Een rapport voor

Ministerie van Defensie

Second Opinion HLO - Samenwerking met de markt

24 april 2015
Engagement: 330022653

Gartner

Inhoudsopgave

1.0 Inleiding 6
1.1 Achtergrond 6
1.2 Doel 6
1.3 Scope 8
1.4 Doelgroep 8
2.0 Analyse high-level ontwerp 9
2.1 Business effecten 9
2.2 ICT Infrastructuur 12
2.3 IT Toepassingen 15
2.3.1 Applicatierationalisering 15
2.3.2 Specifieke vragen t.a.v. IT Toepassingen 16
2.3.3 Overige vragen 16
3.0 Analyse samenwerking met de markt 18
4.0 Risico's 21
4.1 Samenwerken met de markt 21
4.2 Aligneren met de business 21
4.3 Regie-organisatie 21
5.0 High-level financiële analyse 23
6.0 Aanbevelingen 24
6.1 Strategie & Architectuur 24
6.2 Samenwerking met de markt en regievoering 25
6.3 Innovatie en organisatorische inrichting: Bi-modal IT 26
6.4 Applicatierationalisatie en -transitie 27
6.5 Financiele consequenties 28
Bijlage A: Analyse principes IT-infrastructuur 31
Principes Data Center 31
Principes Werkplek 32
Principes Devices 33
Principes Netwerk 33
Principes Telecommunicatie 34
Principes Beheer 34
Principes Beveiliging 35
Bijlage B: Analyse principes IT-toepassingen 36
Bijlage C: Referenties naar de vraagstellingen 41

Gartner

Managementsamenvatting

Managementsamenvatting

In de periode maart / april 2015 heeft Gartner in opdracht van Defensie een onafhankelijke ‘second opinion’ uitgevoerd naar het High Level Ontwerp (hierna: HLO) en de Herijking Sourcing (hierna: HS). Doelstelling van de ‘second opinion’ betrof het beantwoorden van de vraag of de uitdagingen waaraan Defensie de komende periode gesteld is worden aangepakt en ingevuld door de strategische richting zoals vastgelegd in het HLO. Het HLO moet richting geven aan een herijking en inrichting van het projectportfolio Defensie IT infrastructuur. IT technologie is onderhevig aan (ver)snelde veranderingen en daarom wil Defensie kort-cyclisch en incrementeel innoveren. De strategische intentie zoals vastgelegd in het HLO zal in verdere verdiepingsstappen (plateaus) op basis van een door het HLO gekaderd projectenportfolio worden uitgewerkt en uitgevoerd in de zogenaamde uitvoeringsfase.

Opgemerkt dient te worden dat naast het uitvoeren van de ‘second opinion’ Gartner enkele aanbevelingen heeft opgesteld die uitsluitend betrekking hebben op de **uitvoeringsfase** zijnde de fase volgend op de instemming met de in het HLO beschreven strategische intentie.

Analyse HLO

Tijdens de uitvoering van de onafhankelijke ‘second opinion’ heeft Gartner vastgesteld dat met het vaststellen van de strategische intentie zoals vastgelegd in het HLO Defensie de haar gestelde uitdagingen adresseert. Het HLO geeft richting aan de gewenste uitvoering en realisatie van de gestelde ambitie om Defensie te voorzien van een betrouwbare, continue en (be)veilig(d)e IT dienstverlening, waarbij er gecontroleerd ruimte is voor het verder innoveren van de IT-dienstverlening aan de hand van de met de business afgestemde dienstverleningsbehoeften. Waar nodig maakt Defensie hiervoor gebruik van kennis en vakmanschap uit de markt door het aangaan van strategisch samenwerkingsverbanden met de markt.

Gartner stelt als hoofdconclusie dat het HLO als richtinggevend document aansluit bij de doelstellingen van Defensie en als strategische intentie aansluit bij in de markt geobserveerde bewegingen. Daar waar mogelijk zijn voor nu ook al *best practices* meegegeven binnen de kaders van het HLO, te denken is hier aan onder meer het kort-cyclisch aanpakken en verbeteren van de huidige situatie en het incrementeel toewerken naar de in het HLO vastgelegde ambitie.

Gartner heeft in de uitvoering van de ‘second opinion’ vastgesteld dat ingegeven door het ambitieniveau van Defensie een incrementele aanpak de enige juiste manier is om een gecontroleerde realisatie van de doelstellingen (de business-effecten) mogelijk te maken. Dit betekent echter wel dat met het oog op de gewenste gelijktijdige toename van innovatie Defensie in twee verschillende ‘modus operandi’ zich dient te organiseren. Een deel van de organisatie richt zich op het bieden van continuïteit en stabiliteit in de IT-dienstverlening, terwijl gelijktijdig het andere deel zich richt op het door middel van kort-cyclische innovatie en flexibiliteit aanbieden van nieuwe (vormen van) IT-dienstverlening.

Gartner heeft tevens vastgesteld dat het HLO voldoende mate van flexibiliteit biedt om in de komende jaren waar nodig en gewenst (onder meer door zich veranderende technologische mogelijkheden en / of business eisen) wijzigingen te absorberen. Dit vraagt wel dat er een gedegen portfolioproces is dat alle verschillende bewegingen genoemd in het HLO in zich heeft en dat er tevens voldoende kaderstellende principes zijn vastgelegd die op een verdergaand detailniveau toetsend kunnen zijn voor het opstellen van het benodigde en beoogde portfolio (zowel project- en programmaportfolio als ook het uiteindelijke dienstverleningsportfolio). Het HLO voorziet nu niet in deze kaderstellende principes.

Op basis van marktervaringen en Gartner eigen ervaring bij het ondersteunen van organisaties in het rationaliseren van het applicatieportfolio, adviseert Gartner Defensie om een andere zienswijze (en daaraan verbonden kengetallen) te hanteren voor wat betreft het opschonen van het huidige applicatieportfolio. De focus dient daarbij te liggen op verlaging van TCO-kosten en het versnelt kunnen realiseren van nieuwe functionaliteit.

Gartner adviseert dat in de voorliggende periode waarin een verdere detailuitwerking van het HLO plaatsvindt een verdere eenduidige vastlegging van de kaderstellende principes wordt uitgevoerd. Tevens adviseert Gartner Defensie om de recent vastgelegde business effecten verder (in meer detail en verbijzondering) uit te werken tijdens de genoemde uitvoeringsfase omdat deze nu nog onvoldoende gebruikt kunnen worden als richtinggevende parameters voor het evalueren en opstellen van het projectenportfolio. Gartner ziet als een belangrijk verbeterpunt hierin de uitwerking en het contextualiseren van de verschillende *business capabilities* om verdere definitie van kaders en leidende principes mogelijk te maken.

Analyse 'Samenwerking met de markt'

Ten aanzien van het aspect Sourcing concludeert Gartner dat de high-level verkaveling binnen de sourcingdocumentatie (dit betreft zowel de Herijking Sourcing als de daaropvolgend opgestelde nota) een opdeling van dienstverleningen laat zien die grotendeels in lijn is met de markt. Defensie kiest daarbij voor meerdere strategische partners (*best of breed*). De keuze voor meerdere strategische partners (*best of breed*) wordt door Gartner gezien als de juiste te hanteren strategie om te borgen dat de verschillende *business capabilities* ondersteund kunnen worden. De huidige documentatie mist in deze context een nadere uitwerking op aspecten als de uitwerking van de verschillende *service bundles*, het delivery model, commerciële richtlijnen, borging van het competitieve element en life-cycle management. Defensie moet in deze fase de strategie nader uitwerken alvorens kan worden overgegaan tot aanbesteding van de verschillende dienstverleningen.

Gartner onderschrijft verder de aanpak om de samenwerking met de markt gefaseerd en in behapbare delen te realiseren. Een belangrijke reden hiervoor is ook het geleidelijk opbouwen van de regiecompetentie binnen Defensie. Het voorgestelde samenwerkingsmodel en de constatering dat Defensie altijd IT activiteiten onder eigen verantwoordelijkheid uitvoert vanwege haar unieke primaire taakstelling sluit aan bij de gestelde ambities benoemd in het HLO.

Gartner adviseert Defensie met klem wel om aanvullende nuancering aan te brengen in de verschillende sub-domeinen op basis van specifieke *business capabilities* of technologie-expertise en ook ten aanzien van het onderscheid tussen continuïteit en innovatie. Dit dient echter een belangrijke parameter zijn voor het verder opdelen van de dienstverleningen richting specifieke leveranciers voornamelijk op het gebied van IT Toepassingen

Scenarioanalyse en verwachte doorlooptijd

Als onderdeel van de uitgevoerde 'second opinion' is door Gartner een aanvullende analyse uitgevoerd waarbij is ingegaan op vraagstellingen ten aanzien van verwachte doorlooptijd voor het realiseren van de strategische intentie zoals omschreven in het HLO. Daarnaast heeft Gartner ook een eerste aanzet herleid om te komen tot een 'wenkend perspectief'; hierbij is aan de hand van trendverwachtingen en verdere marktobservaties invulling gegeven aan de mogelijke effecten van het gaan uitvoeren en realiseren van de HLO-ambitie afgezet tegen een *Do Nothing* – scenario.

Gartner verwacht op basis van marktobservaties en recent door Gartner uitgevoerde vergelijkbare studies en audits dat de met het HLO ingezette beweging een minimaal te verwachten doorlooptijd kent van vijf jaar. Aanvullend daaraan concludeert Gartner dat het

Do Nothing – scenario geen werkelijk te overwegen optie is voor Defensie gezien het hoge risicoprofiel (de continuïteit van de huidige dienstverlening komt binnen drie tot vijf jaar ernstig in het gedrang) en innovatie is benodigd om aan te sluiten op (markt)ontwikkelingen. Daarnaast zorg het scenario *Do Nothing* ervoor dat de beheerinspanning de komende jaren toeneemt waardoor er meer van het IT budget geconsumeerd wordt aan het 'in de lucht houden' van de bestaande IT-dienstverlening. Dit leidt vervolgens tot het onder druk zetten van het innovatief-'vermogen'. Het HLO biedt de flexibiliteit om stapsgewijs de gewenste verandering door te zetten op een gekozen tempo dat past bij de financiële ruimte en prioriteiten van Defensie. Echter het langdurig uitstellen van transitie en vernieuwing zal op termijn leiden tot operationele risico's. Het tempo zal daarom bepaald moeten worden door de mate van risico-acceptatie in relatie met de financiële overwegingen.

Vervolgstappen

Onderstaande opsomming geeft een overzicht van de meest urgente vervolgstappen t.a.v. de uitvoeringsfase die Gartner voorziet in deze strategische fase:

- Definiëren van de business en IT doelstellingen (specifiek, tijdsgebonden, etc.) en de vertaling richting een high-level plateauplanning (fasering) die is afgestemd met de verschillende Defensie-onderdelen.
- Detailuitwerking van het HLO om het kaderstellende karakter van het document te borgen en beter aan te sluiten op de verschillende *business capabilities* binnen Defensie
- Opstellen van een kostencalculatiemodel voor de voorziene transitie gedurende periode 2015-2020. Hierbij moet onder andere rekening worden gehouden met de transitie- en transitiekosten, gedeeltelijke dubbele beheerlast, kosten t.a.v. regievoering en toegenomen investeringen voor vernieuwing en innovatie. Het kostencalculatiemodel moet meerdere scenario's uitwerken (b.v. Do Nothing, volledig HLO binnen vijf jaar, HLO stapsgewijs realiseren met verschillende plateaus, etc.) voor besluitvorming. Daarnaast moet elk scenario worden voorzien van een risicoanalyse om financiële baten en lasten af te wegen tegen het risicoprofiel.
- Opstellen van een integrale sourcing strategie die kan dienen als fundament voor de samenwerking met de markt en afdoende kaders en principes bevat om richtinggevend zijn voor de komende periode. Daarbij moeten minimaal de volgende aspecten worden uitgewerkt: *service bundles* (opdeling diensten), *engagement model* (*prime contractor, best of breed*), locatie van de dienstverleningen, *delivery model* (*cloud, in-house*), business perspectief (*business capabilities),* commerciële richtlijnen (verrekening op basis van functiepunten of andere werklastkengetallen, penalty-structuur, etc.), life-cycle management en technologie-gebruik.

Rapport

Gartner

1.0 Inleiding

1.1 Achtergrond

Op 1 juli 2014 heeft de Minister van Defensie in het rapport 'Grensverleggende IV/ICT …' aan de Kamer gemeld wat de uitkomsten zijn van onderzoek naar de staat van IT bij Defensie (BS2014019680). De uitkomst hiervan was dat delen van de huidige IT-infrastructuur verouderd zijn, en niet meer volledig geschikt zijn om de belangrijkste bedrijfsprocessen van Defensie te ondersteunen voor de langere termijn.

De huidige IT-infrastructuur is echter nog wel voldoende om via noodmaatregelen op een gecontroleerde manier een aantal jaren vooruit te kunnen, maar zeker niet voldoende toekomstvast om de ambitie van Defensie voor de langere termijn te ondersteunen. In het hierboven genoemde rapport is geconcludeerd dat er voor die delen die niet meer voldoen nieuwe IT-infrastructuur gebouwd dient te worden.

Deze nieuwe IT-infrastructuur dient toekomstvast, flexibel, betaalbaar, veilig, schaalbaar, state of the art etc. te zijn, en dat geldt ook voor de organisatie die dat moet leveren. Om te bepalen welke eisen Defensie stelt aan de nieuwe IT-infrastructuur is het van belang geweest om eerst te bepalen hoe het militair optreden en de bedrijfsvoering zich de komende jaren ontwikkelen en welke business eisen daaruit voortkomen.

In opdracht van Hoofd Directeur Bedrijfsvoering (hierna: HDBV) is er een verdere analyse gemaakt van de business eisen, de staat van de huidige IT en de business continuïteitseisen en wensen van de belangrijkste onderdelen binnen de voorgenomen transitie:

- Spoor Business eisen
- Spoor IT assessment
- Spoor Business Continuïteit
- High-level IT Infrastructuurontwerp
- IT Applicaties visie
- Sourcing

Het high-level IT infrastructuurontwerp moet richting geven aan een herijking en inrichting van het projectportfolio Defensie IT infrastructuur. De techniek verandert snel daarom wil Defensie **kort-cyclisch** en **incrementeel** innoveren. Daarom zal de verdieping van het high-level IT infrastructuurontwerp in de projecten gebeuren.

1.2 Doel

Om zeker te zijn dat het high-level IT infrastructuurontwerp, de herijking van de Sourcing Strategie en de visie op de IT-applicaties richtinggevend zijn en de juiste kaders en prioriteiten geven, heeft HDBV en CDS een *second opinion* laten uitvoeren door Gartner.

Binnen het door Gartner uitgevoerde onderzoek is antwoord gegeven op de volgende vragen langs verschillende aspecten:

1. **Business effecten**
   A. Zijn de business effecten met bijbehorende **doelstellingen richtinggevend** om projecten/trajecten te definiëren?
   B. Kan Defensie met de business effecten met bijbehorende doelstellingen een methodiek ontwikkelen om **kort-cyclisch en incrementeel te innoveren**?
2. **Architectuur**
   A. Is de **architectuur richtinggevend op ontwikkelingen in de IT infrastructuur**? En is sprake van samenhangende componenten in de architectuur? Waar zijn verbeteringen nodig en welke zijn dat?
   B. In welke mate sluit de voorgestelde architectuur aan op de **markt**? Welke zaken zijn te betitelen als commodity en wat is in de toekomstige situatie Defensie specifiek?
   C. In welke mate worden de **beveiligingseisen adequaat afgedekt** binnen de architectuur gegeven de business eisen?
3. **Kaders**
   A. Zijn de geïdentificeerde business eisen voldoende helder vertaald in **kaders aan de IT-infrastructuur**? Welke gebieden kunnen aangescherpt worden?
   B. Zijn de geïdentificeerde **kaders voor de IT voldoende helder** en dragen deze bij aan de invulling de nieuwe IT-infrastructuur? Welke gebieden kunnen aangescherpt worden?
4. **IT-applicaties visie:** Is het ontwerp van de IT-infrastructuur een geschikte basis om de volgende ontwikkelingen op het gebied van IT-applicaties te ondersteunen?
   A. Doorontwikkeling en exploitatie van **Defensie-brede transactie verwerkende systemen** (zoals ERP);
   B. Introductie van **service georiënteerde architectuur** binnen Defensie die gekoppeld wordt met de transactie-verwerkende systemen;
   C. Het ondersteunen van **grootschalig verzamelen van** gegevens (Big data) en het systematisch analyseren van deze data;
   D. Het ondersteunen **van logisch gecentraliseerde gegevensverzamelingen** (basisadministraties) met stamgegevens;
   E. Het voortdurend en **kort-cyclisch innoveren** van het applicatielandschap om aan te sluiten bij ontwikkelingen zoals *serious gaming* en simulatie;
   F. Het ontsluiten van applicaties via moderne, **op de gebruiker afgestemde platforms**, zoals mobiele *devices* en een gebruikersportaal;
   G. Het **integreren van *social media*** in de samenwerking van medewerkers;
   H. Het **uitwisselen van gegevens met partners** van Defensie, rekening houdend met de rubricering van deze gegevens;
   I. Het toepassen van **cloudoplossingen** om gegevens te delen.
5. **Sourcing**

A. Sluiten de kavels zoals genoemd in de **herijking sourcing** voldoende aan bij het high level ontwerp? Kan de sourcing voldoende bijdragen aan de genoemde doelstellingen en principes uit het high level ontwerp?

B. Geeft de verkaveling en het ontwerp voldoende ruimte voor **marktpartijen om (deel)oplossingen** optimaal te kunnen ontwikkelen? Is het ontwerp stringent genoeg dat deze (deel)oplossingen aansluiten op de ambitie en doelstellingen van Defensie? Welke kavels zouden verder opgesplitst kunnen worden, welke aangescherpt en welke samengevoegd?

C. Biedt de gekozen insteek in **sourcing voldoende flexibiliteit** om stapsgewijs mee te groeien in de veranderende context van Defensie en de technologische ontwikkelingen? Welke verbeteringen en aanpassingen in de sourcing zou u voorstellen?

D. Is in de herijking van de sourcing voldoende rekening gehouden met de (ervaring van Defensie) inzake **regievoering** en kan Defensie het **implementatiepad** van het high level ontwerp volgen middels aansturing van marktpartijen?

6. **Algemeen**

A. Welke **kansen en risico's** ziet u bij het realiseren van het voorgestelde ontwerp? Welke maatregelen moet Defensie nemen om deze te borgen.

B. Is de volgorde van ontwikkeling van de IT infrastructuur in de gepresenteerde roadmap **een logisch groeipad**? Waar zijn andere prioriteiten gewenst?

C. Welk deel van de huidige **IT infrastructuur moet op niveau worden gebracht** (geen totaal nieuw concept) zodat het past binnen de nieuwe IT-infrastructuur en voldoet aan de ambitie en doelstellingen van Defensie?

D. In de IT assessment is gekeken naar de **benodigde expertises en tooling** voor het beheren van de voorgestelde IT Infrastructuur. Geeft het ontwerp voldoende ruimte voor het invullen van de benodigde verbeteringen van het beheer (invulling processen en tooling). Welke conclusie kan worden getrokken over de benodigde expertise voor beheer bij de geschetste IT infra in termen van kwaliteit en kwantiteit.

E. Geef een **indicatieve begroting** van de diverse elementen van het high level ontwerp IT infra.

1.3 Scope

De scope van het onderzoek weergegeven in het voorliggend rapport heeft zich beperkt tot bovenstaande vraagstellingen. Om de vraagstellingen eenduidig en helder te beantwoorden is een uitgebreide set aan documentatie opgeleverd aan Gartner en zijn er diverse interviews en presentatiemomenten georganiseerd om bevindingen en aanbevelingen te toetsen met Defensie.

1.4 Doelgroep

De doelgroep voor deze eindrapportage is de IT Governance Board (ITGB) en de Bestuursraad (BR) en overige direct betrokkenen binnen de Defensie.

2.0 Analyse high-level ontwerp

2.1 Business effecten

Binnen het high-level ontwerp (hierna: HLO) zijn 14 *business*-effecten vastgesteld op basis van een informatieverzameling, analyse en validatie met de verschillende Defensie-onderdelen. Deze *business*-effecten zijn vervolgens vertaald naar de zes onderstaande IT thema's (zie Figuur 1).

Thema 1: Business en mens staan centraal, IT sluit aan
Beter opgeleide en toegeruste medewerkers voor hun taak
IT is beslissingsondersteunend binnen alle taken van Defensie
Thema 2: De IT maakt veilig samenwerken in snel wisselende verbanden mogelijk
De inzet van Defensie is altijd in coalitieverband
Defensie kiest voor samenwerking op het gebied van capability ontwikkeling
Security is een enabler voor veilige informatie-uitwisseling
Thema 3: IT is betrouwbaar en beschikbaar
Defensie moet altijd kunnen optreden, ook als niets meer werkt
Thema 4: Met IT is Defensie 'wereldwijd connected'
Defensie opereert wereldwijd
De footprint in het theater is niet groter dan noodzakelijk
Defensie treedt genetwerkt op
Thema 5: IT verwerkt, slaat op en analyseert grote hoeveelheden informatie
Betere informatiepositie dan de tegenstander
Defensie kan verantwoording afleggen
Thema 6: De IT is eenvoudig en snel aanpasbaar
Defensie benut nieuwe technologieën (technology push)
IT ondersteunt de veranderingen binnen Defensie (demand pull)
Defensie wil op sommige taken vooroplopen

Figuur 1 Overzicht business effecten en IT thema's

Het door Defensie gevolgde proces om tot bovenstaande *business*-effecten (opgedeeld naar verschillende IT-thema's) borgt enerzijds dat de herkenbaarheid, en daarmee gedragenheid ten aanzien van deze *business*-effecten binnen Defensie aanwezig is. Anderzijds heeft de gevolgde consolidatie geresulteerd in een overgebleven set van *business*-effecten en IT-thema's die verbijzondering naar de verschillende Defensie-onderdelen onvoldoende inzichtelijk en daarmee mogelijk maakt.

De *business*-effecten binnen het HLO zijn onvoldoende richtinggevend en eenduidig gedefinieerd om te gebruiken als input voor het opstellen van het projectportfolio. Het ontbreekt daarbij vooral aan een duidelijk prioritering in de tijd en een specifieke uitwerking

van het te behalen (business) doel. De *business*-effecten in de huidige vorm missen daardoor het gezochte sturende karakter en bieden onvoldoende eenduidige handvaten voor het opstellen van de projectportfolio. Dit leidt tot onderstaande beantwoording van de vraagstelling voor wat betreft de toepassingsmogelijkheden van de *business*-effecten voor het opstellen van een projectportfolio: ·

Zijn de business effecten met bijbehorende doelstellingen richtinggevend om projecten/trajecten te definiëren?

Nee, de business effecten dienen scherper te worden uitgewerkt om te dienen als richtinggevende parameters voor de definitie, het opstellen en het kunnen toetsen van het projectportfolio van Defensie.

Het in het HLO vastgelegd ambitieniveau stelt Defensie voor een drietal uitdagingen. De onderstaande figuur geeft een samenvatting van deze uitdagingen (Figuur 2):

Figuur 2 Het HLO en de sourcing documentatie schetsen drie grote uitdagingen.

Binnen zowel het HLO als de sourcing documentatie wordt een gefaseerde en incrementele aanpak voorgesteld. Gartner onderschrijft deze aanpak als de juiste manier om een gecontroleerde realisatie van de geambieerde doelstellingen mogelijk te maken.

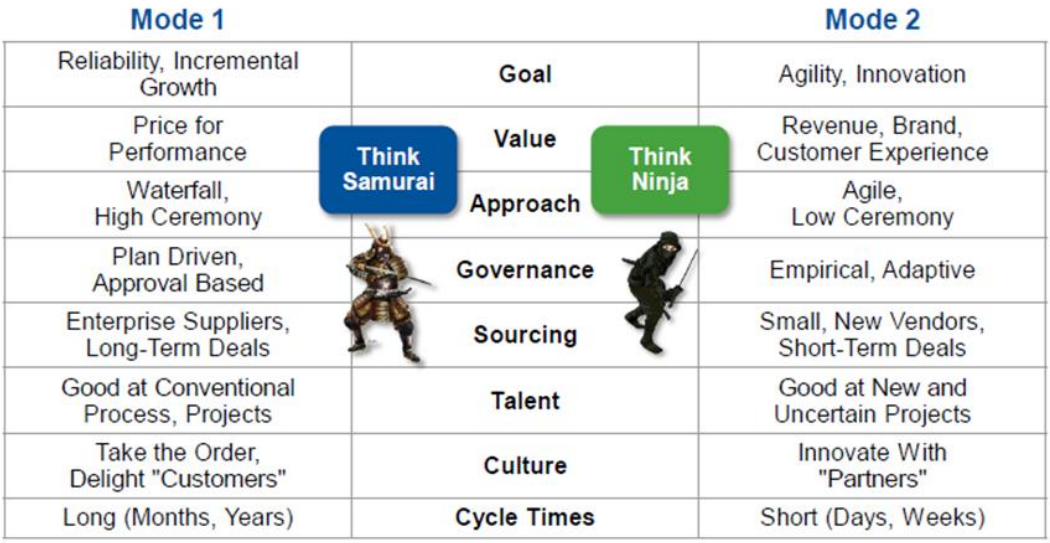
Wel dient Defensie zich te realiseren dat het bewerkstelligen van continuïteit en beveiliging andere eisen aan de organisatie en samenwerking met de markt stelt dan die benodigd voor het vergroten van het innovatievermogen.

De uitdagingen ten aanzien van continuïteit en innovatie stellen Defensie voor een vernieuwingsparadox: *"Met één voet op het gaspedaal en met de andere op de rem".* Om aan deze schijnbare tegenstelling op een juiste en gecontroleerde wijze invulling en realisatie te geven dient Defensie zich te richten en in te richten aan de hand van de twee onderstaande modi:

- **Mode 1:** een organisatie die zich richt op de continuïteit en beveiliging, gedreven door releasematige verandering (*zo min mogelijk*), waterval en kostenoptimalisatie;

- **Mode 2:** een organisatie die zich richt op innovatie door kort cyclische innovatie, gebruik van nieuwe technologieën en innovatieve leveranciers, waarbij verandering per definitie goed is en fouten maken mag.

Deze twee naast elkaar bestaande organisatievormen wordt Bi-modal genoemd en is nader gedetailleerd in het onderstaande figuur.



Figuur 3 De Bi-modal-organisatie (Mode 1 versus Mode 2)

De grootste uitdaging (voor de Mode 1 organisatie) die Gartner ziet is de geleidelijke transitie en het gelijktijdig opschonen van het huidige applicatieportfolio in de oude omgeving naar een nieuwe gestandaardiseerde omgeving. Het HLO voorziet hierin een geleidelijke aanpak in parallel met een applicatie-rationalisatieslag. Gartner marktobservaties laten zien dat vergelijkbare transitietrajecten lang en kostbaar zijn, hetgeen een significante impact heeft op de IT-uitgaven van Defensie gedurende de transitieperiode. Deze kosten drukken, bij gelijkblijvend IT-budget, op de financieringsruimte van innovatieve projecten. Hiervoor zullen de komende jaren duidelijke keuzen gemaakt worden bij het opstellen van de budgettering en projectenportfolio.

Inmiddels is een eerste uitwerking gemaakt van een high-level plateauplanning voor de verschillende IT-domeinen (bv. data center, werkplekken, netwerk). Deze planning moet in lijn worden gebracht met de specifieke doelstellingen die Defensie wil realiseren en het beschikbare budget voor het realiseren van deze verandering.

Bovenstaande analyse leidt tot beantwoording van de vraagstelling:

Kan Defensie met de business effecten met bijbehorende doelstellingen een methodiek ontwikkelen om kort-cyclisch en incrementeel te innoveren?

Ja, ingegeven door het ambitieniveau van Defensie is een incrementele aanpak de enige juiste manier om een gecontroleerde realisatie van de doelstellingen (de *business*-effecten*)* mogelijk te maken. Voor het in Mode 1 opererende deel van Defensie geldt een gefaseerde aanpak van de transitie naar de nieuwe omgeving (elke applicatie en/of applicatieketen krijgt daarbij een prioritering). Voor het in Mode 2 opererende deel van Defensie wordt invulling gegeven aan (ad-hoc) business behoeften op basis van kort-cyclische innovatie.

2.2 ICT Infrastructuur

Binnen het HLO is een uitgebreide set van technologieën en principes beschreven. In aanpak en aanzet vormt dit naar oordeel van Gartner een goede basis tot sturing op het toewerken naar de stip op de horizon. Het HLO sluit aan op de marktontwikkelingen die Gartner waarneemt binnen de ICT-infrastructuur. Gartner stelt op basis hiervan vast dat het HLO daarmee richtinggevend en toekomstvaste IT-realisatie nastreeft.

Na accordering van het HLO adviseert Gartner om een aantal principes verder uit te werken en de consequenties van ieder van deze principes in zowel meer detail en alsook eenduidiger te beschrijven. Ook ten aanzien van de samenhang tussen technologiekeuzen en de verschillende Defensie-onderdelen bestaat er ruimte voor verdere uitwerking.

Binnen de beschikbaar gestelde versie van het HLO is vastgesteld dat een specifieke uitwerking van de verschillende Defensie *capabilities* (bv. commandovoering, intelligence) ontbreekt. Hierdoor is er een onvoldoende eenduidig referentiekader dat kan dienen om de gemaakte keuzen specifiek te maken en in de juiste context te plaatsen. Bijvoorbeeld: het ‘verclouden’ is alleen benodigd wanneer er een behoefte is aan het snel kunnen op- en afschalen van een dienstverlening. Dit is naar verwachting niet voor iedere (vorm van) dienstverlening benodigd. Het principe in de huidige vorm suggereert echter dat alle dienstverlening worden ‘vercloud’, ongeacht mogelijk hoge kosten die daarmee gepaard kunnen gaan.

Een mogelijke indeling naar *business capabilities* is de NATO-classificatie (Nb. gedurende de interviews is aangegeven dat specifieke opdelingen voor Defensie beschikbaar zijn als basis voor het uitwerken van de *business capabilitie*s):

- J1 – Personnel
- J2 – Operational Intelligence
- J3 – Current Operations
- J4 – Logistics/Medical
- J5 – Crisis and deliberate planning
- J6 – Communication and Information Systems
- J7 – Joint Training
- J8 – Finance and Human Resources
- J9 – Policy, Legal, Presentation.

Het gedetailleerde commentaar is opgenomen in Bijlage 1.

Is de architectuur richtinggevend op ontwikkelingen in de IT infrastructuur? En is sprake van samenhangende componenten in de architectuur? Waar zijn verbeteringen nodig en welke zijn dat? Zijn de geïdentificeerde kaders voor de IT voldoende helder en dragen deze bij aan de invulling de nieuwe IT infrastructuur? Welke gebieden kunnen aangescherpt worden?

Ja, de architectuur is richtinggevend op de ontwikkeling in de IT infrastructuur. De gehanteerde principes zijn in grote lijnen samenhangend. Op een aantal specifieke gebieden zijn verbeterpunten gedefinieerd (zie Bijlage A) om de consistentie en samenhang van de principes en kaders te verbeteren.

De keuze voor Cloud-dienstverlening dient nader te worden uitgewerkt. Het 'verclouden' van de eigen dienstverlening of het gebruik maken van Cloud-dienstverlening van externe partijen is afhankelijk van een groot aantal factoren. Gartner heeft hiervoor een *Cloud Decision Model* voor opgesteld waarlangs de verschillende dienstverleningen kunnen worden getoetst voor Cloud-geschiktheid. Het model maakt besluitvorming mogelijk met behulp van de criteria:

- *Vision and Strategy*
- *Market Maturity*
- *Architecture*
- *Data Governance*
- *Demand Management*
- *Finance & Procurement*
- *Security and Risk Management*
- *Service Management*

Zijn de geïdentificeerde business eisen voldoende helder vertaald in kaders aan de IT infrastructuur? Welke gebieden kunnen aangescherpt worden?

Binnen het HLO is een duidelijke vertaling gemaakt van business eisen richting de kaders (principes) van de ICT infrastructuur. De gehanteerde werkwijze wordt door Gartner beschouwd als *best practice*. Gartner ziet als een belangrijk verbeterpunt echter de uitwerking en het contextualiseren van de verschillende *business capabilities*. Specifieke verbetergebieden zijn opgenomen in Bijlage A.

Gartner concludeert dat het HLO **aansluit op marktontwikkelingen** en daarmee ook op de markt (zowel producten als leveranciers). Daarbij dient echter te worden opgemerkt dat het HLO als zodanig nog **geen gedetailleerd architectuurdocument** is. De huidige insteek is volledig agnostisch wanneer het gaat om specifieke oplossingen en/of voorzieningen. Daarmee is het op dit moment nog niet te bepalen in hoeverre zaken kunnen worden betiteld als commodity en in hoeverre Defensie-specifieke oplossingen benodigd zijn. Dit zal nader uitgewerkt moeten worden in het detailontwerp. Gartner adviseert om de uitkomsten voortkomend uit de detailanalyse en detailuitwerking mee te nemen in de te maken keuzen voor wat betreft de samenwerking met marktpartijen vanuit een *commodity*- en / of *niche*-perspectief.

In welke mate sluit de voorgestelde architectuur aan op de markt? Welke zaken zijn te betitelen als commodity en wat is in de toekomstige situatie Defensie specifiek?

Het HLO sluit aan op de dienstverlening die wordt geleverd door marktpartijen. Na accordering van het HLO adviseert Gartner om a.d.h.v. een verdere uitwerking in de uitvoeringsfase concrete uitspraken te doen welke dienstverleningen betiteld kunnen worden als commodity en/of Defensie-specifiek zijn

De principes t.a.v. beveiligingseisen zijn over het algemeen marktconform en in lijn met de business eisen maar missen op vlakken nadere uitwerking. Gedetailleerd commentaar is opgenomen in Bijlage A.

In welke mate worden de beveiligingseisen adequaat afgedekt binnen de architectuur gegeven de business eisen?

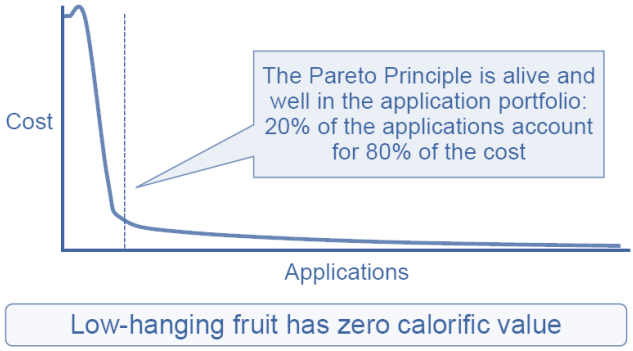
Deze zijn op het niveau van het HLO als document afdoende afgedekt en in lijn met ontwikkelingen in de markt zoals deze door Gartner waargenomen en eisen vanuit Defensie.

2.3 IT Toepassingen

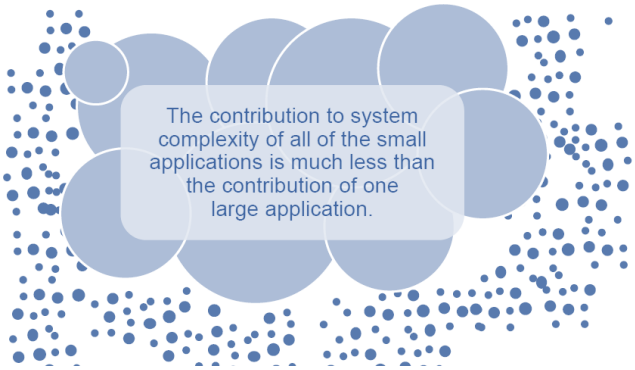
De opgestelde ontwerpprincipes voor IT Toepassing ontberen op aspecten verbijzondering waardoor toepasbaarheid voor Defensie-specifieke onderdelen niet altijd even herleidbaar is. Een detailanalyse met daarbij aanbevelingen voor verbetering is opgenomen in Bijlage B.

2.3.1 Applicatierationalisering

Op basis van marktervaringen en Gartner eigen directe ervaring bij het ondersteunen van organisaties bij het rationaliseren van het applicatieportfolio, is Defensie geadviseerd een andere zienswijze (en daaraan verbonden kengetallen) te hanteren voor wat betreft het opschonen van het huidige applicatieportfolio. (zie hiertoe ook de Aanbevelingen-sectie). De focus dient daarbij te liggen op verlaging van TCO-kosten en het versnelt kunnen realiseren van nieuwe functionaliteit.



Figuur 4 *Mythe 1: Het reduceren van het aantal applicaties reduceert ook de totale kosten*



Figuur 5 *Mythe 2: Afname aantal applicaties reduceert de complexiteit van het IT-landschap*

2.3.2 Specifieke vragen t.a.v. IT Toepassingen

Is het ontwerp van de ICT-infrastructuur een geschikte basis om de volgende ontwikkelingen op het gebied van IT-applicaties te ondersteunen?

Vraag	Antwoord
Het doorontwikkeling en exploitatie van Defensie-brede transactie verwerkende systemen (zoals ERP).	Ja (onvoldoende uitgewerkt) – alleen onduidelijk in hoeverre deze specifieke *capability* ondersteund kan worden door externe SaaS-oplossingen i.v.m. databeveiliging
Het introduceren van service georiënteerde architectuur binnen Defensie die gekoppeld wordt met de transactie-verwerkende systemen.	Ja (onvoldoende uitgewerkt) – met daarbij de nuancering dat het hier niet gaat om de gehele applicatie stack
Het ondersteunen van het grootschalig verzamelen van gegevens (Big data) en het systematisch analyseren van deze data	Onduidelijk – er zijn geen specifieke uitspraken gedaan hoe Big Data wordt ingevuld vanuit een IT-infrastructuur perspectief
Het ondersteunen van logisch gecentraliseerde gegevensverzamelingen (basisadministraties) met stamgegevens	Ja (onvoldoende uitgewerkt) – maar binnen het HLO is niet omschreven hoe men wil toewerken naar gecentraliseerde basisadministratie (MDM)
Het voortdurend en kort-cyclisch innoveren van het applicatielandschap om aan te sluiten bij ontwikkelingen zoals serious gaming en simulatie	Ja (onvoldoende uitgewerkt) - onduidelijk wat hier dan de specifieke eisen voor zijn. Dit zal nader moeten worden uitgewerkt in het detailontwerp
Het ontsluiten van applicaties via moderne, op de gebruiker afgestemde platforms, zoals mobiele devices en een gebruikersportaal. Het integreren van social media in de samenwerking van medewerkers.	Deels – ontbreekt aan nuancering op dit gebied naar de verschillende *capabilities* (zie opmerking principes – Bijlage B)
Het uitwisselen van gegevens met partners van Defensie, waarbij rekening wordt gehouden met de rubricering van deze gegevens	Ja
Het toepassen van Cloudoplossingen om gegevens te delen	Onduidelijk – in hoeverre externe Cloud-toepassingen wel of niet gebruikt kunnen worden. Het ontbreekt aan nuancering op dit gebied naar de verschillende capabilities.

2.3.3 Overige vragen

Is de volgorde van ontwikkeling van de ICT infrastructuur in de gepresenteerde roadmap een logisch groeipad? Waar zijn andere prioriteiten gewenst?	Gartner constateert dat zowel in de volgordelijkheid als afhankelijkheid er omissies zijn. Daarnaast constateert Gartner dat de tijdslijnen van de verschillende roadmaps te ambitieus zijn gesteld. Dit geldt vooral voor de applicatietransitie en rationalisatie

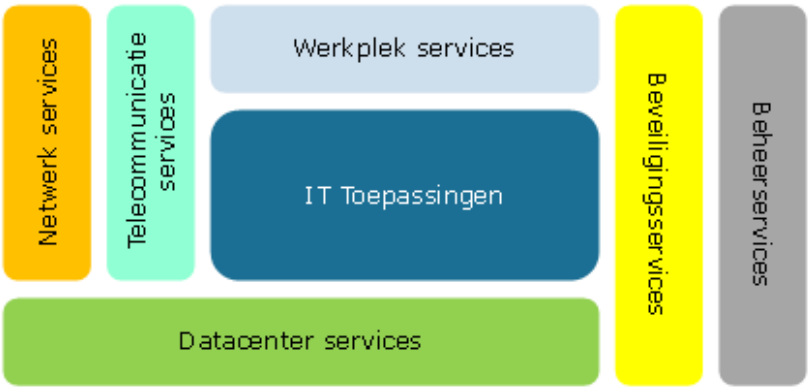
Welk deel van de huidige ICT infrastructuur moet op niveau worden gebracht (geen totaal nieuw concept) zodat het past binnen de nieuwe ICT-infrastructuur en voldoet aan de ambitie en doelstellingen van Defensie?	Defensie hanteert een greenfield-approach waarbij de gehele ICT-infrastructuuromgeving nieuw wordt ingericht en oude voorzieningen worden gemigreerd. De onderhavige vraagstelling kan derhalve, gelet op de gekozen aanpak en de Defensie aangeleverde informatie, niet worden beantwoord.
In het ICT assessment is gekeken naar de benodigde expertises en tooling voor het beheren van de voorgestelde ICT Infrastructuur. Geeft het ontwerp voldoende ruimte voor het invullen van de benodigde verbeteringen van het beheer (invulling processen en tooling)? Welke conclusie kan worden getrokken over de benodigde expertise voor beheer bij de geschetste ICT infra in termen van kwaliteit en kwantiteit?	Het HLO gaat niet specifiek in op de eisen die worden gesteld aan expertise en competentie van medewerkers als ook niet aan de eisen ten aanzien van de te gebruiken tooling voor het beheer van het IT-landschap. Benodigde expertise ten aanzien van het beheer (in kwantiteit en kwaliteit) kent afhankelijkheden met onder meer de gewenste dienstverleningsniveaus en specifieke technologiekeuzes. Doordat deze nog niet inzichtelijk zijn (of herleid kunnen worden op basis van de beschikbaar gestelde informatie) is hierop geen terugkoppeling te geven.

3.0 Analyse samenwerking met de markt

Voor het uitvoeren van de ‘second opinion’ op het domein ‘samenwerking met de markt’ heeft Gartner de documenten ‘Herijking Sourcing Strategie’ en de ‘Nota Scenario Sourcing’ gehanteerd

De ‘Herijking Sourcing Strategie’ schetst de complexiteit van het sourcingsvraagstuk en de verschillende mogelijkheden, maar biedt onvoldoende sturing en geeft geen richting voor besluitvorming op dit onderwerp. De uitspraken in de nota daarentegen zijn eenduidig, en duidelijk en helder verwoord. Gezien de volgordelijkheid van de documentatie is door Gartner voor de hieronder weergegeven analyse voornamelijk uitgegaan van de recente nota bij beantwoording van de vraagstellingen.

De high-level verkaveling binnen de documentatie (herijking en nota) laat een opdeling zien van dienstverleningen die grotendeels in lijn is met de markt.



Figuur 6 *Opdeling naar verschillende dienstverleningsgebieden*

Defensie kiest daarbij voor meerdere strategische partners (*best of breed*). De keuze voor meerdere strategische partners (best of breed) wordt gezien als de juiste om de verschillende business capabilities te ondersteunen. Bij de eerste stap Applicatie Housing & Hosting (AHH) wordt gesproken over een enkele partner. Gezien de diversiteit van de huidige omgeving is een enkele partner naar verwachting niet evident. Door gebruik te maken van een consortium is er 'toegang' tot een bredere set aan expertise. De specifiek benodigde expertise en dus de keuze tot onderverdeling is afhankelijk van de diversiteit van het IT Landschap (zowel infra als apps). Dit is een analyse die op dit moment niet door Gartner is uitgevoerd. Uitgangspunt is dat er sprake is van een zeer gedifferentieerd landschap en dat het voor de hand ligt samen te werken met verschillende leveranciers, elk verantwoordelijk voor specifiek domeinen. Een voordeel van meerdere partijen is daarnaast dat dit zorgt voor een ‘gezonde’ competitieve omgeving en dus hogere kostenefficientie voor Defensie. Gezien het grote volume van de benodigde verandering zijn meerdere leveranciers zeker mogelijk. Een mogelijke opdeling is:

- **Infrastructuur-dienstverlening:** Een enkele leverancier voor de platform-hosting (housing / hosting);
- **Applicatieve-dienstverlening:** Meerdere leveranciers voor de applicatie-transitie (afhankelijk van de ontwikkelstraat) en het applicatiebeheer voor reeds gemigreerde applicaties.

Gartner onderschrijft de aanpak om de sourcing gefaseerd en in behapbare delen te realiseren. Een belangrijke reden hiervoor is ook het geleidelijk opbouwen van de regiecompetentie binnen de Defensie-organisatie. Het voorgestelde samenwerkingsmodel en de constatering dat Defensie altijd IT activiteiten onder eigen verantwoordelijkheid zal doen vanwege haar unieke primaire taak sluit aan bij de ambities uit het HLO.

De sourcingdocumentatie mist de nuancering van de verschillende sub-domeinen op basis van specifieke business capabilities of technologie-expertise. Alsmede ook het onderscheid tussen continuïteit en innovatie. Dit dient echter een belangrijke parameter zijn voor het verder opdelen van de dienstverleningen richting specifieke leveranciers met name op het gebied van IT Toepassingen (Applicatiebeheer- en ontwikkeling).

Sluiten de kavels zoals genoemd in de herijking sourcing voldoende aan bij het high level ontwerp? Kan de sourcing voldoende bijdragen aan de genoemde doelstellingen en principes uit het high level ontwerp?

Nog onvoldoende. Belangrijke paradigma's (pace layering, bi-modal, business capabilities) capabilities komen in zowel HLO als sourcing strategie onvoldoende terug, terwijl dit juist de verbindende elementen zijn tussen de twee documenten. Sourcing in de vorm van strategische samenwerking met de markt kan Defensie helpen haar doelstellingen (versneld) te realiseren. Gartner onderstreept daarmee de keuze die Defensie maakt om vanuit deze samenwerking haar doelen te realiseren.

Geeft de verkaveling en het ontwerp voldoende ruimte voor marktpartijen om (deel)oplossingen optimaal te kunnen ontwikkelen? Is het ontwerp stringent genoeg dat deze (deel)oplossingen aansluiten op de ambitie en doelstellingen van Defensie? Welke kavels zouden verder opgesplitst kunnen worden, welke aangescherpt en welke samengevoegd?

Nog niet afdoende. De verdere vertaling naar de verschillende domeinen en/of *business capabilities* dient verder te worden uitgewerkt in de sourcingdocumentatie. Hiervoor zal ook een verdere uitwerking volgend op het HLO benodigd zijn om beide documenten op elkaar te laten aansluiten. Het gaat hierbij dan met name om de uitwerking van de domeinen applicatiebeheer – en ontwikkeling en de benodigde transitieactiviteiten (gezien de varieteit binnen het landschap bestaat de kans dat dit moet worden opgepakt door meerdere leveranciers).

Biedt de gekozen insteek in sourcing voldoende flexibiliteit om stapsgewijs mee te groeien in de veranderende context van Defensie en de technologische ontwikkelingen? Welke verbeteringen en aanpassingen in de sourcing zou u voorstellen?

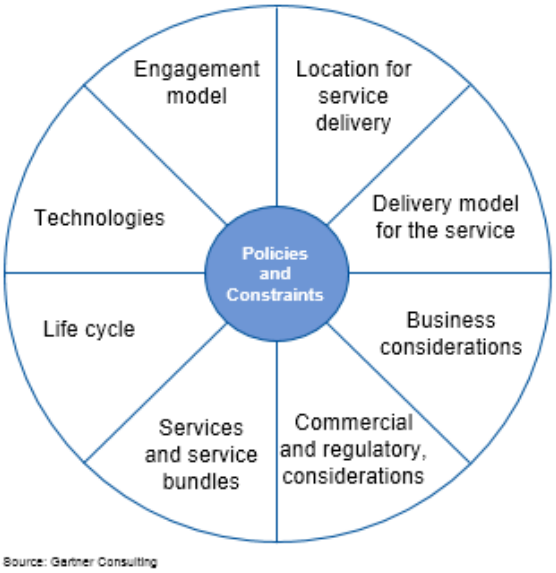
De keuze voor meerdere strategische partners (*best of breed*) wordt gezien als de juiste om de verschillende business capabilities te ondersteunen. Gartner onderschrijft ook de aanpak om de sourcing gefaseerd en in behapbare delen te realiseren. Een belangrijke reden hiervoor is ook het geleidelijk opbouwen van de regiecompetentie binnen de Defensie-organisatie. Het document kan worden verbeterd door een innovatie-paragraaf toe te voegen aan de sourcingdocumentatie die beschrijft hoe Defensie de samenwerking met de markt voorziet.

Gartner heeft vastgesteld dat op dit moment er geen vastomlijnde, duidelijk herkenbare en marktconform opgezette regie-organisatie binnen Defensie is. Gelet op de beoogde doelstellingen, de in te zetten transitie voor de komende jaren, en het continue kunnen borgen gedurende deze periode maar ook daarna, is het geïnstitutionaliseerd zijn van een regie-organisatie noodzakelijk. Het inzetten van een externe strategische partij voor onafhankelijke advisering is een goede keuze om deze competenties versneld op te bouwen binnen de eisen organisatie.

Is in de herijking van de sourcing voldoende rekening gehouden met de (ervaring van Defensie) inzake regievoering en kan Defensie het implementatiepad van het high level ontwerp volgen middels aansturing van marktpartijen?

Gedeeltelijk. Het opbouwen van de benodigde regiecompetenties moet worden beschreven in een aparte paragraaf.

In de uitwerking van een integrale sourcing strategie dienen minimaal de volgende elementen worden opgenomen (zie Figuur 7):



Sourcing Option Dimensions

1. **Engagement Model** covers the different approaches that can be used to contract with one or more service providers for an IT service *(examples prime contractor, best of breed etc)*
2. **Location** covers the options to be considered from where the desired service can be delivered *(examples on shore, regional, off shore etc)*
3. **Delivery Model** covers the different types of model that can be used to deliver the desired service (examples Cloud, IaaS, PaaS, in-house DC etc)
4. **Business Considerations** covers the choices open to deliver the desired service to one or more business units *(examples Sales, Finance, Country XYZ..)*
5. **Commercial and Regulatory Considerations** covers the pricing and other contractual related aspects (SLAs etc) of the approach
6. **Service Bundles** covers the choices open for delivering the service through using a range of different types of service *(examples workplace consists of PC, telephone and printer)*
7. **Life Cycle** covers the different stages of the life cycle of a service *(Example RUN, CHANGE, TRANSFORM, RETIRE)*
8. **Technologies** covers the different types of technology that can be used to deliver the service *(Example UNIX, LINUX, etc)*

Figuur 7 Gartner raamwerk voor uitwerking sourcing strategie

4.0 Risico's

Op basis van de uitgevoerde analyse van het HLO, de herijking Sourcing Strategie en het door Defensie gevolgde proces om te komen tot onder meer de *business*-effecten zijn door Gartner enkele risicogebieden geïdentificeerd behorende bij vergelijkbare transitie-initiatieven zoals in het HLO wordt voorgestaan. Gartner adviseert Defensie deze risico's te mitigeren en heeft gedurende de uitvoering van de 'second opinion' al geconstateerd dat Defensie (zie ook paragraaf 4.2) een aanvang heeft gemaakt met het op een juiste wijze mitigeren van mogelijke risico's. Ieder van de geïdentificeerde risicogebieden is hieronder verder beschreven:

4.1 Samenwerken met de markt

Op basis van de aangeleverde documentatie (onder meer de Herijking Sourcing Strategie alsook de Sourcing Strategie) ziet Gartner een risico ontstaan bij het uitvoeren van de in deze documenten gezamenlijk benoemde aanpak tot samenwerking. Inmiddels is in samenspraak met Defensie vastgesteld dat deze richting niet meer de juiste invulling geeft aan de beoogde Defensie-doelstellingen. Gartner is dan ook van mening dat het opstellen van een nieuwe nota die invulling geeft aan het samenwerken met de markt een eerste en juiste stap is. Hierbij dient rekening gehouden te worden met enerzijds een duidelijke en eenduidige koppeling met de doelstellingen zoals verwoord in het HLO onder meer ten aanzien van de algemene en de 'verbijzonderde' vormen van dienstverlening (zowel huidige als toekomstige). Door deze koppeling te hanteren worden de te maken keuzen ten aanzien van mogelijke marktpartij(en) niet alleen inzichtelijk en transparant, maar sluiten direct aan bij de doelstellingen (de gewenste *business*-effecten) van Defensie. Inmiddels is door Defensie al in een eerste opzet gehoor gegeven aan deze aanbeveling en heeft dit geleid tot het opstellen van een nieuwe nota betreffende de samenwerking met de markt cq. marktpartijen. Dit document kan echter nog niet worden beschouwd als een integrale sourcing strategie.

4.2 Aligneren met de business

Voor het opstellen van het HLO en het herleiden van de beoogde *business* doelstellingen die door middel van het HLO gerealiseerd diende te worden, zijn de zogenoemde *business*-effecten 'opgehaald' bij de *business*. Een dergelijke exercitie heeft niet eerder in een vergelijkbare omvang plaats gehad. Ofschoon Gartner heeft geconstateerd dat de gekozen aanpak- en werkwijze (met name ten aanzien van de consolidatie van de *business*-effecten) enkele verbeterpunten kent, ondersteunt Gartner de gekozen aanpak en beveelt Defensie aan om deze aanpak, na het aanpassen van de geconstateerde verbeterpunten, als *best practice* binnen Defensie blijvend te hanteren. Niet alleen borgt dit de ontstane samenwerking tussen IT en de *business* verder, het biedt ook gelijktijdig de mogelijkheid om gedurende de transitie (en daarna) blijvend te borgen en te controleren of de ingezette richting nog steeds aansluit bij de beoogde *business*-effecten (dit laatste temeer omdat in de tijd *business*-effecten mogelijk zich kunnen wijzigen). Het in continue 'contact' blijven met de *business* dient een van de verantwoordelijkheden te zijn van de in te richten regie-organisatie (zie volgende aanbeveling).

4.3 Regie-organisatie

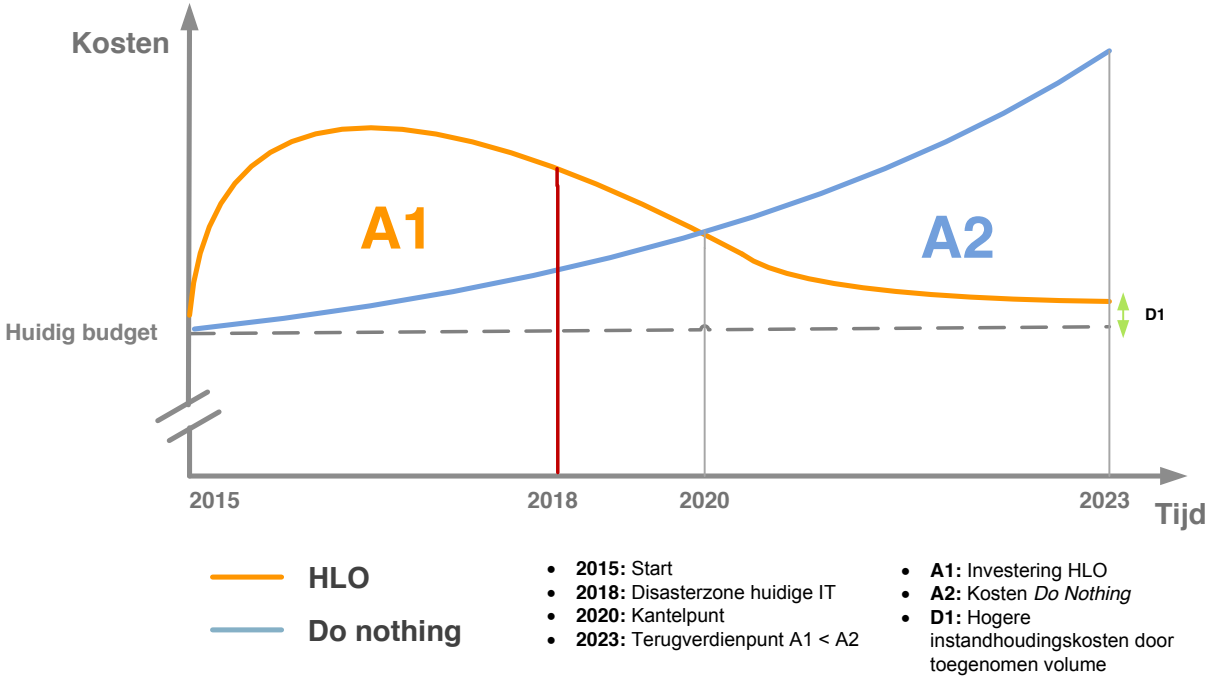
Gartner heeft vastgesteld dat op dit moment er geen vastomlijnde, duidelijk herkenbare en marktconform opgezette regie-organisatie binnen Defensie is. Gelet op de beoogde

doelstellingen, de in te zetten transitie voor de komende jaren, en het continue kunnen borgen gedurende deze periode maar ook daarna, is het geïnstitutionaliseerd zijn van een regie-organisatie noodzakelijk.

Gartner adviseert Defensie om aan de hand van het Gartner 'IS Lite' –model (zie Figuur 10) de regie-organisatie in te richten, waarbij Gartner aanvullend adviseert om voor het invullen van de verschillende rolgroepen afzonderlijk alsook over het geheel heen een samenwerkingsverband (*strategic partnership*) aan te gaan. Een dergelijk samenwerkingsverband heeft een tweetal doelen: enerzijds stelt het Defensie in staat om voor de verschillende regie-rollen waar nodig tijdelijk extra menskracht (zowel kwalitatief alsook kwantitatief) aan te trekken. Om ook in de 'volwassenheid' als regievoerende organisatie te groeien is het van belang dat Defensie een samenwerking aangaat met een ondersteunende, deels aansturende partner die daaraan bijdraagt. Gartner adviseert Defensie om hiervoor een partner te selecteren die geen belang heeft in zogenaamde '*downstream*' activiteiten. De toegevoegde waarde van een dergelijke partij bestaat tevens in het helpen opzetten van de benodigde regie-organisatie vanuit zowel een governance, competentie (kwalitatief en kwantitatief) perspectief. Daarnaast dient deze samenwerkende partner als 'toetssteen' voor wat betreft het aangaan van samenwerkingsverbanden met leveranciers cq. de markt voor wat betreft het buiten Defensie beleggen van bepaalde vormen van dienstverlening.

5.0 High-level financiële analyse

Onderstaand figuur geeft een high-level inschatting van de kostenontwikkelingen over de periode 2015-2023.



Figuur 8 *High-level financiële analyse*

Het scenario *Do nothing* leidt tot een versnelde toename van kosten doordat de instandhoudingskosten exponentieel stijgen gezien meer inspanning benodigd is de continuïteit en beveiliging van het huidige IT landschap te borgen. In 2018 wordt de *disasterzone* bereikt. Vanaf dit tijdstip kan de continuïteit en beveiliging niet meer gegarandeerd worden en ontstaan er risico's in de operatie. Het scenario HLO vraagt een initiële investering waardoor er kosten gemaakt worden boven het huidige budget. In 2020 is er echter sprake van een kantelpunt: de jaarlijkse kosten van het HLO liggen onder de kosten voor het scenario *Do nothing*. Defensie beschikt over een *state-of-art* IT omgeving, de instandhoudingskosten zijn relatief laag en het innovatievermogen van de organisatie is groot. Doordat er gebruik wordt gemaakt van nieuwe technologieën als Big Data en IoT liggen de totale kosten voor IT boven het huidige budget. Rond 2023 wordt na verwachting de *break-even* bereikt t.a.v. kosten (A1 < A2).

Bovenstaande verwachte kostenontwikkeling zal nader uitgewerkt moeten worden in een kostencalculatiemodel (zie paragraaf 6.5).

6.0 Aanbevelingen

Defensie wil dat de komende jaren in het teken staan van een geleidelijke transitie naar een betrouwbare en stabiele nieuwe omgeving. Tegelijkertijd moet er een inhaalslag worden gemaakt om de achterstand in IT in te lopen en het innovatievermogen van de organisatie te vergroten. Deze twee doelstellingen vragen om een verstrekte samenwerking met de markt omdat Defensie op dit moment niet alle benodigde kennis en kunde tot haar beschikking heeft in de eigen organisatie.

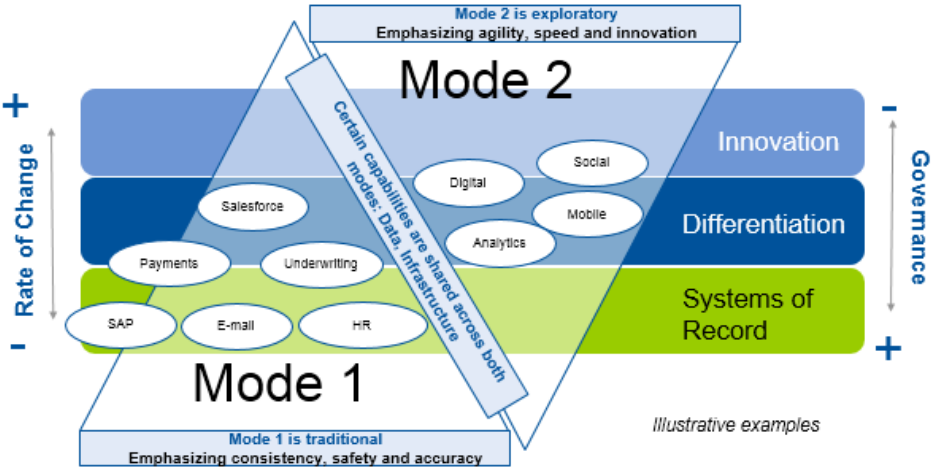
De aanbevelingen zijn verdeeld in de volgende categorieën:

- Strategie & architectuur
- Samenwerking met de markt en regievoering
- Innovatie en organisatorische inrichting: Bi-modal IT
- Applicatierationalisatie en transitie
- Financieel.

Opgemerkt dient te worden dat naast het uitvoeren van de ‘second opinion’ Gartner enkele aanbevelingen heeft opgesteld die uitsluitend betrekking hebben op de uitvoeringsfase zijnde de fase volgend op de instemming met de in het HLO beschreven strategische intentie.

6.1 Strategie & Architectuur

- **SA1:** Maak de doelstellingen specifieker en in de tijd meetbaar waardoor de verdere uitwerking een meer kaderstellend karakter krijgt en kan dienen als basis voor het definiëren van de projectenportfolio:
  - Het specifieker en tijdsgebonden maken van de business doelstellingen en deze opnieuw toetsen met de business eigenaren.
  - Het specifieker en tijdsgebonden maken van de IT doelstellingen gekoppeld aan deze business doelstellingen.
  - Het vertalen van deze doelstellingen naar een high-level plateauplanning. Wanneer wordt welke doelstelling bereikt in de tijd? Deze high-level plateauplanning is vervolgens weer de basis voor de domein-specifieke plateauplanningen.
- **SA2:** Detailleer voor elk IT-domein een ontwerp dat kan dienen als basis voor het vormgeven van concrete projecten en/of de samenwerking met de markt.
- **SA3:** Integreer het concept van *business capabilities* en *pace-layering* (zie Figuur 9) binnen de verdere detailontwerpen om de technologieën en principes nader te duiden en te specificeren voor de Defensie-specifieke context.
- **SA4:** Werk de principes voor IT Infrastructuur en IT toepassingen verder uit op basis van de gedane aanbevelingen (zie Bijlage A & B).
- **SA5:** Stel een realistische transitie *roadmap* op voor de komende 3-5 jaar die een balans aanbrengt tussen prioriteiten vanuit de *business*, beschikbare financiële middelen, organisatorische capaciteit (inclusief de regie-organisatie) en competenties, gefaseerde samenwerking met de markt (voor zowel de dienstverlening alsook de regie-organisatie) en risico-mitigatie.

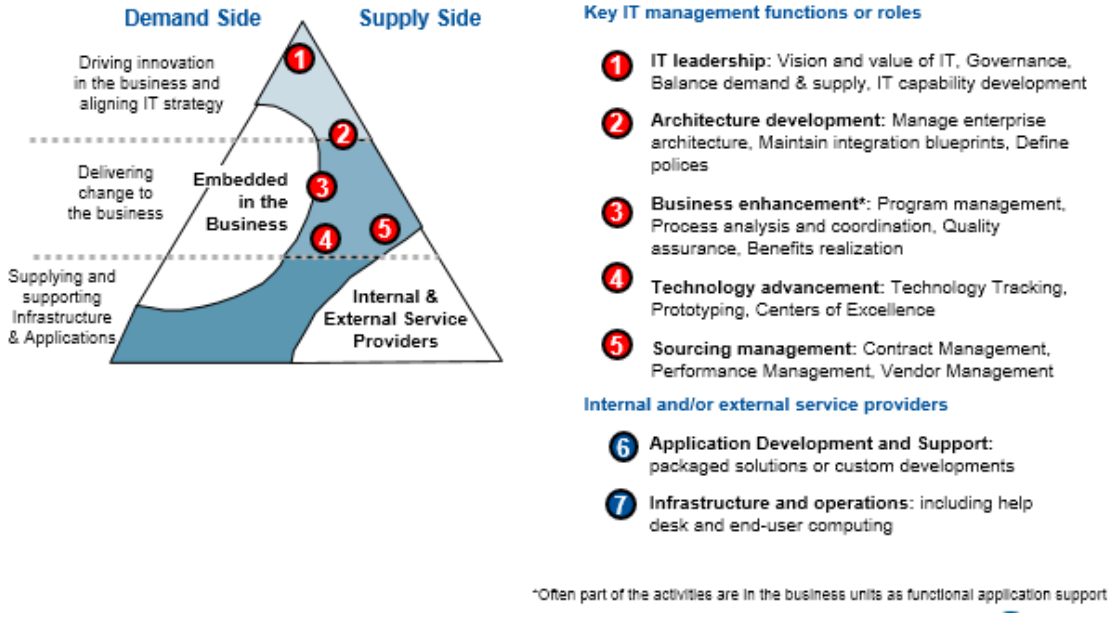


Figuur 9 *Pace-layering (categorisatie van drie verschillende type voorzieningen)*

6.2 Samenwerking met de markt en regievoering

- **SR1:** Stel een integrale sourcing strategie op die de strategische keuzen helder samenvat en verwoord. Documentatie is op dit moment teveel gefragmenteerd in de organisatie. Gebruik een *best practice* template voor het opstellen van deze strategie en adresseer de volgende gebieden: *service bundles* (opdeling diensten), engagement model (*prime contractor, best of breed*), locatie van de dienstverleningen, *delivery model* (*cloud, in-house*), business perspectief (*business capabilities*), commerciële richtlijnen (verrekening op basis van functiepunten of andere werklastkengetallen, penalty-structuur, etc.), life-cycle management en technologie-gebruik.
- **SR2:** De sourcing strategie moet faciliteren voor een ‘Mode 1’ en ‘Mode 2’ organisatie. Defensie heeft specifieke SME-leveranciers nodig voor de verschillende domeinen. Dit moet nader binnen de sourcing documentatie worden uitgewerkt. Dit zal leiden tot een groter aantal leveranciers per dienstverleningsgebied.
- **SR3:** Detaileer de uitwerking van de opdeling van leveranciersgebieden met behulp van een meer Defensie-specifieke opdeling naar de benodigde *capabilities* voor Defensie en beschikbare capaciteiten aanwezig bij de verschillende marktpartijen.
- **SR4:** Hou de regievoering onder aansturing en verantwoordelijkheid van Defensie management en werk met één externe strategische onafhankelijke partner voor het versneld opbouwen en aanvullen van de benodigde regiecapaciteit (naar verwachting op basis van een *staff augmentation* model). Hanteer voor specifiek technologisch, organisatorisch of financieel advies een best-of-breed aanpak en werk samen met volledig onafhankelijke adviesbureaus (op basis van een *fixed price* model).
- **SR5:** Versterk de benodigde regiecompetenties en capaciteit langs vijf hoofdrollen (zie Figuur 10): IT Leiderschap, Architecture, Business Enhancement, Technology Advancement en Sourcing Management met behulp van een aantal plateaus. Naar verwachting zal de totale regieorganisatie een volume aannemen tussen de 175-250

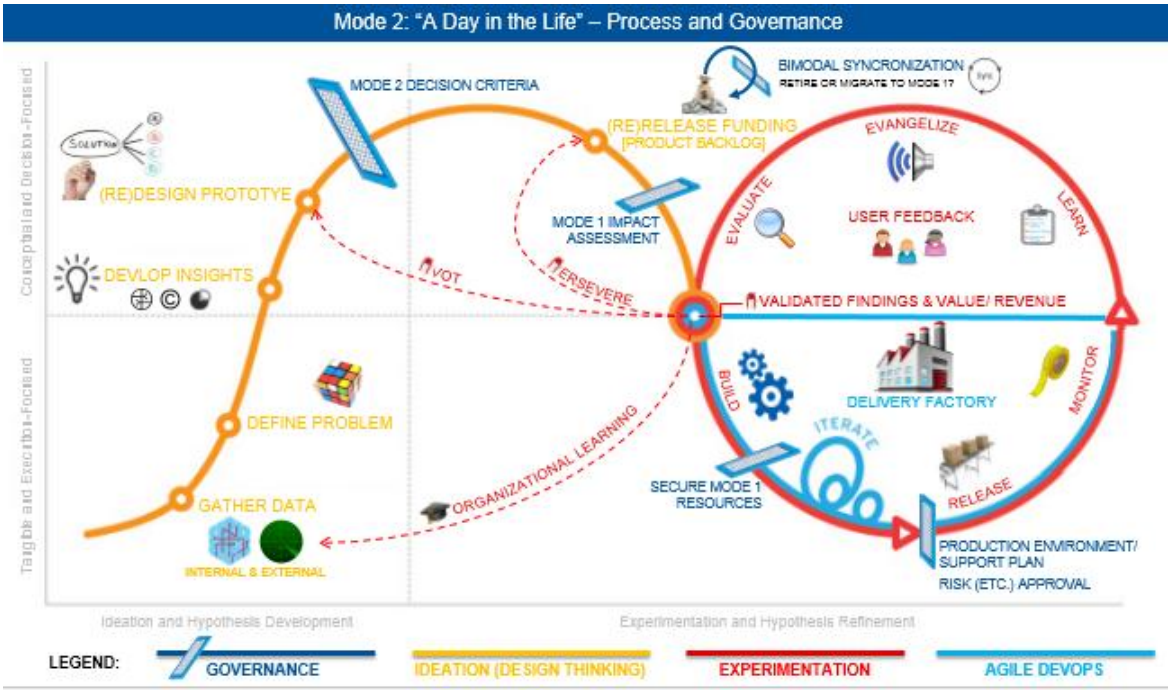
FTE (intern + externe inhuur) voor deze vijf rollen hetgeen meeweegt in de kostenvoet.



Figuur 10 Overzicht IS Lite model

6.3 Innovatie en organisatorische inrichting: Bi-modal IT

- **IN1:** Hanteer een separaat budget voor innovatie dat volledig los staat van het exploitatie en transitiebudget. Maak innovatie **geen** onderdeel van reguliere dienstverlening, met uitzondering van reële aannames t.a.v. verwachte efficiëntiewinst (door nieuwe en verbeterde oplossingen en opgebouwde kennis) gedurende het contract. Geleidelijke doorontwikkeling (bv. procesverbetering) wordt door Gartner gezien als Mode 1 (dus geen innovatie).
- **IN2:** Zet een apart organisatieonderdeel op waarin medewerkers werken met een ondernemerscultuur, een hoge mate van nieuwsgierigheid, inzicht in technologie en durf en werk samen met innovatieve leveranciers met een specifiek expertisegebied en ingewerkt team.
- **IN3:** Definieer een proces en *governance* structuur (zie Figuur 11) met duidelijke koppelvlakken waarin is uitgewerkt hoe ‘synchronisatie’ plaats vindt tussen de twee organisatieonderdelen: Mode 1 en Mode 2 (i.a.w. het laten landen van innovaties binnen de organisatie).



Figuur 11 Integratie-governance tussen Mode 1 & Mode 2

6.4 Applicatierationalisatie en -transitie

Gartner adviseert Defensie ten aanzien van de applicatierationalisatie-doelstellingen om geen doelstellingen te formuleren op basis van aantallen applicaties. Gartner adviseert Defensie om eerder doelstellingen vast te stellen die gelieerd zijn en af te meten zijn aan kengetallen ten aanzien van verlaging van de totale TCO van het applicatieportfolio gecombineerd met het reduceren van dubbele functionaliteit. De laatste is na onderzoek wel uit te drukken in het verminderen van het aantal applicaties en kan derhalve dan ook, maar enkel in die context, als zodanig worden gehanteerd.

Om tot de benodigde inzichten en mogelijkheden te komen die gerealiseerd kunnen worden met het rationaliseren van het bestaande applicatieportfolio adviseert Gartner Defensie de volgende stappen te ondernemen:

- **AM1:** Start met het opstellen van de bestaande applicatiearchitectuur, waarbij naast relevante informatie op *Configuration Item*-niveau tevens inzichtelijk wordt gemaakt welke applicatieafhankelijkheden er zijn (tussen applicaties onderling en applicaties en databronnen). En breng in kaart welke applicaties ondersteunend zijn aan welke primaire en secundaire bedrijfsprocessen.
- **AM2:** Evalueer tevens of de huidige RTO- en RPO-waarden[1] voor de verschillende applicaties in lijn liggen met de voor het proces benodigde waarden. Dit inzicht is nodig om in een later stadium (tijdens de transitie) niet alleen een applicatie om te zetten naar de nieuwe omgeving en / of deze 'om te poorten', maar om ook

[1] Recovery Time Objective (RTO) ook wel herstellingtijd doel genoemd. Een RTO is de tijd waarna een proces(sen)/applicatie(s) na een onderbreking moet teruggebracht zijn op een aanvaardbaar niveau, om een onacceptabele impact op de organisatie te vermijden.

Recovery Point Objective (RPO). De RPO is het punt in de tijd tot waar men minimaal de gegevens moet kunnen herstellen. Het is dus de acceptabele hoeveelheid aan dataverlies uitgedrukt in tijd.

gelijktijdig (als onderdeel van de transitie) de nieuwe omgeving ook zo (hardware-matig) in te richten dat aan de juiste business-eisen wordt voldaan.

- **AM3:** Voer een applicatie portfolio analyse uit om vast te stellen welke applicaties (vanuit functionaliteitsperspectief) overlappende functionaliteit bieden en maak op basis van technologische aspecten (*life cycle*, onderhoudbaarheid, toekomstvastheid, beveiliging) en business aspecten (in hoeverre is de functionaliteit ondersteunend en / of onderscheidend naar de primaire of secundaire bedrijfsprocessen) en kosten inzichtelijk welke applicaties genomineerd worden om (op termijn) te worden uitgezet. Gartner marktobservaties tonen aan dat door het op deze wijze rationaliseren van het applicatieportfolio een aanzienlijk deel van de applicatiekosten (huidige kostenvoet) 'teruggewonnen' wordt. De kostenbesparing die hiermee gerealiseerd wordt kan daarmee 'terugvloeien' in de transitiekosten.
- **AM4:** Stel een transitieplan op waarbij rekening wordt gehouden met de 'belangrijkheid' van de applicatie (of samenhang van applicaties) gecombineerd met de *life cycle* van de applicatie of samenhang van applicaties. Dit draagt bij aan het juist prioriteren van de volgorde van transitie en verminderd kosten doordat de keuze gemaakt kan worden om bepaalde applicaties niet meer te migreren omdat deze end-of-life zijn of binnen de doorlooptijd van de transitie end-of-life worden. Tevens dient in deze stap een *exception list* te worden opgesteld voor die applicaties waarvan mogelijk de *life cycle* al einde is (of op korte termijn) maar die desondanks (vanwege de noodzaak tot het behouden van de functionaliteit) in de transitie worden meegenomen. Ten aanzien van deze laatste categorie zijn er twee gangbare opties die Defensie hierin kan hanteren: Of er wordt extra geïnvesteerd in het inrichten van een goede '*landing zone*' voor de betreffende applicatie in de nieuwe data centers, waarbij er dus akkoord komt ten aanzien van mogelijke additionele (i.e. veelal hogere) kosten, of men verkiest de 'minimale' variant waarbij de business de keuze maakt om een dergelijke applicatie te migreren maar dat er geen aanvullende aanpassingen worden uitgevoerd om bv. een dergelijke applicatie op de gewenste RTO en / of RPO te krijgen. Gartner adviseert Defensie om hiervoor een zogenaamde *Risk Acceptance Agreement*-cyclus in te richten.
- **AM5:** Monitor gedurende de transitiefase continue de gehanteerde planning, in samenspraak met de architectuurfunctie (onder meer vanuit rolgroep binnen de regiefunctie).

6.5 Financiele consequenties

- **FC1:** Opstellen van een kostencalculatiemodel voor de voorziene transitie gedurende periode 2015-2020. Hierbij moet onder andere rekening worden gehouden met de transitie- en transitiekosten, gedeeltelijke dubbele beheerlast, kosten t.a.v. regievoering en toegenomen investeringen voor vernieuwing en innovatie. Het kostencalculatiemodel moet meerdere scenario's uitwerken (b.v. Do Nothing, volledig HLO binnen vijf jaar, HLO stapsgewijs realiseren met verschillende plateaus, etc.) voor besluitvorming. Daarnaast moet elk scenario worden voorzien van een risicoanalyse om financiële baten en lasten af te wegen tegen het risicoprofiel.
  - Exploitatielasten oude omgeving:
    - Infrastructuurdomeinen;
    - Applicatiedomeinen.
  - Bouw data center en transitiekosten nieuwe omgeving;

- ❑ Transitiekosten applicaties (oud naar nieuw);
- ❑ Applicatie-rationalisatiekosten;
- ❑ Exploitatielasten nieuwe omgeving;
- ❑ Kosten voor vernieuwing en innovatie;
- ❑ Kosten voor het opbouwen van de regiecompetentie.

Bijlagen

Bijlage A: Analyse principes IT-infrastructuur

Principes Data Center

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
DC.1 Mix van workloads met verschillende servicelevels	◕	◕	Ja – in context plaatsen	DC.1B moet SMART worden uitgewerkt en in de juiste context worden geplaatst; 100% beschikbaarheid en 0 RPO zijn onrealistisch c.q. zeer duur te realiseren. DC1.A en DC1.B missen in de consequenties eisen aan netwerk latency en bandbreedte *binnen* het DC (zeer belangrijk voor Big Data en scale-out toepassingen)
DC.2 Veilig samenwerken in snel wisselende verbanden	◑	◑	Ja	DC2A. Encryptie is breder dan enkel het gebruik van VPN. Naast fysieke beveiliging van de DC locaties zijn ook maatregelen nodig om alle devices waarop data lokaal opgeslagen mag worden afdoende te beveiligen (endpoint protection is nergens benoemd) DC2.B Fysieke scheiding LGI en HGI heeft ook gevolgen voor fysiek ontwerp DCs; dit is niet benoemd (LGI data mag in defensie DC → zo ja, heeft dit gevolgen voor het fysieke ontwerp van betreffende DC, omdat duidelijk moet zijn wat allemaal fysiek gescheiden moet zijn (bijv. of dit gaat ook om binnenkomend netwerk, stroomvoorziening etc.)
DC.3 Rapid Datacenter deployment	◔	◑	Ja	DC3.A spreekt enkel van server templates; gevirtualiseerde infrastructuur kent ook gevirtualiseerde storage (template voor een virtuele HD) en zelfs netwerken DC3.B Effect is te vaag geformuleerd om richtinggevend te zijn. Wat is "meekijken"?

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
DC.4 Scale-out toepassingen hebben voorkeur	◑	◑	Ja – in context plaatsen	Niet als principe voor de gehele infra maar alleen voor specifieke apps DC4.A: welke Tier definitie geldt hier? Uptime institute, net als bij DC4.B? Consequenties voor netwerk latency tussen de DCs zijn niet benoemd Consequenties voor applicaties (Active-Active te moeten kunnen draaien) zijn niet benoemd DC4.C DC4.D dient te verwijzen naar data rubricering om zo een geschikte locatie voor de off-site back-up eenduidig te kunnen bepalen (een Rijks ODC is bijv. voor LGI mogelijk, voor HGI niet)
DC.5 Autonoom werken in het veld	●	●	Ja	Geen opmerkingen
DC.6 Opslag, analyse en verwerking van grote hoeveelheden gestructureerde en ongestructureerde data (big data) van diverse sensoren, zowel in statische omgevingen als in het veld, moet mogelijk zijn	◕	◕	Ja	DC6.B spreekt van opslag van data in origineel formaat. Voor duurzaamheid mist een periodieke herijking van het opslagformaat en evt. aanpassen ervan a.d.h. ontwikkelingen in techniek/vervangen data formaten

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
DC.7 Defensie private cloud en groei naar hybride cloud			Ja, maar in context plaatsen	Cloud heeft vijf karakteristieken, waarvan drie niet benoemd worden: ▪ Resource pooling ▪ Measured service (i.e. usage-based payment) ▪ Broad network access Daarnaast is niet uitgewerkt wat de consequenties zijn van deze infrastructuurinrichting voor die applicaties die niet verCloud kunnen worden Effect op de organisatie (wie is de cloud broker) is niet benoemd als consequentie
DC.8 Modulaire Datacenters			Ja	DC8.A houdt geen rekening met de "oude", mogelijk niet te virtualiseren werklasten. DC8.B Uitleg dient aangescherpt te worden. indien de bouwblokken gezien dienen te worden als verschillende gevirtualiseerde diensten (IaaS, PaaS), is het mogelijk om deze in verschillende "maten" standaard aan te bieden. Het principe maakt onvoldoende duidelijk wat een "bouwblok" is. DC8.D benoemt geen consequentie van de temperatuurkeuze voor de keuze van fysieke apparatuur (die moet bij de gestelde temperaturen kunnen functioneren)

Principes Werkplek

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
WA.01 IT functionaliteit wordt vanuit een te personaliseren portal aangeboden aan de gebruiker.			Deels – ook apps-gedachtelijn	Wellicht teveel focus op Portaal-gedachte. Dit zal voor slechts een gedeelte van de functionaliteit gelden. Functionaliteit dient ook toegankelijk te zijn zonder internetverbinding (bv. via apps.)
WA.02 Presentatie en invoer van gegevens op maat voor gebruik en device			Ja, maar in context plaatsen	Onvoldoende richtinggevend. Dit principe zal voor een groot gedeelte van de applicaties niet van toepassing zijn.
WA.03 Het applicatie portfolio is maximaal onafhankelijk van rubricering en gebruiksomstandigheden			Ja, maar in context plaatsen	Het gebruik (en of dit mogelijk is) van de applicatie is afhankelijk van de gebruiksomstandigheden (tijd, plaats en context)
WA.04 Het applicatie portfolio is maximaal inzetbaar voor diverse doelgroepen			Aanpassen	Titel principe dekt niet de inhoud, echter standaardisatie en consolidatie van functionaliteit is een goed principe. Inhoud leest: "reuse before buy before build"
WA.05 De werkplek biedt mogelijkheden voor digitale samenwerking in een federatieve context			Ja	Te gericht op een extranet; verlenen van toegang tot eigen applicaties/samenwerkingsruimte op basis van federatief erkende partneridentiteit is niet uitgewerkt
WA.06 Gebruik cloud aware applications			Ja, maar in context plaatsen	Het ver-Clouden van de gehele applicatie portfolio is niet nodig. Het principe is daarmee onvoldoende richtinggevend

Gartner

Principes Devices

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
WD.01 Any Place, Any Time, Any Device	◑	◔	Ja, maar in context plaatsen	Toegang tot bepaalde functionaliteit of data zal afhangen van het device. Dit moet beter worden gecontextualiseerd. Gespannen relatie met WD.03 en WD.07 (BYO apps)
WD.02 Draadloos, tenzij…	◕	◔	Ja, maar in context plaatsen	Draadloos geldt met name voor de specifieke toepassingen wanneer draadloos gewenst is (denk ook aan 3G / 4G).
WD.03 Devices hebben een digitale identiteit	◕	◔	Ja, maar in context plaatsen	Gespannen relatie met WD.01. Moet elk device bekend zijn of niet? Consequenties voor security en Mobile Device Management onvoldoende beschreven.
WD.04 Users hebben een digitale identiteit	◑	◑	Ja	Beperkte diepgang in de uitwerking van het principe (2-factor authenication).
WD.05 Het device portfolio is ingericht op het principe van managed diversity.	◑	◔	Gedeeltelijk	Defensie streeft naar een minimaal aantal devices per gebruiker (kleine footprint). Voor Defensie-beheer maar vanuit gebruikersperspectief juist meerdere devices?
WD.06 Papierloos werken (kantoor)	◕	◔	Onvoldoende beschreven	Consequenties zijn onvoldoende beschreven (b.v. e-Signature, automatische workflows)
WD.07 Defensie optimaliseert continu de weerstand tegen cyber aanvallen	◑	◔	Onvoldoende beschreven	Onvoldoende uitgewerkt wat hier de implicaties van zijn (ophouden ondersteuning, managed devices, beperkingen op BYOD / CYOD, …)
WD.08 Always connected, tenzij…	◑	◑	Gedeeltelijk	Staat haaks op web-based toegang tot functionaliteit. Bij wegvallen connectie zal data opgeslagen moeten worden

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Principes Netwerk

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
NW.1 Netwerk ondersteunt draadloze devices	◔	◔	Ja	In de huidige vorm is de toegevoegde waarde van het principe nihil
NW.2 Al het dataverkeer is vercijferd	◕	◑	Ja, maar in context plaatsen	Checken of dit een valide principe is of dat dit leidt tot veel additionele rekencapaciteit en snelheidsverlies. Op gespannen voet met BYOD
NW.3 Het netwerk brengt overal IP	●	●	Ja	Geen opmerkingen
NW.4 Adhoc netwerk concept voor MUT omstandigheden	◕	◔	Ja	Principe biedt weinig inzicht in de consequenties
NW.5 Netwerk ondersteunt last IT standing	◕	◔	Ja, maar in context plaatsen	Consequenties dienen duidelijker te worden uitgewerkt
NW.6 Netwerk voor veilige communicatie op elke locatie en voor elk niveau van rubricering en met elke partner buiten Defensie	◕	◑	Gedeeltelijk	Toetsen – onduidelijk principe. Er kan ook worden uitgegaan van dat het netwerk per definitie onveilig is. Wat is de toegevoegde waarde als data zelf wordt versleuteld?
NW.7 Authenticatie en autorisatie voor elk device	◕	◔	Gedeeltelijk	Spanningsveld met BYOD.
NW.8 Het IP-netwerk is "transmissie agnostisch"	◔	◑	Gedeeltelijk	IP-netwerk is in principe protocol onafhankelijk (los van laag 1-2). Dient verder te worden uitgewerkt

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Gartner

Principes Telecommunicatie

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TC.1 Eén geïntegreerde communicatie functionaliteit	◑	◔	Ja, maar in context plaatsen	Te algemeen als principe. Differentieert bijv. niet naar MUT omstandigheden (capaciteit)
TC.2 Ondersteuning any place en any device	◕	◑	Ja	Consequenties verder detailleren
TC.3 HGI heeft eigen middelen voor communicatie	◑	◑	Ja, maar in context plaatsen	HGI stelt andere eisen – onduidelijk of dit ook andere middelen moeten zijn dus (fysiek) gescheiden netwerken. Consequentie onvoldoende uitgewerkt
TC.4 De identiteit van gebruikers van communicatiemiddelen moet beschermd kunnen zijn	◑	◔	Gedeeltelijk	Tegenstrijdig met gebruik 3/4G netwerken en/of BYOD
TC.5 Specifieke communicatiefunctionaliteit bij MUT omstandigheid	◑	◑	Gedeeltelijk	Is niet geformuleerd als principe
TC.6 Waar nodig gebruik maken van eigen mobiele netwerken	◑	◔	Onduidelijk	Niet duidelijk beschreven. Wat is de relatie met HGI en LGI? Relatie van ITSM en NIST met principe onduidelijk.

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Principes Beheer

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
BH.1 Gebruikers worden ondersteund via selfservice	●	●	Ja	Geen opmerkingen
BH.2 Beheer is voor de LGI- en de HGI-ketens ingericht volgens dezelfde processen	●	●	Ja	Geen opmerkingen
BH.3 Lifecycle management is ingericht voor elke IT-dienst	◕	◑	Ja	Bij consequenties dienen ook organisatie consequenties te worden benoemd: oude infra en applicaties houden de "oude" organisatie. IT moet een functie bevatten die te "oude" en "nieuwe" wereld met elkaar laat samenwerken, zolang dit nodig is
BH.4 Lokaal beheer in OMUT omstandigheden	◑	◑	Ja	Principe is onvoldoende uitgewerkt. Heeft nl. organisatorische consequenties (uitzenden van beheerders)
BH.5 Geautomatiseerd beheer met moderne tooling	◕	◕	Ja – specifieker maken	Er worden veel verschillende aspecten behandeld binnen dit principe

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Principes Beveiliging

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
BE.1 Alle Defensiemedewerkers hebben een persoonsgebonden gebruikersaccount, gebaseerd op de Basisadministratie Digitale Identiteit Defensie	●	●	Ja	Geen opmerkingen
BE.2 Defensie vertrouwt het identiteitsbeheer van vertrouwde partners waarmee Defensie federatief samenwerkt.	●	●	Ja	Geen opmerkingen
BE.3 Handelingen die worden uitgevoerd op platforms en toepassingen kunnen naar een natuurlijke persoon worden herleid	◕	◑	Ja	De consequentie van deze formulering is dat informatie uit sensoren dus niet automatisch opgehaald kan worden door S2S koppeling – maak onderscheid tussen sensor en applicatie
BE.4 Fysieke en logische toegangsbeveiliging zijn geïntegreerd	◑	◑		Niet geheel duidelijk wat hier wordt bedoeld – nadere uitleg benodigd
BE.5 Autorisaties volgen taakstelling en bedrijfsvoering	●	●	Ja	Geen opmerkingen

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
BE.6 IT infrastructuur is ontworpen op basis van de uitgangspunten 'Security by Design', ' Defence in Depth' en 'Diversity in Defence'	◑	◑	Gedeeltelijk	Worden meerdere aspecten van beveiliging behandeld binnen dit principe. Consequenties en uitleg onvoldoende duidelijk (mist o.a. consequenties voor inkoop van apparatuur en BYOD)
BE.7 De beveiligingsfuncties stellen het beveiligen van de data centraal	●	●	Ja	Geen opmerkingen
BE.8 Integrale geautomatiseerde en meetbare (Cyber) Situational Awareness over alle informatiedomeinen en IT infrastructuur heen	●	●	Ja	Geen opmerkingen
BE.9 In de IT infrastructuur worden voor kritische beveiligingsfuncties producten met gekende kwaliteit ingezet	◕	◑	Ja, maar uitwerken	Onvoldoende specifiek (welke standaarden en/of kwaliteitseisen?)

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Bijlage B: Analyse principes IT-toepassingen

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.01 IT-toepassingen zijn geschikt voor tijd-, plaats-, en device-onafhankelijk werken.	◕	◑	Ja, verdere uitwerking benodigd	Consequenties voor huidige systemen niet uitgewerkt. Consequenties voor (on)beschikbaarheid HGI informatie dienen duidelijker te worden verwoord
TP.02 De interactie tussen mens en systeem (userinterface) is afgestemd op de taak van de gebruiker of de rol in een proces en lijkt zoveel mogelijk op wat de medewerker op basis van marktproducten ook gewend is.	◑	◔	Gedeeltelijk, dient verder te worden uitgewerkt	Welke "gebruiksstandaarden van de consumentenmarkt" worden concreet bedoeld? Meegenomen dient ook te worden dat de "herkenbare" UIs tussen verschillende platformen (Win/iOS) verschillen in look&feel
TP.03 Er is een beperkte mate van keuzevrijheid mogelijk voor de medewerker bij de interactie met IT-toepassingen.	◑	◑	Gedeeltelijk, dient verder te worden uitgewerkt	Kop principe sluit niet aan bij uitleg (interactie met IT toepassing is iets anders dan keuzevrijheid van beschikbare IT toepassingen)
TP.04 Medewerkers beschikken over een uniforme digitale werkruimte.	◑	◔	Ja, verdere uitwerking benodigd	Marktconform is eerder het omgekeerde: de digitale werkruimte past zich aan a.d.h. van verschillende geïdentificeerde persona's. De uitleg lijkt zich vooral te richten op de "basisruimte" die gelijk dient te zijn. Consequenties voor netwerk (beschikbaarheid, bandbreedte) zijn niet beschreven
TP.05 Alle Defensiemedewerkers krijgen een persoonsgebonden gebruikersaccount	◕	◑	Ja	Consequentie van de logging van alle activiteiten niet beschreven (effect op performance, storage etc.) Effect en principe hebben weinig met elkaar te maken

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.06 Medewerkers beschikken over een digitale uitrusting.	◑	◑	Onduidelijk	Principe heeft weinig toegevoegde waarde Uitleg mist een expliciete verwijzing naar TP.01 en TP.07
TP.07 Basis voor het toegangsbeleid (access management) voor de IT-toepassingen is "role based access" en "context based acces".	◕	◔	Ja	Uitleg is prima. Consequenties voor bestaande systemen zijn niet benoemd. Rationale: "rollen dienen overdraagbaar te zijn" is een sine qua non van IAM: een rol dient generiek te zijn gedefinieerd zodat de rol aan meerdere personen toegekend kan worden
TP.08 Commandovoeringssystemen ondersteunen alle missies.	◑	◔	Gedeeltelijk, dient verder te worden uitgewerkt	Uitleg mist expliciete verwijzing naar MUT situaties. Consequenties voor bestaande systemen zijn niet benoemd De zin "De hiervoor gebruikte IT toepassingen … en dienen als functionaliteit integraal te zijn" is onduidelijk

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Gartner

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.09 De IT-toepassingen brengen mensen veilig met elkaar in verbinding	◑	◑	Ja	Consequentie is ook dat het Defensie IVB beleid voorrang conform de NAVO FMN standaarden is/wordt ontwikkeld. Dit is nu enkel impliciet benoemd (vanwege FMN-conform labeling van informatie) maar moet expliciet benoemd worden, ook in de Security principes (is nu nog niet het geval). Veilige verbinding van mensen met sensoren/onbemande wapensystemen?
TP.10 IT-toepassingen zijn geschikt om informatie te delen en te integreren.	●	◔	Ja	Uitleg prima. Consequenties voor bestaande systemen niet uitgewerkt.
TP.11 De beveiliging van IT (infrastructuur en toepassingen) is afhankelijk van het afbreukrisico	◑	◔	Gedeeltelijk, dient verder te worden uitgewerkt	Principe is te algemeen geformuleerd om richtinggevend te zijn. Wat is de voorrang van de verschillende beveiligingsnormen? Wanneer wordt niet voldaan aan "toegankelijkheid, vindbaarheid, uitwisselbaarheid, betrouwbaarheid, authenticiteit en volledigheid"? → hiervoor is definitie van deze termen nodig, vooral betrouwbaarheid, authenticiteit en volledigheid Locatie en context dienen mede bepalend te zijn voor beveiligingseisen

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.12 Het landschap van IT-toepassingen ondersteunt alle vormen van operationele inzet.	●	●	Ja	Geen opmerkingen. Rationale goed uitgewerkt
TP.13 Het landschap van IT-toepassingen van Defensie is een hybride landschap.	◔	◔	Nee	Elk IT landschap is hybride (i.e bestaand uit meerdere systemen), dit is een open deur. Principe heeft weinig toegevoegde waarde. Relatie met de business effect onduidelijk
TP.14 De hybridestructuur werkt voor Defensie-brede processen als één samenhangend stelsel voor de informatievoorziening.	◕	◕	Ja, aanpassing benodigd	End-to-end procesondersteuning is een gegeven. Uitleg LGI/HGI integratie is goed Alternatieve titel: "Het totale applicatielandschap van Defensie werkt voor Defensie-brede processen als één samenhangend stelsel voor de informatievoorziening" dekt de lading beter
TP.15 De herkomst van de IT-toepassingen is divers.	◔	◔	Nee	Dit is geen principe, maar een gegeven. Principe heeft weinig toegevoegde waarde.
TP.16 Voor veranderingen van IT-toepassingen geldt 'geen maatwerk'.	◕	◑	Ja	Rationale geeft goed uitleg. Volgorde van voorkeur kan verschillen per capability.
TP.17 Stamgegevens worden eenmalig opgeslagen en meervoudig gebruikt.	◑	◔	Ja, aanpassing benodigd	Zoals geformuleerd ondersteunt dit principe MUT niet. De consequenties daarvan zijn niet uitgewerkt (bijv. dat lokaal opslag van bepaalde gegevens onder bepaalde omstandigheden nodig zal zijn). In tegenspraak met TP.20

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.18 De IT-toepassingen garanderen adequate informatiebeschikbaarheid voor commando-voering.	◑	◑	Ja, aanpassing benodigd	Rationale is niet duidelijk (voor niet-defensie specialisten) Zie TP.22
TP.19 Commandovoeringssystemen ondersteunen een continu en ononderbroken proces.	◑	◕	Ja, aanpassing benodigd	Rationale: idem als TP.18 Zie TP.22

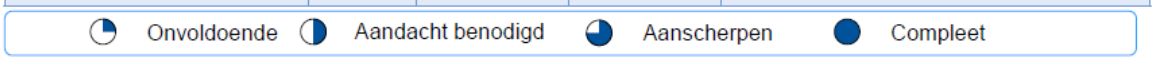
◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.20 IT-toepassingen zijn geschikt om wereldwijd informatie uit te wisselen via gangbare militaire of publieke communicatiemiddelen.	●	●	Ja	Rationale geeft goed uitleg Geen opmerkingen
TP.21 IT-toepassingen zijn geschikt om statisch, ontplooid, mobiel, uitgestegen en te voet beschikbaar te worden gesteld (SOMUT).	●	◑	Ja	Rationale geeft goed uitleg Consequenties voor huidige systemen niet benoemd
TP.22 Commandovoeringsystemen vormen een gesloten keten.	●	●	Ja	Geen opmerkingen Rationale is duidelijker verwoord dan bij TP.18 en TP.19
TP.23 Commandovoeringssystemen voldoen aan alle gebruikersomstandigheden.	◑	◑	Ja, overlap adresseren	Overlap met TP.22

◔ Onvoldoende ◑ Aandacht benodigd ◕ Aanscherpen ● Compleet

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.24 IT-toepasssingen zijn geschikt om met grote hoeveelheden gegevens om te gaan.			Ja, aanpassing benodigd	Uitleg is goed; echter de kop suggereert dat alle IT Toepassingen met grote hoeveelheden data moeten kunnen omgaan - wat niet waar is volgens de uitleg. Rationale is onduidelijk. Er wordt onderscheid gemaakt tussen opslag "bij de bron" en "bij Defensie"; waarmee waarschijnlijk een onderscheid tussen "decentraal bij de bron" en "centraal bij Defensie" bedoeld wordt

Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.25 Nieuwe delen van IT-toepassingen zijn modulair, schaalbaar en aanpasbaar (designed to change)			Ja	Moet beter worden uitgelegd in de context van de verschillende business capabilities. Verdergaande eisen aan schaalbaarheid en aanpasbaarheid zijn niet altijd van toepassing.
TP.26 Voor veranderingen in het landschap van IT-toepassingen geldt het principe 'kleinschalig en kort-cyclisch'.			Nee	Dit principe zal voor een gedeelte van de applicaties niet van toepassing zijn; verandersnelheid is afhankelijk van de *pace layer*. Rationale zoals geformuleerd heeft een ongewenst effect op voorspelbaarheid van projectportfolio (geen vaste ontwikkelrichting)
TP.27 Het systeemlandschap van de toekomst is een enabler voor innovatie.			Gedeeltelijk	Te algemeen om goed richtinggevend te zijn. Biedt wel de mogelijkheid om *pace layering* van het landschap expliciet te benoemen. Consequenties voor bestaande applicaties zijn niet benoemd.
TP.28 Nieuwe delen van IT-toepassingen maken gebruik van scheiding tussen presentatie, logica en data-laag, tenzij de standaard logica in een IT-toepassing is gebaseerd op best practices.			Ja, aanpassing benodigd	Hoe worden de standaard-toepassingen hieraan getoetst?
TP.29 Bij de selectie van nieuwe IT-toepassingen geldt 'buy before make'.			Overlap	Principe overlapt met TP.16



Eisen aan IT	Uitleg en rationale	Consequenties	Marktconform	Opmerkingen
TP.30 Nieuwe delen van IT-toepassingen dienen schaalbaar te zijn m.b.t. resources van onderliggende IT-infrastructuur.			Ja, dient worden aangepast	Zal niet voor alle toepassingen even noodzakelijk zijn, echter het feit dat applicaties binnen een gevirtualiseerde infrastructuur moeten kunnen functioneren is een goed principe.
TP.31 Nieuwe delen van IT-toepassingen zijn geschikt om te worden aangeboden aan gebruikers volgens het principe SAAS (software as a service).			Nee, dient te worden ge-contextualiseerd	Uitleg is verwarrend: "Gebruikers benaderen IT-toepassingen via internettoepassingen en Cloud-technologie". Wordt hiermee bedoeld dat gebruikers de IT-toepassingen via **internet technologie** benaderen? Dat is een van de Cloud karakteristieken (zie NIST definitie) Dit principe zal voor een gedeelte van de applicaties niet van toepassing zijn; het ver-SaaSen van de gehele applicatie portfolio is niet nodig. Het principe is daarmee onvoldoende richtinggevend

Bijlage C: Referenties naar de vraagstellingen

Business effecten	Paragraaf
Zijn de business effecten met bijbehorende doelstellingen richtinggevend om projecten/trajecten te definiëren?	Paragraaf 2.1
Kan Defensie met de business effecten met bijbehorende doelstellingen een methodiek ontwikkelen om kort-cyclisch en incrementeel te innoveren?	Paragraaf 2.1
Architectuur	
Is de architectuur richtinggevend op ontwikkelingen in de ICT infrastructuur? En is sprake van samenhangende componenten in de architectuur? Waar zijn verbeteringen nodig en welke zijn dat?	Paragraaf 2.2
In welke mate sluit de voorgestelde architectuur aan op de markt? Welke zaken zijn te betitelen als commodity en wat is in de toekomstige situatie Defensie specifiek?	Paragraaf 2.2
In welke mate worden de beveiligingseisen adequaat afgedekt binnen de architectuur gegeven de business eisen?	Paragraaf 2.2
Kaders	
Zijn de geïdentificeerde business eisen voldoende helder vertaald in kaders aan de ICT infrastructuur? Welke gebieden kunnen aangescherpt worden?	Paragraaf 2.2
Zijn de geïdentificeerde kaders voor de ICT voldoende helder en dragen deze bij aan de invulling de nieuwe IT infrastructuur? Welke gebieden kunnen aangescherpt worden?	Paragraaf 2.2
IT Applicaties visie	
Is het ontwerp van de ICT-infrastructuur een geschikte basis om de volgende ontwikkelingen op het gebied van IT-applicaties te ondersteunen: A. Het doorontwikkeling en exploitatie van Defensie-brede transactie verwerkende systemen (zoals ERP) B. Het introduceren van service georiënteerde architectuur binnen Defensie die gekoppeld wordt met de transactie-verwerkende systemen. C. Het ondersteunen van het grootschalig verzamelen van gegevens (Big data) en het systematisch analyseren van deze data. D. Het ondersteunen van logisch gecentraliseerde gegevensverzamelingen (basisadministraties) met stamgegevens.	Paragraaf 2.3

E. Het voortdurend en kort-cyclisch innoveren van het applicatielandschap om aan te sluiten bij ontwikkelingen zoals *serious gaming* en simulatie. F. Het ontsluiten van applicaties via moderne, op de gebruiker afgestemde platforms, zoals mobiele devices en een gebruikersportaal. G. Het integreren van social media in de samenwerking van medewerkers. H. Het uitwisselen van gegevens met partners van Defensie, waarbij rekening wordt gehouden met de rubricering van deze gegevens. I. Het toepassen van Cloudoplossingen om gegevens te delen.	
Sourcing	
Sluiten de kavels zoals genoemd in de herijking sourcing voldoende aan bij het high level ontwerp? Kan de sourcing voldoende bijdragen aan de genoemde doelstellingen en principes uit het high level ontwerp?	Hoofdstuk 3.0
Geeft de verkaveling en het ontwerp voldoende ruimte voor marktpartijen om (deel)oplossingen optimaal te kunnen ontwikkelen? Is het ontwerp stringent genoeg dat deze (deel)oplossingen aansluiten op de ambitie en doelstellingen van Defensie? Welke kavels zouden verder opgesplitst kunnen worden, welke aangescherpt en welke samengevoegd?	Hoofdstuk 3.0
Biedt de gekozen insteek in sourcing voldoende flexibiliteit om stapsgewijs mee te groeien in de veranderende context van Defensie en de technologische ontwikkelingen? Welke verbeteringen en aanpassingen in de sourcing zou u voorstellen?	Hoofdstuk 3.0
Is in de herijking van de sourcing voldoende rekening gehouden met de (ervaring van Defensie) inzake regievoering en kan Defensie het implementatiepad van het high level ontwerp volgen middels aansturing van marktpartijen?	Hoofdstuk 3.0
Algemeen	
Welke kansen en risico's kunnen aanvullend zich voordoen bij het realiseren van het voorgestelde ontwerp? Welke maatregelen moet Defensie nemen om deze te borgen.	Hoofdstuk 4.0
Is de volgorde van ontwikkeling van de ICT infrastructuur in de gepresenteerde roadmap een logisch groeipad? Waar zijn andere prioriteiten gewenst?	Paragraaf 2.3
Welk deel van de huidige ICT infrastructuur moet op niveau worden gebracht (geen totaal nieuw concept) zodat het past binnen de nieuwe ICT-infrastructuur en voldoet aan de ambitie en doelstellingen van Defensie?	Paragraaf 2.3

In het ICT assessment is gekeken naar de benodigde expertises en tooling voor het beheren van de voorgestelde ICT Infrastructuur. Geeft het ontwerp voldoende ruimte voor het invullen van de benodigde verbeteringen van het beheer (invulling processen en tooling)? Welke conclusie kan worden getrokken over de benodigde expertise voor beheer bij de geschetste ICT infra in termen van kwaliteit en kwantiteit?	Paragraaf 2.3
Geef een indicatieve begroting van de diverse elementen van het high level ontwerp ICT infra.	Hoofdstuk 5.0

Any questions regarding this Report should be addressed to:

Peter Kivits
Managing Partner
Gartner Nederland BV

Gartner