekozen oplossing

Antwoord
De cultuuromslag is groot, de oplossing is om de ambitie te blijven handhaven maar gezamenlijk ik kleine stappen (menselijke-maat) de veranderingen door te voeren, zorg voor duidelijke (business) resultaten (verhogen van adaptief vermogen). Doe dit samen met de markt en ketenpartners. Investeer in elkaar, laat ook partners initiatief nemen en visa versa. Impact op samenwerking bespreekbaar maken en "verstoringen" duiden op hoog niveau. Dit bestuurlijk ook beleggen! Zorg voor een goede onafhankelijke regie (regie op samenwerking) op deze samenwerking en de bijbehorende knelpunten.

Meerkeuze optie: Voordelen

Antwoord
Voordelen deadlines en samenwerken (en de knelpunten) worden hierdoor ketenproblemen die gezamenlijk opgelost moeten worden, hierdoor kun je de culturele stappen blijven garanderen. De business moet impact van prioriteiten blijven accepteren als een keten-probleem i.p.v. van de traditionele klant leveranciersrelatie (menselijke maat, kleine stappen gezamenlijke keten invulling business in de lead)

2.1.4.2 Uitdaging: Constant stimuleren van cultuurverandering richting agile, innovatief, out of the box, gericht op business value in plaats van IT standaard, geen bloedgroepen meer maar logische keuzes

Meerkeuze optie: Gekozen oplossing

Antwoord
Als eerste dient er een andere manier van verwerven gedaan te worden om een andere (=succesvolle) manier van projecten te realiseren. In plaats van een mantel-overeenkomst voor inhuur te komen tot echte partnership met marktpartijen, bijvoorbeeld door wel langdurige samenwerking met elkaar af te spreken maar ieder kwartaal de doelen voor de komende 3 maanden vast te leggen. Dus samenwerking met marktpartijen op basis van echte partnership ! Verder zien wij als externen een aantal interne muren welke geslecht dienen te worden zodat er ook binnen Defensie echt samengewerkt gaat worden.

Meerkeuze optie: Voordelen

Antwoord
Dit leidt tot snellere resultaten tegen lagere kosten. Door de samenwerking met de marktpartijen is kennisoverdracht en innovatie gewaarborgd. Dit geheel leidt tot implementatie van best practices waardoor kwaliteit verhoogd wordt en blijft.

2.1.4.3 Uitdaging: het ecosysteem op juiste wijze in stand houden, waarbij alle partijen recht wordt gedaan

Meerkeuze optie: Gekozen oplossing

Antwoord
Verkenning van het mini-competative concept zoals bijvoorbeeld in gebruik bij Pro-Rail

2.1.4.4 Uitdaging: Bereid te zijn werkprocessen maximaal aan te passen aan de solution, niet andersom (durf op onderdelen techniek te adopteren als toekomstige asset en zet de mogelijkheden centraal, niet de kenmerken van de huidige omgeving waar het in moet landen)

Meerkeuze optie: Gekozen oplossing

Antwoord

Maak gebruik van kennis uit de markt om dit middels solution mapping en assessments te sturen. Leveranciers van oplossingen hebben hier vaak best practices voor.

Meerkeuze optie: Voordelen

Antwoord

Door de oplossing leidend te laten zijn zal Defensie meer waarde genereren van deze oplossing. Maatwerk wordt voorkomen en Defensie blijft flexibel.

2.1.4.5 Uitdaging: veilige en prikkelende innovatie omgeving met een strakke control op de gedefinieerde meerwaarde

Meerkeuze optie: Gekozen oplossing

Antwoord

Een gedefinieerde meerwaarde wordt van te voren beschreven in een redelijke concrete probleemstelling uit een praktijksituatie. Dit wordt voorgelegd aan het Innovatieve team. Zij worden niet beperkt in oplossingsmogelijkheden.

Van te voren heldere afspraken maken over inzet en eigenaarschap van het eindproduct en/of gebruiksrecht.

Een prikkelende omgeving goed beschreven. Deelnemers moeten een goede beeld kunnen krijgen van de werkelijke situatie. Dat zou via simulatie kunnen. Living Lab.

Meerkeuze optie: Voordelen

Antwoord

Oplossingen krijgen die je niet verwacht maar wel een substantiële verbetering geeft aan de eindgebruikers.

2.1.4.6 Uitdaging: Coördinatie over de keten - service integratie in een multipolaire wereld

Meerkeuze optie: Gekozen oplossing

Antwoord

Opnemen in Contractuele vastlegging - partnerschap bestaat bij de gratie van ruimte geven aan beide (of alle partijen). Zolang alle partijen sturen (via mens, proces en technologie) op de juiste uitkomst en ook zo beloond worden krijgt de gebruiker wat hij/zij zoekt. Aan de andere kant kan er maar 1 partij verantwoordelijk zijn

Meerkeuze optie: Voordelen

Antwoord

Duidelijkheid voorde betrokkenen en focus op uitkomst voor de gebruiker en niet de individuele commerciële belangen

2.1.4.7 Uitdaging: De samenwerking met marktpartijen op basis van echte partnership.

Meerkeuze optie: Gekozen oplossing

Antwoord
Niet een zozeer een dichtgetimmerd contract maar een set van afspraken hoe samen te werken, hoe verschil van inzicht wordt opgelost, en hoe we netjes afscheid van elkaar kunnen nemen. Formuleer een groeipad.

Meerkeuze optie: Voordelen

Antwoord
1. Je selecteert een marktpartner die het aandurft en wil. 2. De relatie moet blijven voor beide partijen wat opleveren (geen lock-ins) 3. Onderscheid te maken tussen een 'veilige' opdracht en risicovolle opdrachten

2.1.4.8 Uitdaging: de nieuwe business doelen bij schakelen

Meerkeuze optie: Gekozen oplossing

Antwoord
Verbindt business en IT. Business krijgt de lead. IT moet de business als klant gaan zien. Moet gaan leren om pro actief vanuit signalen van de business al in te gaan schatten welke veranderende servicevraag er aan komt. Kan via intelligence (data, servicesystemen, etc.) , kan via relatiemanagement, kan door regie. Strategisch planningsproces gezamenlijk inrichten. Gevolg: IT is niet meer reactief, en dus te laat, maar deel van de business. En IT wordt niet meer gezien als rigide (kan alleen maar zoals IT vindt dat het moet). Business owners over iT aanstellen zodat er een match is tussen vraag en aanbod. IT moet value to business gaan leveren, dit is een gezamenlijke verantwoordelijkheid, en een gezamenlijke investeringsagenda.

Meerkeuze optie: Voordelen

Antwoord
Wederzijdse duidelijkheid tussen Business en IT over portfolio, time to value, innovatie, verantwoordelijkheden. Je krijgt een IT die mee kan bewegen met de business. Zeker naar de toekomst toe (snelle veranderingen) is dit een KSF. En IT wordt niet meer verrast door plotselinge business vragen. Er ontstaat transparantie in de prestaties van IT.

2.2 Verantwoordelijkheden

2.2.1 Hoe ziet u (idealiter) de verdeling van verantwoordelijkheden van het IT-Management in de exploitatiefase

Meerkeuze optie: Verantwoordelijkheid Defensie

Antwoord
Het HR-management van de Eigen ingezette medewerkers in IT-management
Input voor innovatie
Voorzien in adequate en tijdige besluitvorming gerelateerd aan acceptatie van (deel)oplossingen (zie principes van professioneel opdrachtgeverschap)
Demand Management
Insourcen dan wel ondersteunen en onderhouden
IT Financial Management
flexibiliteit
De mogelijkheid in stand houden zaken terug te nemen wanneer de omstandigheden dat vragen
Besluiten tot uitfaseren en in gebruik nemen toepassingen
Project Portfolio Management
Lessons learned te delen, geode en minder goede
Ontwikkelen van (een gepaste set) stuurinstrumenten en deze inzetten op het moment dat een marktpartij haar afspraken niet nakomt
Nieuwe en innovatieve oplossingen inbrengen
Service lifecycle management
relatie op basis van Trust en Control inrichten
innoveren en men komt tot een nieuw verantwoordelijkheid model
Service Integration en Governance
Doorbelasten aan afnemers binnen Defensie
Service leveren en onderhouden en rapporteren (binnen de samenwerking en de SLA), aangeven van continue verbeteringen
contractbeheer
Het functioneel managen van het MinDef Inkoopproces
Bewaken van de gekozen standaardisatie en bewaken dat er geen vormen van shadow IT gaan optreden gebaseerd op historische belangen
kwaliteit en inzet eigen personeel
Goede uitvraag (als het onduidelijk is, nodig voor cultuuromslag en vertrouwen
Openstaan voor nieuwe ideeën, andere oplossingen
security
zorgen voor win win.
Integraal (data) beheer van de repositories t.b.v. applicatie, service en infrastructuur portfolio management. Operationeel door marktpartijen te gebruiken en actueel te houden.
Creëren, leveren en beheren van omstandigheden die de markt nodig heeft voor het leveren en beheren van all-in solutions
Openstaan voor veranderingen en nieuwe marktontwikkelingen
creëren van samenwerkingsplatform
Sturend op veranderagenda (service strategie en architectuur)
Coördinerend op project exploitatie en eind verantwoordelijk voor business verandering

Antwoord
Regisserend op service management en integratie
servicelevel bepalen
relateren aan opdrachten en beslissingen
Innovatie inbrengen
aligned houden van thema's, doelstellingen, eisen
Verantwoordelijkheid over de kwaliteit (put your money where your mouth is)
regie
Bereid zijn partnership met marktpartijen aan te gaan
Integraal incidentmanagement
Hoewel Security Management naar mijn mening onder verantwoordelijkheid van Defensie moet vallen kunnen onderdelen (bv SOC) gedelegeerd worden naar de Markt
Behoeftestelling richting markt.
Goed opdrachtgeverschap met duidelijke verantwoordelijkheden
Basisregistratie
Kiezen van de uit te werken innovatie
expliciteren van ambitie
Integraal changemanagement
Effectief en efficiënt uitvoeren van opgedragen taken
Uitbesteden of zelf beheren
Veranderingen in Integrale planning (impact en uitvoering) gerelateerd aan Politiek en bestuur
regie
Goede verankering van plannen en beleid in de MinDef begroting
beveiliging
functionaliteit
business eisen
Security
geld
Business/IT alignment
Event Management Information Security Management IT Service Continuity Management Release and Deployment Management
aanbieden van innovatieruimte aan markt, business en IT
voldoende expertise ook over de defensie processen
prioriteiten
Business Relationschip Management Change Evaluation Demand Management Design Coordination Financial Management Service Portfolio Management Service Validation and Testing Strategy Management for IT Services Transition Planning and Support
Functionaliteit

Antwoord
Leveren van omstandigheden en beheer van de omgeving waarin een oplossingen aan de leverancier landt (zie principes van professioneel opdrachtgeverschap)
portfoliomanagement
Prioriteitstelling
Infrastructuurbeheer bij operationeel optreden (?). Kan/mag markt dit?
snelle besluitvorming
Change management
Business Impact
Functionaliteit
Security
Beschikbaar stellen van productowners die kennis hebben van de werkprocessen
Eisen stellen en beheren (zie principes van professioneel opdrachtgeverschap)
Professionele Opdrachtgeverschap met voldoende Ervaring, kennis en capaciteit.
input release management.
security beleid
functioneel applicatiebeheer

Meerkeuze optie: Verantwoordelijkheid Markt

Antwoord
Maatregelen om gedefinieerd risico's met verantwoordelijkheid voor resultaat het hoofd te kunnen bieden
vernieuwing
Consulterend service strategie en architectuur Faciliterend in verandermanagement waarbij voor een gedekte verantwoordelijk voor realisatie Eindeverantwoordelijk bij service levering en management
transparante rapportages van geleverde services en inspanning
openstaan voor nieuwe samenwerkingsvormen
Leveren metrics voor sturing
Gezamenlijk verantwoordelijkheid te dragen
Opleveren van impact analyses bij voorgenomen wijzigingen
Bereid zijn partnership met Defensie aan te gaan
innovatie
Een gezonde businesscase
kwaliteit en inzet eigen personeel
MinDef spiegelen op haar aanpak, sturing, doelen, kennis en competenties, etc. vanuit de relatiegedachte
strategische partner zijn. Dat betekent dat er relaties zijn op verschillende niveaus. Escalatie niveaus van te voren inregelen wanneer besluitvorming op lager niveau vast loopt.
selectie partners
Deeloplossingen turnkey aanleveren (waar het kan/mag)
Kwalitatief hoogwaardige producten
Integraal functionerende oplossing, als all-in solution
oplossing
Nieuwe ideeën aandragen voor oude problemen die elders al succesvol zijn opgelost
technologie
Opleveren op basis SLA
Access Management

Antwoord
Availability Management Knowledge Management Service Asset and Configuration Management Service Introduction Supplier Management
Capaciteit leveren (handjes)
innovatie
Exploitatie en beheer van de ontwikkelstraten
Continue kunnen leveren
Capacity Management Request Fulfillment Service Catalogue Management Service Level Management
Innovatiekracht leveren
Change Management Incident Management Problem Management
Inbreng kennis en ervaring
Technisch applicatiebeheer, derde (tweede?) lijns helpdesk, implementeren nieuwe releases.
Proactieve verbeter voorstellen

3 Businesscase

3.1 Welke elementen zijn volgens u van grote invloed op de kosten bij de realisatie van de groeikern?

U kunt algemene zaken benoemen, maar ook specifieke. Selecteer dan a.u.b. eerste het desbetreffende onderdeel

Meerkeuze optie: Algemeen

Antwoord
Als u vraagt naar 'costdrivers' waarom dan niet naar 'benefitdrivers'? Immers, een businesscase begint niet met kosten, maar met gewenste baten. Kosten zijn in eerste aanleg relatief en volgen als consequentie van de baten. Als je vooruit wil als defensie is het de vraag waarom je niet stelt; "we sturen altijd op de baten, de kosten mogen zo hoog zijn als nodig is, zolang het maar een bepaald verhouding kent tot de baten". Nu is de kans groot dat er zodanig op financiën wordt gestuurd dat innovaties en maatregelen die 'veel geld' kosten het loodje leggen, terwijl diegene waar minder aan wordt uitgegeven mogelijk heel 'duur' zijn omdat de kosten hoger zijn dan de baten, wel doorgang vinden. Oftewel; veel geld / hoge kosten moet niet het criterium zijn, wel de relatieve kosten t.o.v. de baten. Hiermee geef en partners de ruimte om innovatief te zijn en hun nek uit te steken, anders word je geconfronteerd met een markt die alleen maar de eerder gemaakte kosten wil terugverdienen.
Ontwerp vraagt om inzet van bleeding edge technologie.
Vasthouden aan onhaalbare of moeilijk haalbare deadlines.
Het ontbreken van pragmatische keuzes en te veel vasthouden aan de uitgangspunten in het IT ontwerp, waardoor onnodig generieke oplossingen gerealiseerd moeten worden. Voorbeeld: één werkplek voor alle soorten gerubriceerde informatieve in alle omstandigheden (SOMUT).
Te kiezen doel technologieën
De maten waarin de extreme grenzen waarin Defensie opereert (zeker in het veld) zullen terugkomen in de gedetailleerde eisen op enig moment, denk bijv. aan connectivity
de meegegeven scope
koppelingen tussen generieke en specifieke ICT
nadruk die wordt gelegd op focus en alleen dat doen wat nodig is
Doorlooptijden van beslissingen aan defensie zijde versus het bekende leegloop effect bij de partners (ook de mate van agile)
benodigde schaalbaarheid en flexibiliteit
Algemeen: het niet sturen op het incasseren van de beoogde baten. Per batengebied uit de businesscase een business verantwoordelijke aanwijzen.
Gaat defensie voor 'goed is goed genoeg' of voor ultra modern, bleeding edge
Het ontbreken van een strategie voor het daadwerkelijk uitzetten van bestaande voorzieningen.
Hoeveel Defensie zelf kan en wil bijdragen aan de realisatie - geheel zonder Defensie kunnen de marktpartijen het ook niet realiseren....
Het niet willen/kunnen standaardiseren van infrastructuur en toepassingen over alle Defensie onderdelen, leidend tot alle vormen van maatwerk.
Gebrek aan standaardisatie
flexibiliteit in combinatie met hoge kwaliteit
het al dan niet overnemen/in samenwerking realiseren van de benodigde functionaliteit
De snelheid van besluitvorming
Alle risico's komen voort uit (een combinatie van) onzekerheden en complexiteiten; dat wil zeggen een tekort aan informatie, resp. een overload aan informatie. Hiervoor is eerder op Europese schaal met ISPL een zeer bruikbaar onderzoek gedaan dat heeft geleid tot een best-practice op het gebied van onzekerheden en complexiteiten die (soms in combinatie) zijn gelinkt aan hele specifieke risico's. Dit overzicht van risico's (en

Antwoord
achterliggende onzekerheden en complexiteiten) is een bijzonder bruikbare basis voor het redelijk sluitend definiëren van costdrivers.
Over specificeren
gebruik bleeding edge technologie
De scope van de groeikern zoals die uiteindelijk neergezet moet worden - is nog onvoldoende duidelijk
Omscholing/bijscholing/aannemen en laten afvloeien van bestaande IT medewerkers.
de mate waarin defensie voorop wil lopen
Transitiebesturing - snel en bewegelijk met mandaat i.p.v. bureaucratisch en traag met versplinterde besluitvorming
Inwerk periode
Snelheid van besluitvorming
snelheid van realisatie
24/7 beschikbaarheid
Incorrecte aannames van deelnemers van de implementatie, over-sell en underperform van markt en ketenpartners (pas haalbare ambitie toe!)
Alles wat met migratie van en tijdelijke voorzieningen op de bestaande IT te maken heeft
Financieringsmodel - afwenteling capex t.b.v. opex
Planning invoering in combinatie met bestuurlijke besluiten/ continuïteit. Langzame besluiten, verlate besluiten, geen aandacht, geen prioriteit, alleen sturen op eindresultaat
mate waarin standaarden acceptabel zijn op basis van beschikbare technologie
unieke functionaliteit voor defensie (maatwerk)
(vormgeving van) samenwerking tussen partners en defensie
Dingen kunnen misgaan/mislukken
Kosten voor het verwerven van knowhow.
beveiligingseisen
De wijze van verwerving
Onduidelijke sturing van functionele scope. Niet richten van de vraag
voor regie (SPOT) BOP
besluitvorming en afstemming

Meerkeuze optie: IT Infrastructuur

Antwoord
Vast kunnen houden aan ambitie om kracht van de markt Optimaal te benutten- Mate van vrijheid te geven aan de markt om binnen kaders oplossingen te bieden
robustheidseisen (klimaat, schade door gebruik, etc.)
Het koppelen van hybride infrastructuren
werk vanuit het principe van schaalbaarheid
Standaardisatie waar mogelijk verkort de realisatieperiode
te veel zelf doen door MinDef
Continuïteit gekoppeld aan flexibiliteit is duurder dan alleen focus op continuïteit (huidig) of focus op flexibiliteit (markt)
Mate van openheid t.o.v. cloudoplossingen
Richtlijnen op standaardisatie
RPO/RTO eisen
Complexiteit en samenhang met Toepassingen, applicatie rationalisatie en de sturing hierop
de benodigde uitvoering van de infrastructuur vanuit de taken van defensie

Antwoord
Een infrastructuur voor heel Defensie
Future proof en adaptief zijn voor nieuwe toepassingen
Aantal systemen, service levels, continuiteit eisen
Het percentage defensiespecifieke inrichting
zowel oude als nieuwe omgeving in de lucht. zorg dat de periode zo klein mogelijk is.
Volledige vernieuwing van infrastructuur en datacenters
Hardware & Software

Meerkeuze optie: IT Beveiliging

Antwoord
Het koppelen van hybride infrastructuren
De stevige eisen die Defensie stelt zullen marktpartijen voor extra kosten plaatsen t.o.v. hun standaard producten of skills.
Niet compatible zijn met NATO en EU standaarden: indeling in LGI/HGI wijkt af.
Cyber security is essentieel voor het voorkomen van dure risico's. Ga dichter op de werkelijkheid analyseren en sturen. Richt daar een logisch en efficiënt instrumentarium voor in
Visie t.o.v. offensieve t.o.v. preventieve beveiliging
Remmende factor als de implicaties niet smart gemaakt kunnen worden, sentiment bij bestuur en management kunnen remmend werken.
Beveiliging moet dienend zijn en geen extra belemmering
de noodzakelijke eisen die defensie stelt aan beveiliging
Levertijd van crypto boxen etc. kunnen zorgen voor vertraging en dus extra kosten

Meerkeuze optie: IT Toepassingen

Antwoord
Waardegedreven ondersteuning versus lage dagelijkse rates
Voorkom grote rigide projecten, zoek naar herbruikbaarheid en flexibiliteit.
Betrek markt adequaat voor binnenhalen innovatieve impulsen
Zorg voor actueel kennis en competentie niveau
Toepassingen worden niet vanuit de business value, maar vanuit IT driven gerealiseerd. Risico dat geld wordt besteed aan services die niemand gaat gebruiken is daarmee groot
Modernisatie technologieën om levensduur functionaliteit te verlengen
Richtlijnen m.b.t. rationalisatie - bijv. Kan 1 oplossing over alle defensie onderdelen daadwerkelijk worden afgedwongen
Openstaan voor nieuwe methodieken, best practices en bestaande frameworks
Standaardisatie, rationalisatie en haalbaarheid. Werkelijke drive om ook de Kill toe te passen! Durven werken met standaarden en loslaten van maatwerk als deze GEEN bewijsbare toegevoegde waarde heeft voor de ketens!
Durf ten alle tijden de stekker uit een initiatief te trekken. Daarbij helt het enorm wanneer voor een agile aanpak wordt gekozen. De roll back period is dan relatief kort, en de (budgettaire) schade ook relatief beperkt
universele inzet van de toepassing zullen reduceren kosten
Het aanpassen van COTS/NOTS producten naar 'Defensie-geschikt'
Maatwerk kost meer dan een standaard oplossing

Meerkeuze optie: IT Management

Antwoord
Het laten samenwerken van meerdere partijen met hun eigen tooling en processen.
Werk vanuit architectuur, maar maak er geen religie van
Optimalisatie governance over alle defensie onderdelen en marktpartijen
Durf door te vragen op doelen, doelstellingen. Definieer meetbare KPI's en stuur er ook op
Inzet tooling ter vervanging van handmatige processen
Standaardisatieregie processen en overdrachtsmomenten
Betrek de business consequent om mismatch van vraag en aanbod te voorkomen
SM cultuur (en ik bedoel geen Service Management), we moeten het toch doen... als we het niet doen krijgen we toch bovenlangs te horen dat het moet..... Anders durven en werkelijk doen, communiceren in business-impact i.p.v. IT doelstellingen, haak aan bij de opdrachtgevers zowel defensie als ketenpartners. Zorg voor een werkende samenwerking (en investeer allen hierin)
Outsourcen of zelf doen
Creatie PAAS en IAAS laag t.b.v. Dev-Ops
Werk op alle niveaus met dezelfde (near) real time data waar het gaat om sturing, rapportage en besluitvorming. Iedereen praat over hetzelfde. Dit voorkomt mismanagement en dure fouten
doorlooptijd voor besluitvorming
open standaarden kunnen kosten reduceren
Het invoeren van de regie-organisatie met de juiste skills.
Onjuiste tooling en rapportage in meerdere systemen. Zorg dat alles in een systeem staat. Een waarheid wat de werkelijke planning is.
De benodigde standaardisatie van de IT-processen, werkwijzen en tooling (IT4IT / "ERP" voor IT organisatie)
Nieuwe opzet processen en tooling versus (hergebruik) bestaande

3.2 Welke elementen zijn volgens u van grote invloed op de kosten bij de exploitatie van DoIT?

U kunt algemene zaken benoemen, maar ook specifieke. Selecteer dan a.u.b. eerste het desbetreffende onderdeel

Meerkeuze optie: Algemeen

Antwoord
Zelfde type elementen als bij vorige vraag
De mate waarin de mensen op de werkvloer voorbereid zijn op de verandering in processen, middelen, software, etc. - denk aan opleiding/voorlichting gehad hebben
Verslappen van de aandacht voor gekozen uitgangspunten. Risico op terugval naar oude gedrag
De mate waarin de mensen op de werkvloer de vernieuwing geaccepteerd hebben als een vooruitgang - succes van verandermanagement
Capaciteit nodig bovenop de bestaande organisatie als effect van Bimodaal IT.
Het aantal uitzonderingen dat toegestaan wordt c.q. de impact daarvan
Educatie. Zorgwekkend matig niveau in de markt. Wat pricing omhoog stuwt.
De mate van standaardisatie die Defensie met haar partners wist te bereiken in de realisatie fase
de mate waarin de transitie slaagt m.n. op het gebied van organisatie, mensen en cultuur
tijdsframe van bedreigingen (global) die steeds smaller wordt. hoe wordt dit opgevangen om aansluiting en continuïteit te garanderen!
Geen duidelijke afspraken over delen van winst en gerelateerde inzet
Mensen, die blijven hangen in oude werkwijzen en processen en procedures.
Sterkte van de operationele integrator-rol
Het toestaan van maatwerkoplossingen in de breedste zin van het woord
Outsourcen of zelf doen
Grootte van de retained organisatie
Aantal wijzigingen per tijdseenheid
Als het einddoel is bereikt, is de verwachting dat de exploitatie kosten aanzienlijk zullen dalen. SecDevOps teams kunnen veel sneller dan via een waterval overeenstemming over de eisen bereiken en deze ook parallel realiseren.
Politieke invloed in breedste zin des woords
cultuur change.
Snelheid en adoptief vermogen organisatie

Meerkeuze optie: IT Infrastructuur

Antwoord
de benodigde opzet van de infrastructuur i.r.t. de defensie taken
Vasthouden aan oude omgevingen, geen afscheid durven nemen
Hoe hoog dient de beschikbaarheid/ redundantie te zijn
Uitwijk inregelen. Afhankelijk van scope. Eigen satcom verbindingen op veel locaties kan tot veel meer kosten leiden.
Grootte en hoeveelheid van systemen, Service Levels

Meerkeuze optie: IT Beveiliging

Antwoord
Ecosysteem up to date houden t.b.v. toegang marktpartijen
Dat beveiliging een doel op zich kan worden
Samenwerking tussen de Defensie onderdelen
Fysieke of digitale beveiliging
In exploitatie is dit goed ingeregeld inclusief een eigen DefSOC. Zal afhankelijk zijn van de Cyberaanvallen.

Meerkeuze optie: IT Toepassingen

Antwoord
ook bij lage netwerk beschikbaarheid een optimale applicatie beschikbaarheid op locatie leveren
de mate waarin het lukt om hier tot flexibele, schaalbare contractvormen te komen
Geen kill in applicatie rationalisatie, omdat de business toch geen afscheid wil nemen, dubbele investeringen oud en nieuw
de makkelijke en snelle integratie van verschillende koppelingen dus geen black box
Minder toepassingen en meer standaardtoepassingen kan de kosten verlagen.

Meerkeuze optie: IT Management

Antwoord
de mate waarin een actuele afstemming op effecten en eisen kan worden geborgd
Niet de juiste skills om de veranderingen tot stand te kunnen brengen, geen voorbeeld gedrag en echt leiderschap over de veranderingen. Terugval in oude gewoontes (niet samenwerken maar klant leverancier spel)
Hoeveelheid partners per deelgebied (bv voor infrastructuur, per applicatie etc.), scherpte van de grenzen

4 Security

4.1 Waar ziet u nu de grootste beperkingen bij de samenwerking die voortkomen uit de gestelde beveiligingseisen.

Antwoord
agile en devops bestaan bij de gratie van fouten kunnen maken - veiligheidseisen kunnen daarmee conflicteren
het werken met data van verschillende classificatieniveaus
Nieuwe mogelijkheden zijn wellicht niet eenduidig benoemd. Dan moet eerst de BA er wat van vinden.
Integrale plaatje over de vele systemen, services, processen en mensen heen. en dan (near) real time
cultuur defensie (hiërarchie, kleding, houding en gedrag) staat haaks op cultuur ICT ontwikkelaars (autonomie, uitspreken mening, kleding, etc.)
Conflicterende eisen: bijvoorbeeld 'zero footprint' bij operationele inzet.
procedures en rigiditeit daarvan
adequaat managen van autorisaties en authenticatie op bv veranderende rollen
Data kan in verschillende situatie verschillende rubricering kennen - hoe hiermee op te gaan i.s.m. met de markt
Security is een gegeven en daarmee randvoorwaardelijk aan de samenwerking
Voor samenwerken en innoveren is veel inzicht in defensieprocessen nodig, niet iedereen kan dat inzicht krijgen en dus mee-innoveren
zorgen dat screeningstrajecten van in te zetten marktpartijen sneller verloopt dan nu.
hoe dicht zit je met security analyse op de brondata. Zo weinig mogelijk aggregeren
de goede balans vinden tussen afscherming van gegevens en beschikbaar stellen van gegevens t.b.v. samenwerking
Het evenwicht tussen preventieve en detectieve maatregelen
Continuïteit van "gevalideerde" externe personen
Juridisch: aansprakelijkheid bij vervolgschade, bijvoorbeeld in operatieën
Beveiliging dient ten dienste te zijn i.p.v. Beperkingen op te leggen.
Lage netwerkcapaciteit en beperkte bereikbaarheid, legt bijvoorbeeld zijn beperking op aan monitoring- en detectieoplossingen die in netwerken met een vaste infrastructuur soms al uitdagend genoeg zijn
IP samen vastleggen en beveiligingseisen gaan niet hand in hand
het samenwerken tussen personen met een verschillend informatieprofiel (delen van informatie kan/mag niet)
Samenwerking en Beveiligingseisen gaan niet altijd hand in hand
Data rubricering en uitbestede IT diensten (bijv. Werkplek) zullen soms conflicteren
De interne bereidheid om samen te werken
mogelijkheid tot delen van kennis
Voorbereiding
de mens centraal
maintenance en innovatie
Beperking inzet (snelheid) van innovatie door screeningseisen
Pragmatisch denken
Flexibiliteit
Innovatie en inzicht in mogelijkheden binnen defensie

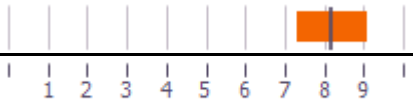
5 Evaluatie

5.1 Wat heeft u in de sessie niet kunnen inbrengen?

Antwoord
Soms worden vragen te binair gesteld. Laat ook ruimte voor nuance
de overgang van heden naar de IT van de toekomst. hoe worden de verschillende teams in en uitgefaseerd
doorlooptijd in combinatie met vakantie komt kwaliteit niet ten goede
Nuance en begrip van andermans punten
niets
Eind deze week zal blijken wat het ook ons (de leveranciers) oplevert :)
Alles, maar mis wel wat interactie met de deelnemers
niets specifiek

5.2 Wat vond u van deze sessie?

Invuladvies: Geef een score tussen 1 en 10, waarbij:
1 = geen goede sessie
10 = hele goede sessie
Sessie IT management

Onderdeel	-	Gemiddelde van de score	St.dev.
Sessie IT management		8,2	0,9
		8,2	0,9

5.3 Welke tips, suggesties of opmerkingen heeft u voor ons of kunt u ons meegeven?

Antwoord
Goed concept
Systeem vooraf introduceren, snellere start
na bijv. eerste ronde kleine workshops vanuit de kennisgebieden om input te geven op aanvullende of ontbrekende gegevens
Meer interactie om eenzijdigheid insteek partijen te challengen en daarmee samenhang te creëren. Dit waardevolle initiatief zou ook kunnen fungeren als verander management voor partijen onderling
Iets uitgebreidere voorbereiding/voorlichting van de sessies richting leveranciers.
Vooraankondigen van de vragen (beter kunnen voorbereiden op de sessie)
het getuigd van durf
verbeter de spilter ICT, werkte niet altijd goed op mijn macbook. meer tijd inplannen voor onderlinge afstemming
kennis gebieden van de partners door middel van vragen meer groeperen gedurende de sessie en vandaar uit kennisvragen aanscherpen.
gezien het doel van de sessie geen opmerkingen
Ik zou markt nog steviger uitdagen om per item/domein meer inhoudelijke mensen te sturen

Antwoord
Meer voorbereidingstijd op de vragen, snelheid ligt nu erg hoog
Combineren met een interactie met de deelnemer iets wellicht meer gefocuste onderwerpen waardoor je en kort kunt spreken en kunt scoren
-Een voorbereiding op de vragen
goed georganiseerd en zeer effectief om in korte termijn de antwoorden en prioriteiten van 16 man samen te voegen. Is voor herhaling vatbaar.
Ik zou het volgende keer specifieker maken. Nu soms te generiek, of te veel theorie om op te reageren.
Goede sessie
Een globaal idee van de vragen, aangezien de aangeleverde documentatie dusdaning breed is dat het lastig is over alle onderwerpen door te denken in zo'n korte termijn