Ministerie van Defensie

GrIT Grensverleggende IT

Basisrapportage 2022

Inhoud

Managementsamenvatting

Voor u ligt de basisrapportage van het programma Grensverleggende IT (GrIT). Het programma kent een aanloop sinds 2014. Inmiddels is het contract getekend en is een, voor Defensie, unieke samenwerking met de markt aangegaan. Nadat er tijd is uitgetrokken om deze samenwerking goed vorm te geven, zijn nu de eerste blokken van GrIT in ontwikkeling en verloopt het programma zoals verwacht. Door middel van deze basisrapportage wordt u geïnformeerd over de achtergrond, opzet en de governance van het programma, als mede over de voortgang van het programma in het eerste jaar.

Naast de verschijning van deze basisrapportage, ontvangt u ook de eerste voortgangsrapportage, deze beslaat de periode van 1 januari 2022 tot en met 30 juni 2022. Vervolgens worden de voortgangsrapportages halfjaarlijks met uw Kamer gedeeld, de voorjaarsrapportage voor 1 april en de najaarsrapportage voor 1 oktober. De rapportages zullen dezelfde opbouw hebben als het voortgangshoofdstuk in deze basisrapportage. Ook zullen dezelfde figuren gebruikt worden om bijvoorbeeld de voortgang in de realisatie weer te geven. Deze consistentie maakt het voor uw Kamer mogelijk de voortgang te volgen gedurende de looptijd van het programma. De actualiteit, juistheid, volledigheid en consistentie van de informatie in deze rapportages wordt gewaarborgd door een brede reviewlijn en een controle van de Auditdienst Rijk (ADR). Daarnaast zal de ADR jaarlijks een accountsrapport schrijven.

1 Inleiding

Het programma Grensverleggende IT (GrIT) is op 22 januari 2021 door de Tweede Kamer aangewezen als groot project. Dat betekent dat er conform de Regeling Grote Projecten wordt gerapporteerd. De uitgangspuntennotitie[1] vormt, met de Regeling Grote Projecten, de leidraad voor de basisrapportage en periodieke voortgangsrapportages. In de basisrapportage worden de uitgangspunten en de afspraken bij de start van het programma toegelicht, wordt er een overzicht gegeven van wat het programma inhoudt en wordt de voortgang in 2021, het eerste jaar van de realisatie van GrIT, beschreven. Deze basisrapportage is het fundament voor de toekomstige voortgangsrapportages over GrIT en is gebaseerd op Plan A' inclusief de business case (in dit document samen aangeduid als 'de business case'). Deze voortgangsrapportages zal de Tweede Kamer elk half jaar ontvangen, voor 1 april en voor 1 oktober. In de voortgangsrapportages worden de mutaties en de actuele stand van zaken ten opzichte van de vorige rapportages gedeeld.

De basis voor de voortgangsrapportage is de business case die eerder vertrouwelijk met de Tweede Kamer is gedeeld (Kamerstuk 35 728, nr. 2). Een deel van de informatie is commercieel vertrouwelijk, met name omdat de financiële informatie de marktpositie en eventuele onderhandelingsruimte van het ministerie van Defensie schetst. Openbaring hiervan kan de onderhandelingspositie in eventuele toekomstige aanbestedingstrajecten schaden. Deze elementen zijn daarom opgenomen in een separate commercieel vertrouwelijke bijlage.

De achtergrond en aanleiding van GrIT zijn in hoofdstuk 2 beschreven. Het programmadoel en de governance worden in hoofdstuk 3 nader toegelicht. In hoofdstuk 4 wordt de aanpak, de planning en de kosten zoals eerder beschreven in de business case van GrIT geschetst. Hoofdstuk 5 beschrijft de voortgang van de realisatie van de blokken in 2021. In bijlage A van dit document is een toelichting op alle blokken opgenomen en bijlage B bevat de lijst met afkortingen.

[1] De uitgangspuntennotitie groot project Grensverleggende IT is vastgesteld op de procedurevergadering van de vaste commissie voor Defensie van 9 december 2021.

2 Achtergrond en aanleiding

2.1 Historie

In 2014 is de Tweede Kamer geïnformeerd over de uitkomsten van een rapport naar de staat van de IV/ICT van Defensie. Hierin werd geconcludeerd dat de IV/ICT ondermaats was en dat het risico op uitval te groot was (Kamerstuk 31 125, nr. 34). Naar aanleiding hiervan is het programma GrIT geïnitieerd. Op basis van BIT-adviezen (Kamerstuk 31 125, nr. 104 en 115) is de opzet en planning van het programma herzien en nader uitgewerkt. Eind 2020 is het contract met een extern consortium gesloten. Ook zijn er in een heroverwegingstraject twee hoofd-scenario's gedefinieerd en is er op basis van een afwegingskader de keuze gemaakt voor één hoofdscenario (Kamerstuk 31 125, nr. 115). De definitieve business case is gedeeld met de Tweede Kamer (Kamerstuk 35 728, nr. 2). Hierop heeft de Tweede Kamer GrIT aangemerkt als groot project (Kamerstuk 35 728, nr. 1).

Op 1 januari 2021 is de realisatiefase van het programma GrIT gestart. De realisatie zal conform planning eind 2027 zijn afgerond. Over de voortgang is tot nu toe middels het Defensie Projectenoverzicht en de afwijkingsrapportages op het Defensie Projectenoverzicht gerapporteerd.

2.2 Doel en baten van het programma

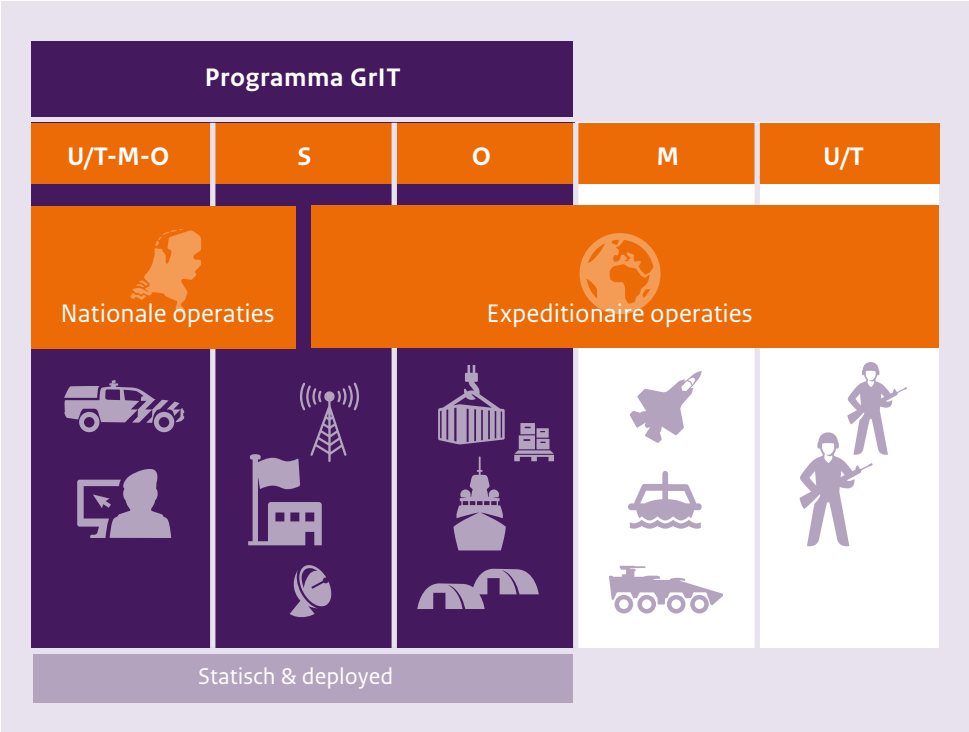
Met GrIT vervangt en vernieuwt Defensie een groot gedeelte van de IT-infrastructuur. Defensie legt zo een solide fundament voor de vervanging en vernieuwing van het applicatielandschap waarmee de bedrijfsvoering wordt gemoderniseerd en de digitale slagkracht wordt vergroot. Defensie realiseert daarmee tevens het fundament voor informatiegestuurd werken en optreden, zoals opgenomen in actielijn 6 'informatiegestuurd optreden' van de Defensienota 2022. Defensiemedewerkers worden in staat gesteld sneller informatie te delen en te analyseren. Zij krijgen altijd en overal toegang tot dezelfde moderne en veilige werkomgeving en samenwerking met in- en externe partners (waaronder in EU- en NAVO-verband) wordt makkelijker door beveiligde gegevensuitwisseling. Deze baten worden gerealiseerd door de realisatie van deelprojecten, de zogenoemde blokken van het programma.

3 Wat is GrIT?

3.1 Scope van GrIT

In de context van snelle technologische ontwikkelingen en cyberdreigingen is het voor Defensie cruciaal te kunnen werken en handelen op basis vanuit de best mogelijke informatiepositie. Defensie realiseert het fundament hiervoor door de beschikbaarheid en veiligheid van de IT-infrastructuur voor internationale missies, nationale inzet, gereedstelling en reguliere werkzaamheden te verbeteren. Naast de IT-infrastructuur, is ook de migratie van de te behouden applicaties in scope (Migratie van de Keep Applicaties [MKA]). Zie paragraaf 4.1.4 voor een gedetailleerde uitwerking.

Met GrIT realiseert Defensie de IT-infrastructuur voor het zogeheten statische en ontplooide domein. In figuur 1 is dit visueel weergegeven met daaronder een nadere beschrijving van de verschillende domeinen.



Figuur 1 ***Scope GrIT***

De domeinen laten zich als volgt beschrijven:

- **Statisch (S)**: wijze van optreden vanuit vaste, niet verplaatsbare infrastructuren die voor lange(re) tijd worden gebruikt.
- **Ontplooid (O)**: wijze van optreden vanuit verplaatsbare infrastructuren waarbij het tijdens de verplaatsing van een infrastructuur niet mogelijk is om vanuit de betreffende infrastructuur door te werken.
- **Mobiel (M)**: wijze van optreden vanuit verplaatsbare infrastructuren waarbij het tijdens de verplaatsing van een infrastructuur wél mogelijk is om vanuit die infrastructuur door te werken.

- **Uitgestegen (U)**: wijze van optreden waarbij in de directe omgeving van een vaste of verplaatsbare infrastructuur wordt gewerkt.
- **Te voet (T)**: wijze van optreden waarbij in de directe omgeving geen vaste of verplaatsbare infrastructuur aanwezig is.

3.1.1 Kwalitatieve baten

Met GrIT worden de onderstaande zes kwalitatieve baten voor de defensieonderdelen gerealiseerd.

1. Business en mens staan centraal, IT sluit aan
De IT is ondersteunend aan de krijgsmacht. De geïndividualiseerde werkplek is intuïtief en toegang is apparaat-onafhankelijk, waardoor de gebruiker in verschillende omstandigheden optimaal kan werken. Technologische ontwikkelingen kunnen snel centraal worden doorgevoerd zonder apparaten te hoeven innemen.

2. De IT maakt veilig samenwerken in snel wisselende verbanden mogelijk
Door GrIT kunnen medewerkers eenvoudig en veilig samenwerken met grotere groepen via een mobiele of vaste werkplek, zowel binnen Defensie als met (EU- en NAVO-)partners.

3. IT is betrouwbaar en beschikbaar
Defensie heeft controle over en het eigendom van de vernieuwde IT-infrastructuur. Deze infrastructuur, inclusief de bijbehorende middelen, bevindt zich fysiek op defensieterreinen. De bedoeling is dat Defensie met haar IT altijd en wereldwijd kan optreden.

4. Met IT is Defensie 'wereldwijd *connected*'
Een robuuste infrastructuur betekent voor Defensie een basisvoorziening IT-infrastructuur die interoperabel is en altijd en overal werkt ter ondersteuning van de uitvoering van de grondwettelijke hoofdtaken, waar ook ter wereld en voldoet aan de defensie-eisen op het gebied van continuïteit, stabiliteit, veiligheid en efficiëntie.

5. De IT is geschikt voor het verwerken, opslaan en analyseren van zeer grote hoeveelheden informatie.
De nieuwe IT is geschikt voor decentrale en centrale informatieverwerking en zal deze verwerking dynamisch verdelen op basis van situatie en behoefte. Daarnaast stelt de nieuwe IT Defensie in staat om de grote hoeveelheden gegenereerde data nog steeds adequaat te archiveren en zo eenvoudiger en beter verantwoording af te leggen. Door de verbeterde informatieverwerkingscapaciteit zal Defensie in staat zijn een betere informatiepositie op te bouwen en effectiever te opereren.

6. De IT is eenvoudig en snel aanpasbaar
Het snel beschikbaar maken van IT is verankerd in alle lagen van de GrIT-architectuur. Vanuit een dienstencatalogus zijn IT-diensten eenvoudig aan te vragen. De nieuwe IT-infrastructuur is flexibel aan te passen aan externe en interne ontwikkelingen en is in staat om nieuwe behoeften en technologieën te ondersteunen. Hierdoor is het mogelijk om nieuwe technologieën te benutten en de IT-veranderingen te ondersteunen.

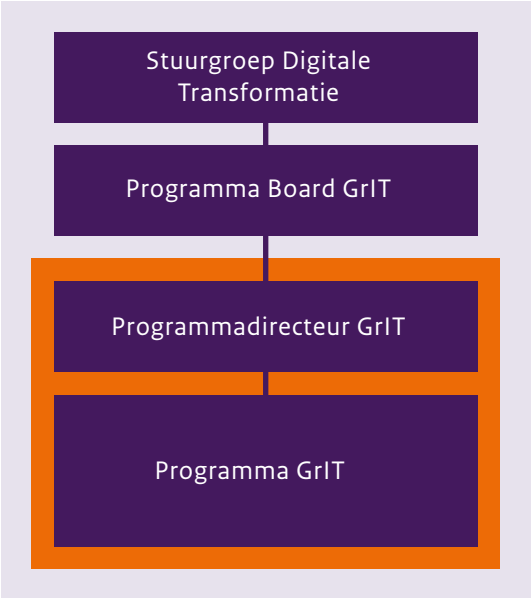
3.1.2 Kwantitatieve baten

Voor Defensie wordt meerwaarde gecreëerd in de vorm van een toekomstvaste, wendbare en flexibele IT-infrastructuur. Hoewel de exploitatiekosten van de nieuwe infrastructuur hoger zijn dan die van de huidige IT, wordt meer functionaliteit verkregen voor Defensie en voorkomt de overgang snel oplopende toekomstige kosten voor instandhouding van de oude infrastructuur. Door het vervangen en vernieuwen van de IT-infrastructuur kan een deel van

de huidige IT worden uitgefaseerd. De budgetten die hierdoor vrijkomen worden aangewend voor de exploitatie van de vernieuwde IT-infrastructuur. In hoofdstuk 4 en in de commercieel vertrouwelijke bijlage wordt hier dieper op ingegaan.

3.2 Governance GrIT binnen Defensie

Om de samenhang met de andere grote defensiebrede IT/BV-programma's te borgen en de beschikbare, schaarse capaciteit te verdelen, is voor de realisatieperiode een besturingsmodel ingericht. Deze nieuwe governance is gebaseerd op de adviezen van ABDTOPConsult [2], het Adviescollege ICT (AcICT, voorheen Bureau ICT-Toetsing, BIT) en de in opdracht van de CIO uitgevoerde evaluatie van de governance. De governance volgt het door AcICT genoemde drielagenmodel. De drie verschillende lagen zijn in figuur 2 schematisch weergegeven en worden hieronder toegelicht.



Figuur 2 ***Governance GrIT***

3.2.1 Stuurgroep Digitale Transformatie

Op het hoogste niveau vormt de bestuursraad samen met Defensie Materieel Organisatie (DMO) en Joint Informatievoorzienings Commando (JIVC) de stuurgroep Digitale Transformatie. De stuurgroep stuurt de digitale transformatie van Defensie aan, borgt de samenhang, neemt besluiten over de verdeling van schaarse capaciteit en neemt besluiten met een grote (financiële) impact. Door deze governance-inrichting kan ook de samenhang met andere grotere IT/BV-programma's, zoals Roger en Foxtrot, worden geborgd.

3.2.2 Programma Board GrIT

De Programma Board GrIT (PB), voorgezeten door de plaatsvervangend CDS, ziet toe op de uitvoering van het programma GrIT. Hiertoe monitort de PB de voortgang van het programma en stuurt deze waar nodig bij. De PB fungeert binnen Defensie als eerste escalatieniveau voor de programmadirecteur. De PB GrIT is gemandateerd om besluiten met een kleinere impact te nemen, om hiermee de stuurgroep Digitale Transformatie te ontlasten en het programma niet onnodig te vertragen.

[2] Zie het rapport 'Gescheiden Werelden'.

3.2.3 Programmaorganisatie GrIT

Defensie en het consortium hebben samen op het derde niveau de programmaorganisatie GrIT ingericht. De programmadirecteur stuurt de programmaorganisatie aan en heeft mandaat om binnen de afgesproken kaders besluiten te nemen. De programmadirecteur rapporteert aan de stuurgroep Digitale Transformatie en de PB GrIT en is eindverantwoordelijk voor de realisatie van GrIT.

3.2.4 Aansluiting staande organisatie

Het programma GrIT is gepositioneerd binnen DMO/JIVC. De programma-organisatie is verweven met de staande organisatie. Het consortium neemt deel aan diverse JIVC-overleggen, om de aansluiting van GrIT op de JIVC-organisatie te waarborgen. De programmadirecteur GrIT is lid van de directie van DMO/JIVC, waardoor de integratie van de huidige en nieuwe IT zijn geborgd. De vormgeving van de nieuwe JIVC-organisatie, in relatie tot de doorontwikkeling van GrIT, wordt in nauwe samenwerking met de medezeggenschap opgepakt. De governance van DMO/JIVC zelf valt buiten de scope van het programma GrIT en wordt daarom niet opgenomen in deze rapportage. In de overlegstructuren van het programma GrIT is aansluiting met DMO/JIVC geborgd. De ontwikkelingen van de organisatie zijn beschreven in paragraaf 5.9.

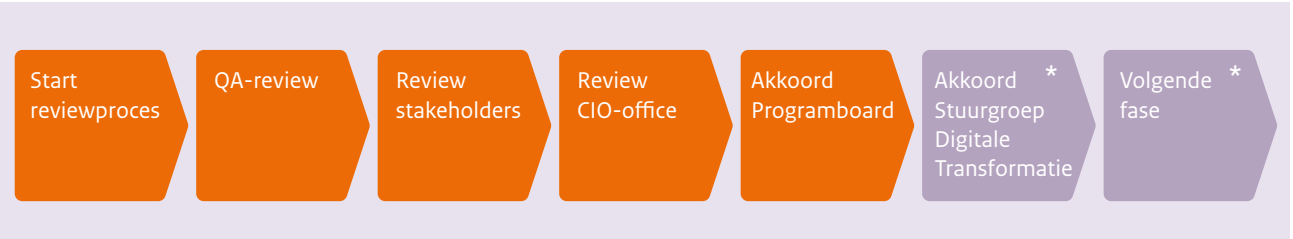
3.2.5 Toetsing en review

Voordat een blok gerealiseerd kan worden, worden de bijbehorende plannen enkele keren getoetst en gereviewd. Een door Defensie af te roepen blok begint met het opstellen van een initiatiedocument. Deze wordt, na de kick-off met onder andere de defensieonderdelen, geschreven door het programmateam en ondergaat een kwaliteitscheck door Quality Assurance (QA) GrIT. Daarna wordt deze gereviewd door de stakeholders, zoals de defensieonderdelen, en vervolgens getoetst door de CIO, alvorens deze wordt voorgelegd voor besluitvorming aan de PB en/of de stuurgroep Digitale Transformatie.

Als het initiatiedocument is goedgekeurd, volgt er een Ontwerp-Uitvoeringsplan Realisatie en een Defensie Activiteitenplan met een conceptversie van het Ontwerp-Uitvoeringsplan Terbeschikkingstelling. Het totstandkomingsproces volgt dezelfde stappen als het initiatiedocument. Daarna worden de stukken aangeboden aan de PB en de stuurgroep Digitale Transformatie.

Het Technisch Ontwerp wordt in het Strategisch Technologie Overleg besproken voordat deze definitief wordt gemaakt. De validatie van het Technisch Ontwerp vormt eveneens onderdeel van de besluitvorming door PB en de stuurgroep Digitale Transformatie.

Als laatste wordt er het definitief Ontwerp-Uitvoeringsplan Terbeschikkingstelling geschreven en aan de PB voorgelegd ter besluitvorming alvorens deze wordt besproken in de stuurgroep Digitale Transformatie. Ook dit document volgt de diverse toetsingen en reviews. Waar nodig kunnen derde partijen worden ingeschakeld om op specifieke blokken een review uit te voeren. In Kamerstuk 31 125, nr. 115 is een toelichting gegeven op de stappen die een blok doorloopt. Deze zijn hieronder schematisch weergegeven



* *Optioneel*

Figuur 3 ***Reviewproces***

3.2.6 Wet- en regelgeving

GrIT realiseert de nieuwe IT-infrastructuur van Defensie. Er zijn vooral technische gegevens nodig om de infrastructuur te bouwen en in gebruik te kunnen nemen. Het programma verzamelt geen inhoudelijke data en voert hier ook geen analyses op uit. Het werkelijke gebruik van deze nieuwe IT-infrastructuur zal plaatsvinden door de toepassingen en applicaties die op deze infrastructuur in gebruik worden genomen. Op deze toepassingen is, afhankelijk van de toepassing, de reguliere wet- en regelgeving toepasbaar, zoals de uitvoeringswet AVG, de wet op de inlichtingen- en veiligheidsdiensten, de baseline informatiebeveiliging overheid en de Wet Open Overheid. Ook het Defensie Beveiligingsbeleid (DBB) is onderdeel van het programma van eisen. Dit wordt voor, tijdens en na de bouw getoetst en er wordt een accreditatie afgegeven door de Beveiligingsautoriteit. Onderdeel van het DBB is privacy. Via de Voorschrift Informatiebeveiliging Rijksdienst Efficiënt & Effectief (VIR E&E) worden persoonsgegevens onderkend en worden er eisen gesteld aan de bescherming daarvan. Wanneer er relevante ontwikkelingen zijn zal dit in de voortgangsrapportage(s) worden vermeld.

4 Inhoud programma GrIT

De programma aanpak is gebaseerd op een structurele strategische samenwerking tussen Defensie en een consortium als businesspartner. Binnen het consortium werkt een aantal complementaire marktpartijen samen om de nieuwe IT-infrastructuur in gezamenlijkheid met Defensie te realiseren. Na de realisatie zal Defensie ook het beheer in samenwerking met het consortium verzorgen. Er is daarom een contract afgesloten van tien jaar, met daarna vijf maal de optie om twee jaar te verlengen. De bouw en uitrol van de blokken duurt zeven jaar. Bij de realisatie ligt de prioriteit allereerst op het Hoog Gerubriceerde Informatie (HGI)-domein en het ontplooide domein (missies en gereedstelling). Parallel aan de migratie naar het nieuwe HGI-domein wordt het huidige TITAAN [3] afgebouwd. Daarna wordt de vernieuwing van de IT-infrastructuur binnen het Laag Gerubriceerde Informatie (LGI)-domein gestart.

4.1 Blokken en clusters

Het programma GrIT bestaat uit 42 [4] blokken te herkennen aan hun unieke code startend met 'BR-0'. De blokken voegen allemaal zelfstandig waarde toe en zijn individueel aan te besteden. Het consortium heeft als kernverplichting om een goed werkende IT-infrastructuur te realiseren en aan Defensie ter beschikking te stellen. Dit gebeurt in nauwe samenwerking. De meeste blokken zijn technisch van aard, aangezien met GrIT het technisch fundament wordt gerealiseerd van de nieuwe IT-infrastructuur. Elke keer dat delen van de IT-infrastructuur zijn vervangen en vernieuwd en deze functioneren, start de uitfasering van dit deel van de huidige IT-infrastructuur.

De blokken Camp New Amsterdam (BR-027), Wegwerken knelpunten huidige IT (BR-034) en Ontmantelen Defensie Applicaties (ODA, BR-035) betreffen activiteiten die al enige tijd voor de start van het programma GrIT in uitvoering waren binnen Defensie. Omwille van continuïteit en voortgang op deze lopende activiteiten zijn zowel de budgetten als de aansturing vanuit de DMO/JIVC lijn gecontinueerd. Omdat deze blokken randvoorwaardelijk zijn voor het programma GrIT zal in rapportages over de voortgang van deze blokken worden gerapporteerd. De blokken Internet op de Legering (BR-012), E-Welfare (BR-013), Enterprise Integration Services (BR-031), Data Analytics & Visualisatie & Geo (BR-032) en Enterprise Search & Language Support (BR-033) zijn nog niet afgenomen door Defensie.

De blokken zijn ingedeeld in elf clusters, gebaseerd op de mogelijke inzet van medewerkers met gelijksoortige expertise. In figuur 4 wordt de clustering van de 42 GrIT-blokken weergegeven, met in de volgende sub-paragrafen uitleg over de clusters. In bijlage A is een toelichting opgenomen van de individuele blokken.

Door de aanpak in blokken vindt gedurende de uitvoering van het programma een geleidelijke transitie plaats naar de nieuwe IT-infrastructuur. De modulaire planning (zie paragraaf 4.2) geeft op hoofdlijnen het startmoment van de realisatie van een blok weer, wanneer deze gereed is voor de initiële inzet en wat de duur is van de uitrol. Onderdeel van de aanpak is dat

[3] Het *Theatre Independent Tactical Adaptive Armed Forces Network* (TITAAN) is een netwerkoplossing waarmee overal ter wereld onder alle omstandigheden uit standaardbouwstenen een robuust en betrouwbaar netwerk voor militaire bevelvoering kan worden samengesteld.

[4] In de business case staan 43 blokken beschreven. Blok IT Service Management is vervangen door Project Beheerprocessen waardoor de samenhang met de huidige IT het meest effectief kan worden gerealiseerd.

blokken waar nodig worden geaccrediteerd door de Beveiligingsautoriteit van Defensie, zodat de digitale weerbaarheid is geborgd.

Housing	Operationele Compartimenten & Modules Ontplooid	Private Cloud Platform	Migratie Keep Applicaties	Connectivity	Moderne Werkplekomgeving	Mobiele Netwerken	Unified Comms.	IT Security	IT Operations	GES (opt.)
BR-025 Twin DC	**BR-028** Operationele compartlmenten	**BR-014 tot 017** Private Cloud Platform	**BR-036** HGI	**BR-010** Protected Core Network	**BR-007** Individual Workplace	**BR-001** Defensie Mobiele Netwerk	**BR-002** Unified Comms.	**BR-021** Security Operatlons Center	Project beheerprocessen	**BR-030** Information Mngmt.
BR-026 Uitwijk DC	**BR-029** Modules Ontplooid		**BR-037** Ontplooid	**BR-011** Local Area Network	**BR-008** IT Basis Toepassingen		**BR-003** Contact Center	**BR-022** Identity & Acces mgmt.	**BR-018** IT Service mgmt.	**BR-031 *** Enterprise Int. Services
	BR-020 Yellow Domain		**BR-038** LANTEK	**BR-012 *** IODL	**BR-009** Collab. & Comm. Services		**BR-004** Operationnal Chat	**BR-023** Information Exchange Gateway	**BR-019** IT Operationnal mgmt.	**BR-032 *** Data analytics visualisatie
			BR-039 Confi	**BR-013 *** Welfare			**BR-005** Critical Comms.	**BR-024** IT-toegangscontrole		**BR-033 *** Ent. Search & Language Support
			BR-040 LGI							
			BR-041 KMAR							
			BR-042 Medisch							
			BR-043 Complex							

* *Optionele blokken*

Figuur 4 ***Clustering GrIT blokken***

4.1.1 Housing blokken - Twin datacenter en datacenter op de uitwijklocatie

Het twin datacenter huisvest de nieuwe IT van Defensie. Met het twin datacenter (BR-025) wordt de continuïteit van de IT sterk verbeterd doordat er bijvoorbeeld bij storingen snelle terugval is op een tweede datacenter. Daarnaast kan Defensie terugvallen op het uitwijkdatacenter (BR-026). Bovendien is er een betere beveiliging voor brandpreventie, stroomuitval en andere mogelijke calamiteiten.

4.1.2 Operationele compartimenten en Ontplooide modules

De IT-boxen, kleine, mobiele lokale datacenters die met uitzendingen en oefeningen meegaan, worden vernieuwd in het blok Modules Ontplooid (BR-029). De huidige boxen zijn groter en zwaarder dan de nieuwe boxen.

4.1.3 Defensie Private Cloud Platform

Het Defensie Private Cloud Platform wordt via vier blokken (BR-014 tot en met BR-017) gerealiseerd. Hierop kunnen applicaties draaien, zoals bijvoorbeeld SAP, die het informatiegestuurd werken, de efficiëntie van de bedrijfsvoering en de kwaliteit van de managementinformatie bevorderen.

4.1.4 Migratie Keep Applicaties

De door Defensie gebruikte applicaties moeten van de oude naar de nieuwe IT-infrastructuur worden overgezet, de zogeheten applicatiemigratie. Deze migratie vindt plaats met behoud van functionaliteit. In sommige gevallen zal de functionaliteit van applicaties op de nieuwe IT-infrastructuur verbeterd zijn. De migratie naar de nieuwe IT-infrastructuur verbetert zowel de beschikbaarheid als beveiliging van applicaties.

De migratie omvat onder andere het overzetten van bijbehorende data, testen van de werking van de applicaties op de nieuwe IT-infrastructuur en het documenteren van de audit trail. De migratie wordt zo gestandaardiseerd als mogelijk uitgevoerd. Door tijdig alle te behouden applicaties (KEEP-applicaties) over te zetten kan de oude IT-infrastructuur zo snel mogelijk uitgefaseerd worden. Hierdoor neemt de kans op dubbele beheerlasten af.

4.1.5 Connectivity blokken - Nieuwe veilige verbindingen met NAVO partners

Het realiseren van het blok Protected Core Network (BR-010) stelt Defensie in staat op een moderne, veilige en flexibele manier verbindingen met NAVO- en EU-partners te realiseren. Hierdoor kan Defensie met NAVO-partners via de nieuwste standaarden communiceren waarbij Defensie externe partner- en commerciële netwerken kan gebruiken. Hiermee geeft Defensie invulling aan de afspraken over het Federated Mission Networking van de NAVO. Ook worden de interne operationele communicatiemogelijkheden (via de blokken Operational Chat, BR-004, en Critical Communications, BR-005) verbeterd.

4.1.6 Moderne werkplekken

Door het realiseren van cluster Moderne Werkplekomgeving gaat de defensiemedewerker beschikken over één set aan functionaliteiten dat het beste aansluit op zijn of haar werkzaamheden. De benodigde (defensie)applicaties kunnen gemakkelijk worden bereikt. Extra functionaliteiten kan een medewerker eenvoudig zelf aanvragen en worden snel en zoveel mogelijk geautomatiseerd gerealiseerd.

4.1.7 Mobiele netwerken

Een specifiek blok is het Defensie Mobiele Netwerk (BR-001) waarmee Defensie de beschikking krijgt over eigen mobiele communicatiemogelijkheden. Defensiemedewerkers moeten altijd, overal en onder alle omstandigheden veilig en interoperabel kunnen communiceren. Hiervoor is een betrouwbare mobiele dekking cruciaal. Met het Defensie Mobiele Netwerk is Defensie niet langer afhankelijk van één telecomprovider en altijd zeker van een goede en extra veilige, wereldwijde mobiele dekking.

4.1.8 Unified Communications

De verschillende communicatiemogelijkheden, bijvoorbeeld chat, worden met de nieuwe IT-infrastructuur verbeterd. Alle gebruikers krijgen overal dezelfde functionaliteit beschikbaar via de realisatie van blok Unified Communications (BR-002). Ook wordt het mogelijk om

veilig en vertrouwd samen te werken met grotere groepen via elke mobiele of vaste werkplek; binnen Defensie, met NAVO- en EU-partners en anderen.

4.1.9 IT Security

Direct gekoppeld aan het Defensie Private Cloud Platform (paragraaf 4.1.3) zijn de security blokken. Via het blok Identity & Access Management (BR-022) wordt een veilige en gecontroleerde persoonsgebonden toegang tot de Defensie IT geborgd. Hiermee beschermen we ook digitaal wat ons dierbaar is en kan Defensie veilig en *real time* informatie delen in snel wisselende verbanden met NAVO- en EU-partners, NGO's, kennisinstituten en leveranciers. BR-021 levert het nieuwe Security Operations Center (SOC).

4.1.10 IT Operations (IMS)

Er zijn nieuwe oplossingen ontworpen voor het efficiënt uitvoeren van het beheer van de IT-infrastructuur. Het platform ter ondersteuning van de basis ITIL processen (Incident, Problem, Change, Asset & Configuration Management) en het aanvragen van nieuwe diensten via een selfservice catalogus (BR-018) wordt gebouwd.

Het blok IT Operational Management (BR-019) ondersteunt de IT organisatie in haar beheertaken. Het omvat services zoals het monitoren van IT diensten, het analyseren van gedragsverandering in de IT omgeving en het inzichtelijk maken van de samenhang van IT diensten. Naast het verschaffen van inzicht in de status van het landschap is er ondersteuning voor het (automatisch) uitvoeren van beheeractiviteiten zoals het oplossen van incidenten, wijzigen en bijwerken van IT diensten.

Het blok Yellow Domain (BR-020) levert een omgeving waarin inzicht is in de status van alle IT bij Defensie. In het Yellow Domain worden alle beheergegevens samengebracht om inzicht te krijgen in al deze omgevingen om zo efficiënter en effectiever te kunnen beheren.

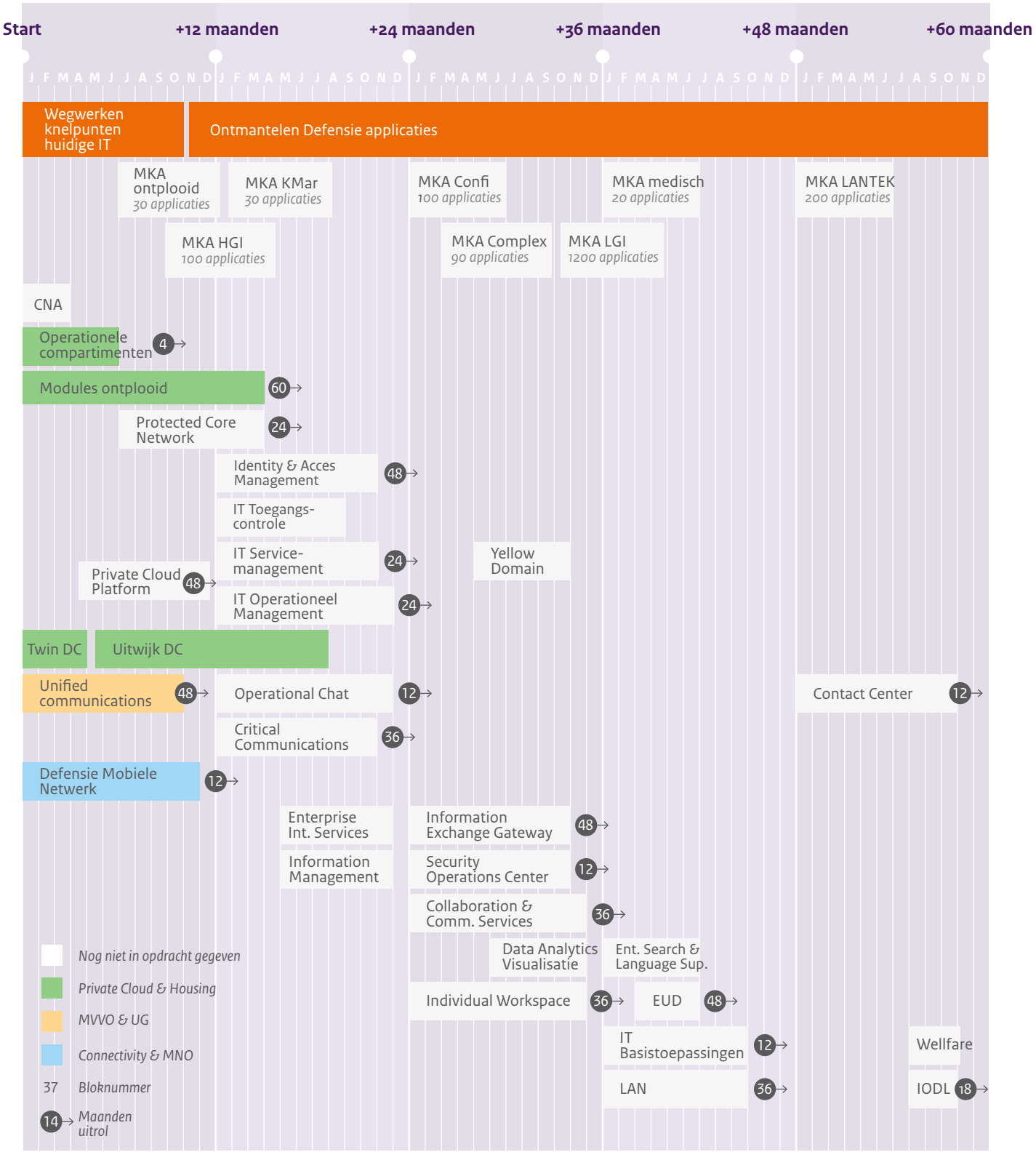
4.1.11 Generieke Services (GES)

GES zijn toepassingen die generiek door andere applicaties kunnen worden gebruikt. Er zijn drie generieke services in scope meegenomen; platformen en databases, informatie labeling en generieke ontwikkelstraat.

4.2 Planning en afhankelijkheden

Defensie realiseert de bouw van GrIT in zeven jaar. Het laatste blok moet afgerond zijn in 2027. Zoals in paragraaf 4.1 is beschreven bestaat GrIT uit 42 blokken die ingedeeld zijn in elf clusters. De blokken voegen allemaal afzonderlijk waarde toe en worden als deelprojecten gegund en gerealiseerd. Defensie houdt binnen de planning controle over wanneer een blok uitgevoerd kan en gaat worden. Indien opportuun of noodzakelijk kan Defensie ervoor kiezen een blok eerder of later te realiseren. De Kamer wordt over de voortgang van de blokken geïnformeerd met de voortgangsrapportages.

In figuur 5 is de referentieplanning zoals deze in de business case is opgenomen, weergegeven.



Figuur 5 ***Referentieplanning GrIT uit business case***

Blokken zijn zodanig samengesteld dat ze op ieder willekeurig moment in de tijd zelfstandig gerealiseerd kunnen worden. De volgorde van de blokken is ook op die basis samen met de defensieonderdelen, binnen de kaders van de CDS, bepaald. In principe leidt vertraging van één blok niet tot vertraging op een ander blok. Zolang nieuwe functionaliteiten niet beschik-

baar zijn, wordt gebruik gemaakt van functionaliteiten die door de huidige IT worden geboden. Door de modulaire opbouw van het programma is de impact op de rest van de blokken en het programma in het geheel beperkt. Soms maken blokken gebruik van nieuwe functionaliteiten die door andere blokken worden opgeleverd. Zo is de Individual Workspace (BR-007) afhankelijk van de Private Cloud (BR-014 t/m BR-017) en Security blokken (BR-021 t/m BR-024). De eerste MKA-blokken (BR-036 en BR-037) maken gebruik van de blokken Operationele Compartimenten (BR-028) en de Modules Ontplooid (BR-029). De overige MKA-blokken (BR-038 t/m BR-043) zijn eveneens afhankelijk van de Private Cloudblokken.

Per blok zijn in het contract mijlpalen vastgelegd. Na het opstellen van het Initiatie Document (ID) wordt dit, via de CIO-Office bij het AcICT aangeboden. De aanbevelingen/uitkomsten van de AcICT-toets worden verwerkt in Ontwerp Uitvoeringsplan voordat dit ter goedkeuring wordt aangeboden aan de PB GrIT.
Tijdens de vernieuwing en vervanging van de IT-infrastructuur is Defensie afhankelijk van de huidige IT welke nu in beheer is bij DMO/JIVC/Git&Infra. Doordat de scope van het contract binnen de dienstverlening van deze afdeling valt en personeel van de afdeling bijdraagt aan de realisatie van de blokken, is deze afhankelijkheid geborgd.

4.3 Opzet

GrIT wordt door Defensie in samenwerking met een consortium van marktpartijen gerealiseerd. Het consortium is samengesteld uit diverse leveranciers en heet Athena.

De drie kernorganisaties in Athena brengen ieder op hun eigen terrein kennis en ervaring in, die in combinatie met de kunde van Defensie bijdraagt aan het succesvol uitvoeren van het programma. Het consortium wordt geleid door IBM. IBM beschikt over ervaring met en kennis over het realiseren en exploiteren van bedrijfskritische IT-infrastructuur. Unica is een technische dienstverlener die werkt aan duurzame innovaties die bijdragen aan functionele, gezonde en veilige leef- en werkomgevingen. Atos is gespecialiseerd in de ondersteuning bij digitale transformatie en in *cloud*, cybersecurity en *high-performance computing*.

4.4 Samenwerking

Het consortium is verantwoordelijk voor de realisatiewerkzaamheden en de daaruit volgende diensten in de terbeschikkingstellingsfase (exploitatie), waarbij wordt gewerkt met duidelijke en breed gereviewde opdrachtdocumenten. In overleg met de defensieonderdelen en JIVC wordt de fasering van de vervanging en vernieuwing van de IT-infrastructuur geoptimaliseerd. Ook op het vlak van architectuur en *lifecycle*-management van de huidige IT-infrastructuur wordt intensief samengewerkt met het consortium. De architecten van het consortium en Defensie overleggen wekelijks over IT vernieuwing, *lifecycle*-management en andere IT vraagstukken, zodat voor een goede aansluiting wordt gezorgd. Het contract bevat een Producten- en Dienstencatalogus (PDC). Daarin staat welke producten en diensten Defensie geleverd krijgt, tegen welke kosten en met welke beschikbaarheid. Dataprotectie en continuïteit van de dienstverlening worden geborgd doordat het consortium het eigendom van de toegepaste hardware in de IT-Infrastructuur bij levering overdraagt aan Defensie.

Zowel de bouw van de blokken (de realisatie) als de exploitatie (de terbeschikkingstelling) vindt plaats in gemengde teams, zodat voldoende kennis beschikbaar is voor een (on) voorziene beëindiging van de samenwerking met het consortium (exit) en Defensie de IT-infrastructuur zelfstandig kan verzorgen en continueren.

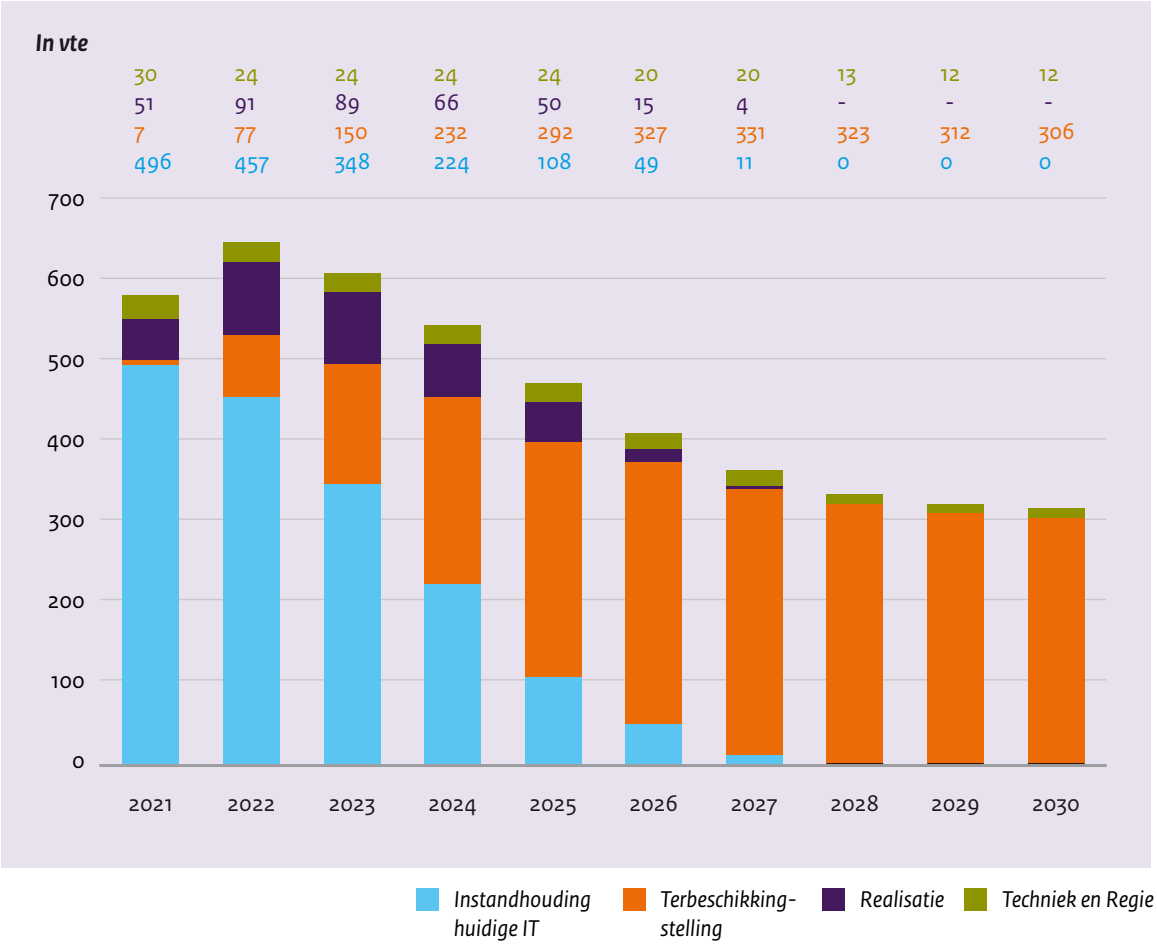
4.5 Gerelateerde projecten en programma's

Omdat met GrIT de nieuwe IT-infrastructuur wordt gerealiseerd, zijn projecten die baat hebben bij deze infrastructuur gerelateerd aan het programma GrIT. De huidige IT-infrastructuur kan echter op korte termijn dergelijke projecten ondersteunen en GrIT is niet afhankelijk van de uitvoering van die projecten. Zo zijn ook de programma's Roger en Foxtrot indirect verbonden met, maar niet afhankelijk van, het programma GrIT. Over deze programma's wordt gerapporteerd middels het Defensie Projectenoverzicht (Foxtrot) en het Rijks ICT-Dashboard (Roger).

4.6 Benodigde capaciteit

Voor het realiseren en beheren van de nieuwe IT-infrastructuur werkt Defensie met het consortium in gemengde teams. Naast capaciteit voor realisatie en beheer, is capaciteit vereist voor de invulling van de programmaorganisatie, zoals transitiemanagement en de regie op het contract. Verder vraagt het in stand houden van de huidige IT capaciteit. Naarmate het programma vordert zal dit afnemen. In de jaren 2022 en 2023 verwacht Defensie de hoogste totale inzet (figuur 6).

In de uitvoeringsplannen van elk blok wordt de verhouding tussen defensiepersoneel en het personeel van het consortium en de gefaseerde instroom van defensiepersoneel vastgelegd. Dit zodat het defensiepersoneel kennis en ervaring kan opdoen tijdens de bouw van een blok. Per blok en per fase (realisatie en terbeschikkingstelling) verschilt het aandeel van defensiemedewerkers. Eventuele capaciteitstekorten mogen door het consortium worden ingevuld, waardoor inhuur in de uitvoering wordt voorkomen.



Figuur 6 ***Benodigde capaciteit volgens business case***

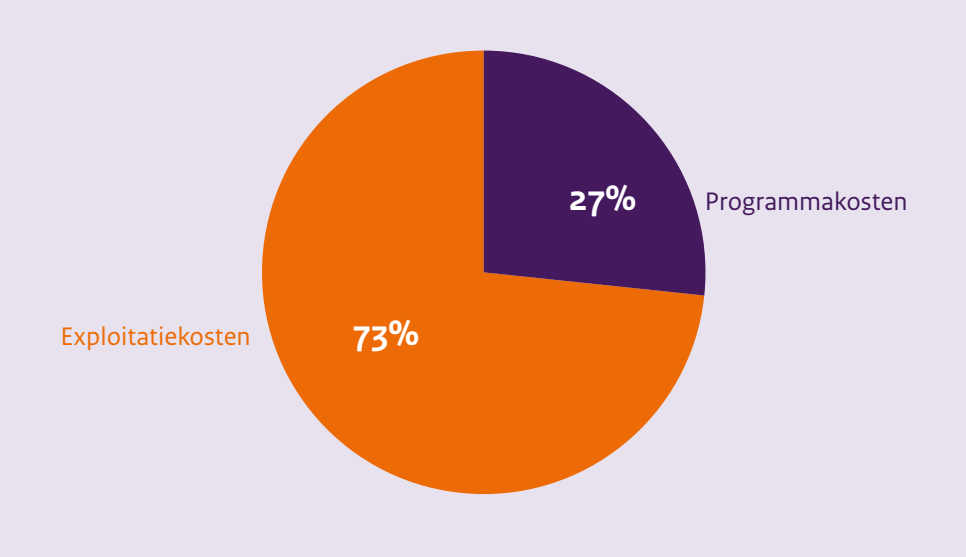
4.7 Opbouw kosten

In de GrIT-rapportages wordt gewerkt met een commercieel vertrouwelijke bijlage met gedetailleerde financiële gegevens. De peildatum van de financiele gegevens in deze paragraaf van de basisrapportage is 1 januari 2021.

In de business case zijn naast de kosten voor de bouw van de nieuwe IT-infrastructuur ook de exploitatiekosten opgenomen. De kosten in de business case zijn dan ook te onderscheiden in:

1. De programmakosten voor de realisatie van de nieuwe IT-infrastructuur (zeven jaar) en
2. De exploitatie van de huidige en nieuwe IT-infrastructuur (tien jaar).

De exploitatiekosten vormen met 73% het grootste aandeel van de kosten in de business case. De opbouw van de kosten uit de business case en daarmee ook de contractwaarde is gedeeld in Kamerstuk 35728, nr. 2 en is, zoals hieronder weergegeven, groter dan het budget dat in Kamerstuk 31 124 nr. 118 is vermeld, daar dit geen volledige kostenopgave was.



Figuur 7 ***Kostenopbouw in de business case GrIT***

De realisatie van het programma wordt uitgedrukt in de programmakosten, waarover eerder in het Defensie Projectenoverzicht en de bijbehorende Afwijkingsrapportage is gerapporteerd.

4.7.1 Programmakosten

De programmakosten kennen de volgende componenten:

- **Realisatie consortium**: dit zijn de kosten voor het realiseren van de nieuwe systemen en bestaan grotendeels uit manuren van het consortium en de kosten voor de (ver)bouw van de datacenters.
- **Transitiemanagement**: de kosten van de programmaorganisatie, die de transitie naar de nieuwe IT coördineert.
- **Inzet Defensie in gemengde teams**: de kosten van IT-personeel van Defensie dat meebouwt aan de nieuwe IT binnen de scope van de programmakosten voor de realisatie van de nieuwe IT-infrastructuur.
- **Voorbereiding op het programma**: de kosten die zijn gemaakt en zijn aangegaan in de voorbereidende en contracteringsfase van het programma.

- **Dubbele beheerlasten**: bij het vervangen van de ene IT-omgeving door de andere is sprake van een overgangsperiode waarin zowel de huidige als de nieuwe IT-infrastructuur moet worden beheerd. Hierdoor ontstaan dubbele beheerlasten. Deze kosten zijn daarom, als onderdeel van het programma, apart gebudgetteerd. Voor het realiseren van het programma binnen de kaders van de business case is het zo kort mogelijk houden van deze overgangsperiode een belangrijke doelstelling van het programma en valt daarom binnen de verantwoordelijkheid van het programma.
- **Innovatie**: om een minimale financiële ruimte voor innovatie te borgen op het gebied van IT-infrastructuur wordt vanaf 2024 rekening gehouden met een jaarlijks innovatiebudget, verder toegelicht in de commercieel vertrouwelijke bijlage.
- **Risicoreservering**: elk IT-programma kent risico's. Om de effecten van risico's die zich voordoen bij de investeringen op te vangen is in het programmabudget rekening gehouden met een risicoreservering. Over de risicoreservering wordt in detail gesproken in de vertrouwelijke bijlage. Deze reservering is niet van toepassing op de risico's in de exploitatie.

4.7.2 Exploitatie

De exploitatie bestaat uit drie hoofdonderdelen, te weten:

1. De **voortzetting van de huidige activiteiten** die door GrIT worden beïnvloed maar die niet door GrIT worden vervangen. Hieronder worden de uitgaven geschaard die voortkomen uit de voortzetting van bestaande IT-activiteiten binnen DMO/JIVC die door GrIT worden beïnvloed maar die niet door GrIT worden vervangen. Hierbij valt te denken aan de periodieke vervanging van gebruikersapparatuur, zoals smartphones en laptops.
2. Het **beheer van de huidige IT** welke door GrIT wordt vervangen. Dit omvat de kosten van personeel, softwarecontracten en hardware voor het beheer van de huidige IT, welke door de uitvoering van het programma GrIT worden vervangen. De kosten van dit beheer nemen af naarmate de nieuwe IT wordt geïmplementeerd.
3. Na oplevering van de nieuwe IT het **beheer van de nieuwe IT**. Dit omvat de kosten van personeel, softwarecontracten en hardware voor het beheer van de nieuwe IT. De kosten van dit beheer nemen toe naarmate de nieuwe IT wordt geïmplementeerd. Daarnaast is de inzet van Defensie in de gemengde teams hierin opgenomen.

Het beheer van de huidige IT binnen de kaders van GrIT loopt af en de daarmee bespaarde kosten worden ingezet voor de financiering van het beheer van de nieuwe IT.

4.8 Risico's

Ten tijde van het opstellen van de business case is door de diverse stakeholders een risico-inventarisatie uitgevoerd. Risico's en de beoogde mitigaties die hieruit voortkwamen zijn gehanteerd als uitgangspunten bij de start van de realisatie. Na de start van de realisatie zijn deze risico's verdiept en geactualiseerd en zijn er nieuwe risico's geïdentificeerd; deze worden samen met onderstaande drie initiële risico's en de mitigerende maatregelen verder toegelicht in paragraaf 5.7.

4.8.1 Belangrijkste risico's business case

De drie hoofdrisico's die ten tijde van het opstellen van de business case zijn geïdentificeerd, zijn:

1. Defensie is onvoldoende in staat om regie te voeren over een potentieel omvangrijk en langdurige contract voor de realisatie en terbeschikkingstelling van IT-diensten welke onder verantwoordelijkheid van het consortium worden voortgebracht. Defensie heeft de verantwoordelijkheid om de regierol te vervullen. De regieorganisatie als onderdeel van de

afgesproken governancestructuur zal op een gelijkwaardig niveau professioneel ingevuld moeten zijn bij de start van het contract om de realisatie van de eerste blokken succesvol te laten verlopen.
De kans op vertraging in de realisatie en de als gevolg hiervan boven het budget oplopende kosten worden hiermee gemitigeerd. Door een vertraagde levering en/of acceptatie van de prestaties zal weliswaar ook een latere betaling aan het consortium plaatsvinden, echter de kosten van de instandhouding van de huidige IT-infrastructuur lopen eveneens langer door.

2. Contractuele geschillen. De omvang en complexiteit van de contractdocumentatie zouden ertoe kunnen leiden dat partijen verschillende lezingen hanteren van de op schrift gemaakte afspraken. Dit kan leiden tot hapering in de samenwerking.
3. Baten worden niet of slechts gedeeltelijk gerealiseerd. Vertraging in de uitvoering van het plan en/of het niet of het later uitfaseren van de huidige IT-infrastructuur kan tot gevolg hebben dat de beoogde baten niet of slechts gedeeltelijk worden gerealiseerd.

Risico	**Business case**	
	Kans	Impact
1. Onvoldoende regie	Klein	Zeer groot
2. Contractuele geschillen (intentie)	Klein	Zeer groot
3. Afbouw van de huidige IT vindt niet (snel genoeg) plaats	Klein	Groot

Figuur 8 ***Risicotabel***

5 Voortgang jaar 1, 2021

5.1 Algemeen

In dit hoofdstuk wordt ingegaan op de voortgang in 2021. Er zijn op 31-12-2021 geen wijzigingen van het beoogde eindproduct ten opzichte van product zoals beschreven in de business case. Wel is er een kleine uitbreiding van de scope en bijbehorend budget geweest. De ontwikkelingen worden hieronder toegelicht.

Housing	Operationele Compartimenten & Modules Ontplooid	Private Cloud Platform	Migratie Keep Applicaties	Connectivity	Modern Werkplek-omgeving	Mobiele Netwerken	Unified Comms.	IT Security	IT Operations	GES (opt.)
BR-025 R Twin DC	**BR-028** T Operationele compartl-menten	**BR-014** I **tot 017** Private Cloud Platform	**BR-036** I HGI	**BR-010** I Protected Core Network	**BR-007** N Individual Workplace	**BR-001** I Defensie Mobiele Netwerk	**BR-002** I Unified Comms.	**BR-021** I Security Operatlons Center	Project beheer-processen R	**BR-030** N Information Mngmt.
BR-026 N Uitwijk DC	**BR-029** R Modules Ontplooid		**BR-037** I Ontplooid	**BR-011** N Local Area Network	**BR-008** N IT Basis Toepas-singen		**BR-003** N Contact Center	**BR-022** I Identity & Acces mgmt.	**BR-018** N IT Service mgmt.	**BR-031** * Enterprise Int. Services
	BR-020 N Yellow Domain		**BR-038** N LANTEK	**BR-012** * IODL	**BR-009** N Collab. & Comm. Services		**BR-004** N Operatio-nal Chat	**BR-023** I Information Exchange Gateway	**BR-019** N IT Operatio-nal mgmt.	**BR-032** * Data analytics visualisatie
			BR-039 N Confi	**BR-013** * Welfare			**BR-005** N Critical Comms.	**BR-024** I IT-toegangs-controle		**BR-033** * Ent. Search & Language Support
			BR-040 N LGI							
			BR-041 N KMAR							
			BR-042 N Medisch							
			BR-043 N Complex							

N *Nog te starten* I *Initiatie* R *Realisatie* U *Uitrol*
T *Terbeschikkingstelling/Exploitatie* * *Optionele blokken*

Figuur 9 ***Status blokken***

5.2 Status blokken

Na het tekenen van het contract, is begin 2021 door Defensie en het consortium de omschakeling gemaakt van contractvoorbereiding naar uitvoering. De samenwerking werd in 2021 extra bemoeilijkt door COVID-19. Daarnaast is in 2021 het besluitvormingsproces rond de blokken mede op basis van het vierde BIT-advies verder ontwikkeld.

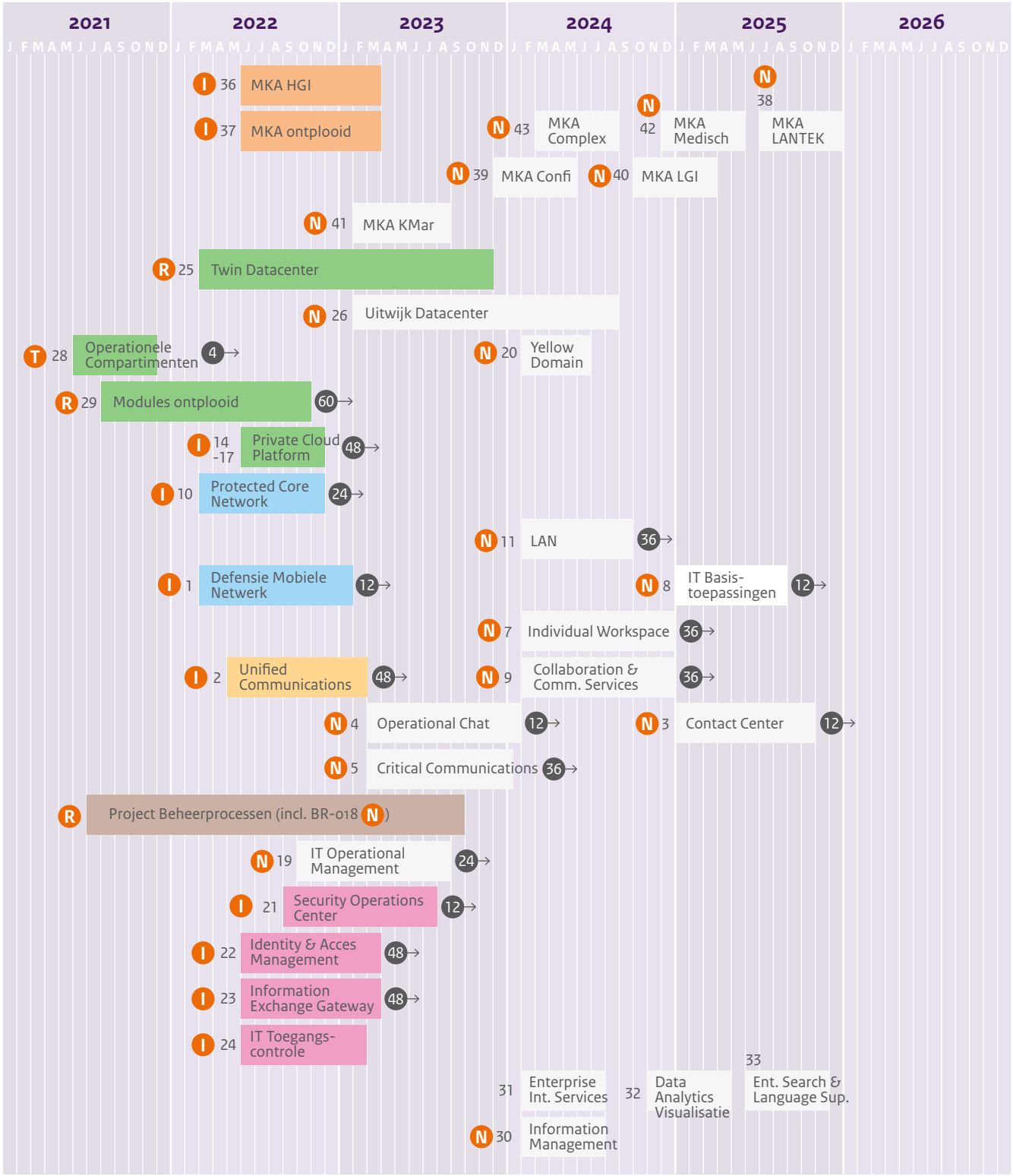
Het jaar 2021 was het startjaar van de realisatiefase van GrIT. In dat jaar lag de focus op het maken van initiatiedocumenten voor de te realiseren blokken.

Eind 2021 werd aan zestien blokken en aan één project gewerkt, welke zich in verschillende fases bevinden. De vier Private Cloud blokken staan als één punt in het overzicht, conform de clustering (figuur 9).

Er is gestart met de voorbereidingen van de bouw van het nieuwe duurzame twin datacenter (BR-025). De blokken die zorgen voor de realisatie van het datacenter lopen naar schatting langer door dan eerder gepland, door het uitblijven van een definitief besluit over de vergunningen vanwege de stikstofproblematiek.

Op basis van de ervaringen met het verkrijgen van de onherroepelijke omgevingsvergunning voor de bouw van het twin datacenter, heeft Defensie besloten de verbouwing van de uitwijklocatie (BR-026) te ontkoppelen van de realisatie van het nieuwe twin datacenter. De verbouwactiviteiten voor de (ver)bouw uitwijklocatie worden pas opgestart zodra de onherroepelijke omgevingsvergunning beschikbaar komt (naar verwachting in 2023).

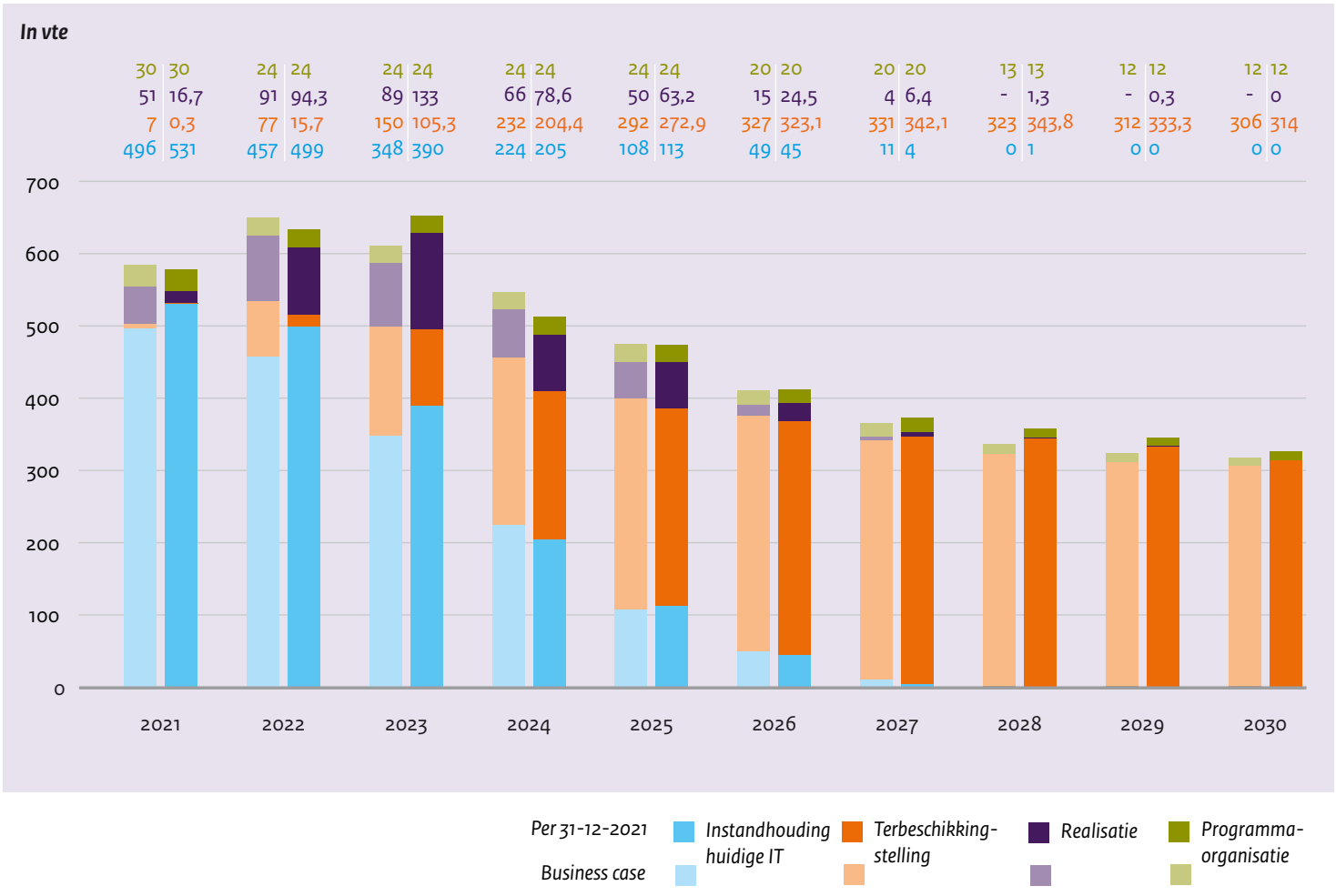
De planning en de status van de blokken per 31 december 2021 is in figuur 10 visueel weergegeven. In december 2021 is het blok Operationele Compartimenten (BR-028) opgeleverd en de exploitatie gestart. Ook het blok Camp New Amsterdam (BR-027) is in 2021 volgens planning opgeleverd. Dit blok is randvoorwaardelijk voor de uitvoering van het programma GrIT. Het blok End-User Devices (BR-006) loopt gedurende het hele programma.
De uitvoer van het programma en daarmee de start van de blokken is over het algemeen later gestart dan oorspronkelijk beoogd, omdat het goedkeuringsproces verder gestroomlijnd is gedurende de eerste periode van het programma.



Figuur 10 ***Planning 31-12-2021***

5.3 Capaciteit

Voldoende capaciteit is een belangrijke randvoorwaarde om het programma succesvol te realiseren. De arbeidsmarkt is in 2021 krapper geworden en de vraag naar IT-personeel is binnen en buiten Defensie fors toegenomen onder andere door het vrijkomen van extra middelen in 2021.
Defensie is een unieke samenwerking aangegaan met de markt. Aan de start van het programma is tijd genomen om de programma-organisatie goed neer te zetten en op elkaar ingespeeld te raken. Er zijn hierdoor blokken later gestart dan voorzien. Dit zorgt voor een beperkte verschuiving van de benodigde capaciteit (figuur 11). Om capaciteit beschikbaar te krijgen werkt Defensie intensief samen met het consortium. In het eerste jaar waren er nog geen capaciteitstekorten. In de CIO-oordelen zijn adviezen gegeven over capaciteit, deze zijn opgevolgd. Capaciteit blijft echter een risico.



Figuur 11 ***Benodigde capaciteit per 31-12-2021***

5.4 Kosten

5.4.1 Realisatie

Realisatie consortium: dit zijn kosten voor de bouw van blokken door het consortium. Bij de realisatie van de blokken is in 2021 € 17,2 miljoen aan extra kosten ontstaan, dit is verder toegelicht in de commercieel vertrouwelijke bijlage. Extra kosten worden gefinancierd uit de

risicoreservering. Door een verschuiving in de planning dalen de verwachte uitgaven van Modules Ontplooid (BR-029) met € 10,7 miljoen. Er wordt bekeken of dit vrijgevallen budget beschikbaar kan worden gesteld voor tempobehoud van de huidige planning.

Het maken van een planningstool, die zowel voor de oude als de nieuwe IT kan worden gebruikt is toegevoegd aan de scope van het programma. Deze scopewijziging van € 0,9 miljoen is voor Defensie als geheel budgetneutraal doordat het bijbehorende budget uit een bestaand project is overgeheveld naar het programma GrIT.

Figuur 12 ***Financiële ontwikkeling programmakosten.***

Overige componenten: de gemaakte kosten voor transitiemanagement vallen binnen het daarvoor gestelde kader. De dubbele beheerlasten en de inzet van Defensie in de gemengde teams (voor wat betreft het investeringsdeel) blijven op basis van de huidige inzichten nagenoeg ongewijzigd, maar schuiven in de tijd op als gevolg van verschuivingen in de planning, doordat enkele blokken later zijn gestart dan oorspronkelijk gepland.

Om de kostenposten in de business case beter aan te laten sluiten op de defensiebegroting, is ervoor gekozen om de posten te herstructureren. Hierdoor schuift € 25 miljoen euro van de exploitatiekosten naar de programmakosten.

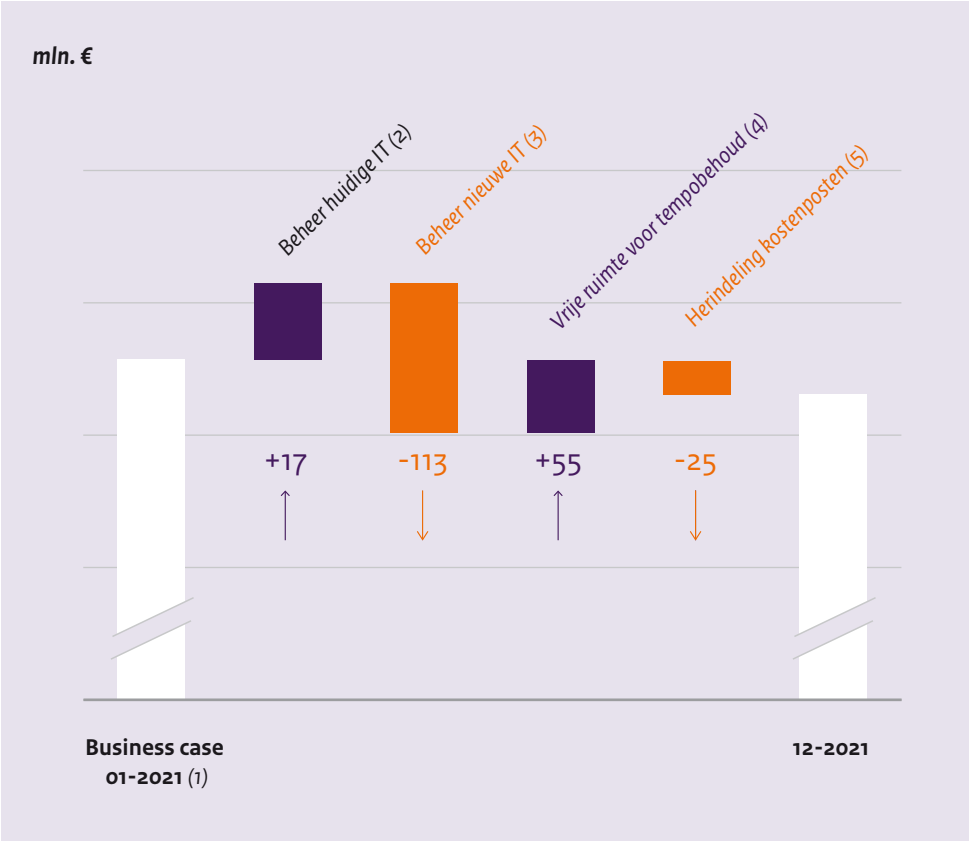
Risicoreservering: Na bovenstaande uitputting van de risicoreservering en actualisatie van de risico-inschatting van het programma blijft de resterende risicoreservering per 31-12-2021 groter dan de totale verwachtingswaarde van de geïdentificeerde risico's en is daarmee voldoende om deze te dekken. In de vertrouwelijke bijlage wordt hier in detail op toegelicht.

5.4.2 Exploitatiekosten

Als gevolg van verschuivingen in de planning worden enkele blokken later gestart dan in de business case verwacht (zie paragraaf 5.2). Delen van de nieuwe IT-infrastructuur zullen later live gaan en Defensie zal langer gebruik maken van de huidige IT-infrastructuur. Doordat de huidige IT-infrastructuur lagere beheerlasten kent dan de nieuwe IT, zullen in de periode 2021-2030 de totale beheerlasten lager zijn. Daar staat tegenover dat Defensie pas later gebruik kan maken van de aanvullende functionaliteit en continuïteit die de nieuwe IT biedt.

Als gevolg van de verschuivingen in de planning dalen de verwachte kosten met € 55 miljoen. Verwachte uitgaven voor het beheer van de huidige IT (circa € 58 miljoen) en een afname van de kosten voor het beheer van de nieuwe IT (inclusief de inzet van Defensie in de gemengde teams) met circa € 113 miljoen. Het saldo blijft beschikbaar binnen het programma GrIT en ook hier wordt bekeken of het kan worden aangewend voor tempobehoud van de huidige planning.

Zoals hierboven reeds genoemd, is er daarnaast in verband met de herindeling van de kostenposten € 25 miljoen euro van de exploitatiekosten naar de programmakosten verschoven.



Figuur 13 ***Financiële ontwikkeling exploitatiekosten***

5.4.3 Budget

Totaalbudget GrIT bij start samenwerkingsovereenkomst (1-1-2021)	€ 3.078 mln.
Budgetuitbreiding gedurende 2021	€ 0,9 mln.
Totaalbudget GrIT per 31-12-2021	**€ 3.079 mln.**

5.4.4 Gerealiseerde kosten 2021

Gedurende 2021 is binnen het programma GrIT € 62,5 miljoen aan investeringskosten gemaakt. Hiervan is € 42,8 miljoen uitgegeven aan realisatie activiteiten die zijn uitgevoerd door het consortium. Binnen de exploitatiekosten van DMO/JIVC is een bedrag van € 186,1 miljoen toegewezen aan het programma GrIT. Hiervan is in 2021 € 10,6 miljoen uitgegeven aan het beheer van de nieuwe IT.

5.4.5 Verplichtingen binnen investeringen

Verplichtingenstand per 1-1-2021	Aangegane verplichtingen gedurende 2021	Kasuitgaven 2021	**Verplichtingenstand per 31-12-2021**
€ 32,9 mln.	€ 120,6 mln.	-/- € 55,4 mln.	€ 98,0 mln.

De kasuitgaven in 2021 (€ 55,4 miljoen) zijn lager dan de eerder genoemde € 62,5 miljoen aan kosten in de investeringen van de business case. In de business case worden namelijk ook kosten toegekend die zijn gemaakt door de inzet van Defensiepersoneel in gemengde teams en transitiemanagement.

5.5 Governance

In het eerste jaar van de realisatie van het programma GrIT is de governance mede op basis van de eerdere AcICT-adviezen aangescherpt. In januari 2021 is de stuurgroep Digitale Transformatie ingesteld. De werkprocessen binnen het programma zijn met behulp van externe ondersteuning aangescherpt.

5.6 Kwaliteitsmanagement

Eind 2021 is er een onafhankelijke Quality Assurance rol (QA-rol) ingericht binnen het programma. Naast de interne toetsing wordt op belangrijke blokken een extern bureau ingehuurd voor een extra kwaliteitscheck. Daarnaast wordt op alle initiatiedocumenten een CIO-oordeel uitgevoerd. Na een positieve uitkomst worden de plannen aangeboden aan AcICT. Deze werkwijze en de op advies van AcICT doorgevoerde verbetering zijn eerder toegelicht in Kamerstuk 31125, nr. 119.

5.7 Risicomanagement en -beheersing

Risico's worden onder controle gehouden door middel van escalaties naar de drie managementlagen, zoals benoemd in hoofdstuk 3. Per kwartaal wordt over de beheersing van de belangrijkste risico's gerapporteerd. Risicomanagement is een doorlopend proces en vast onderdeel van de programmabeheersing. Tijdens de contracteringsfase in 2020 (en eerder) en nu in de realisatiefase wordt de ontwikkeling van de risico's op continue basis bijgehouden en mitigerende acties actief gemonitord. Alle risico's van zowel Defensie als het consortium worden geregistreerd in een gezamenlijke database.

Na de start van de realisatiefase van het programma in 2021 zijn de bestaande risico's uit de business case verdiept en geactualiseerd. Daarnaast hebben zich nieuwe risico's voorgedaan. Het totale overzicht is hieronder weergegeven.

1. **Defensie is onvoldoende in staat regie te voeren.** Defensie heeft het team na de start verder opgeschaald, waar nodig ondersteund door inhuur. Dit heeft op dit moment nog niet geleid tot significant hogere kosten. Daarnaast zijn er stappen genomen in het verbeteren van de governance, waaronder het instellen van een stuurgroep Digitale Transformatie.
2. **Schaarste aan personele capaciteit.** De realisatie van het programma vindt plaats door de inzet van gemengde teams bestaande uit medewerkers van het consortium en Defensie. Als Defensie niet in staat is de benodigde capaciteit beschikbaar te stellen, kan het programma vertraging oplopen of extra inzet van capaciteit vanuit het consortium vergen. In de oorspronkelijke business case is extra inzet niet voorzien. Binnen het programma is een capaciteitsproces ingericht om vroegtijdig knelpunten te signaleren. De vraag naar specialisten kan een knelpunt worden voor toekomstige blokken.
3. **Chipschaarste en lange levertijden.** Een effect van de wereldwijde pandemie is de verstoring van productie- en logistieke ketens. Dit leidde tot een wereldwijde chipschaarste. Door tekorten ontstonden leveringsproblemen in alle sectoren van producten waarin chips zijn verwerkt. Er is besloten de benodigde hardware vroegtijdig te bestellen waardoor geen knelpunten zijn ontstaan op dit gebied.
4. **Technologische ontwikkelingen en actuele behoefte Defensie leiden tot wijzigingen in onder andere het Technisch Ontwerp.** De IT ontwikkelt zich in een snel tempo. Voor opdrachtverstrekking wordt gecontroleerd welke producten gebruikt gaan worden en of deze nog steeds toekomstvast zijn. Onderdeel van de aanpak per blok is het bloksgewijs actualiseren van het technisch ontwerp, zodat altijd sprake is van een actueel technisch ontwerp.
5. **Contractuele geschillen.** Contractuele geschillen vormen een mogelijk risico. Er zijn in 2021 geen contractgeschillen geweest.
6. **Baten worden niet of slechts gedeeltelijk gerealiseerd.** Om te voorkomen dat de latere start van de bouw van het twin datacenter voor vertraging zorgt, is een interim housing strategie vastgesteld. Er is gekozen de huidige datacenters tijdelijk te benutten voor het onderbrengen van de eerste GrIT-diensten. Daarnaast zijn voorbereidingen gestart om eerder te beginnen met de security-blokken.
7. **Weerstand tegen veranderingen.** GrIT introduceert zowel nieuwe IT als een nieuwe beheerorganisatie, wat tot onrust kan leiden bij personeel. Er is daarom veel communicatie over de komst van GrIT met bijvoorbeeld voorlichtingssessies. Daarnaast is er veel aandacht voor opleidingen en is er begeleiding voor de zachte kant van de verandering.
8. **Externe factoren.**
   - Verkrijgen omgevingsvergunningen voor de bouw van de datacenters in het licht van de stikstofproblematiek. Voor het realiseren van de bouw van de nieuwe datacenters (BR-025 en BR-026) zijn omgevingsvergunningen noodzakelijk. In augustus 2021 is door het Rijksvastgoedbedrijf de aanvraag voor de omgevingsvergunningen voor het twin datacenter ingediend bij het bevoegd gezag. Om de kans op succes te vergroten zijn noodzakelijke stikstofreducerende maatregelen genomen en zijn externe stikstofdepositieberekeningen gemaakt voor de aanvraag. Uitvoering kan pas gestart worden na het verkrijgen van de onherroepelijke vergunningen. Eventuele bezwaar- en beroepsprocedures maken de doorlooptijd voor het verkrijgen van de omgevingsvergunningen onzeker. Dit heeft in 2021 niet tot consequenties voor de doorlooptijd van andere blokken geleid. De huidige datacenters blijven de continuïteit van de IT garanderen.
   - COVID-19. Gedurende de opstart van GrIT werd duidelijk dat de effecten van COVID-19 lang zouden kunnen duren. De voorziene intensieve samenwerkingssessies, workshops en teambuilding om het programma te starten moesten allemaal digitaal plaatsvinden.

Risico	Laatste inzicht	
	Kans	Impact
1. Onvoldoende regie	Klein	Zeer groot
2. Tekort aan menskracht	Zeer groot	Gemiddeld
3. Levertijden hardware door chiptekorten	Klein	Klein
4. Wijzigingen in TO als gevolg van technologische ontwikkeling en actuele behoefte Defensie	Gemiddeld	Klein
5. Contractuele geschillen (intentie)	Klein	Zeer groot
6. Afbouw van de huidige IT vindt niet (snel genoeg) plaats	Klein	Groot
7. Weerstand tegen de verandering binnen GII (medezeggenschap, bonden)	Klein	Klein
8. Externe factoren: (COVID-19, vergunningstrajecten, etc.)	Klein	Groot

Figuur 14 ***Risicotabel***

5.8 Regie en invulling samenwerking

In 2021 is een eerste update van het in paragraaf 4.4 beschreven exit-plan ontvangen.

5.9 Ontwikkelingen nieuwe organisatie

Binnen DMO/JIVC komt een afdeling Generieke Infrastructuur Services (GIS), voor de medewerkers van de gemengde teams. De vormgeving van de nieuwe DMO/JIVC-organisatie in relatie tot de doorontwikkeling van GrIT gebeurt in nauwe samenwerking met de medezeggenschapscommissie. Defensiemedewerkers kunnen solliciteren naar een functie bij GIS. De IT-Academy biedt leerlijnen aan zodat medewerkers zich geschikt kunnen maken voor deze nieuwe werkzaamheden, in principe zijn de huidige medewerkers basisgeschikt. De werving en selectie van deze GIS medewerkers vindt plaats tijdens de bouw van een bepaald blok, op deze manier kan opleiding en training gelijktijdig plaatsvinden en kan de medewerker op de nieuwe functie beginnen zodra de overdracht naar beheer plaatsvindt. Bij de nieuwe afdeling GIS wordt ook invulling gegeven aan het thema een leven lang leren, net als in de rest van de IT-organisatie.

5.10 Ontwikkelingen consortium

Zoals in media was te lezen vond in 2021 een wijziging plaats bij IBM. Er is een afsplitsing van IBM gemaakt, genaamd Kyndryl. In de nieuwe organisatie zijn de beheerde infrastructuur-diensten ondergebracht. Defensie is hier tijdig over geïnformeerd en heeft ingestemd met de overdracht van alle verplichtingen van IBM naar Kyndryl.

5.11 Communicatiemomenten 2021

De ontwikkelingen van het programma GrIT zijn op de volgende momenten gerapporteerd.

Kamerstuk	Titel	Datum
35728-2	Aanbieden commercieel vertrouwelijke definitieve business case GrIT	11-02-2021
n/a	Rapportage Rijksdashboard ICT	31-03-2021
27830-338	Afwijkingsrapportage t.o.v Defensie Projectenoverzicht 2020	19-05-2021
2021D24061	Definitief BIT-advies GrIT blokken	22-05-2021
31125-119	Reactie definitief BIT-advies GrIT blokken	17-06-2021
2021-0000177294	Onderzoeksrapport Voortgangsrapportage GrIT in het DPO 2021 - ADR	15-09-2021
27830-344	Defensie Projecten Overzicht 2021	21-09-2021

Tabel 1 ***Overzicht van momenten van informeren Tweede Kamer in 2021***

Bijlage A *Toelichting Blokken*

Hieronder een korte toelichting op de GrIT-blokken.

Defensie Mobiele Netwerk – BR-001

Door een zelfstandige Mobile Network Operator te worden, is Defensie in tijden van crisis niet langer afhankelijk van één telecomprovider. Er kan nationaal en internationaal worden *geroamed* over de gecontracteerde providers. Daarnaast kan de beveiliging worden verbeterd door de introductie van een eigen SIM-kaart.

Unified Communications – BR-002

Dit blok realiseert alle componenten om waar ook ter wereld veilig en betrouwbaar te kunnen communiceren via spraak, video of chat. Daarnaast wordt het mogelijk om veilig en vertrouwd samen te werken met grotere groepen via elke mobiele of vaste werkplek; onderling, met NAVO- en EU-partners en anderen.

Contact Center - BR-003

Dit blok realiseert alle componenten waarmee snel en effectief interne en externe *servicedesks* kunnen worden ingericht. De servicegerichtheid van de *servicedesks* worden hiermee vergroot waardoor gebruikers sneller geholpen kunnen worden.

Operational Chat - BR-004

Dit blok realiseert alle componenten waarmee snel en effectief gechat kan worden door operationele eenheden op basis van NAVO-standaarden. Hiermee kan altijd en overal effectief worden samengewerkt met NAVO-partners.

Critical Communications - BR-005

Dit blok realiseert alle componenten waarmee onder alle omstandigheden van en naar operationele eenheden kan worden gecommuniceerd op een veilige en betrouwbare manier, ook met partners.

End-User Devices - BR-006

In dit blok wordt het plaats- en tijdsonafhankelijk werken mogelijk gemaakt. Hiervoor is een ruim assortiment *devices* beschikbaar in elke gebruiksomstandigheid (statisch en ontplooid) en rubriceringscompartiment (LGI & HGI).

Individual Workspace - BR-007

De Individual Workspace biedt de gebruiker dezelfde functionaliteit op elk type apparaat (desktop, laptop, tablet en smartphone), op uniforme wijze.

IT Basis Toepassingen - BR-008

Dit blok voorziet in de IT Basis Toepassingen die elke gebruiker binnen Defensie nodig heeft. Dit zijn de standaard kantoorapplicaties. Ze zijn dan ook op alle werkplekken beschikbaar mits rubricering dit toestaat.

Collaboration & Communications Services - BR-009

Collaboration biedt een uniforme samenwerkingsruimte waar defensiemedewerkers documenten en kennis kunnen delen en (gelijktijdig) kunnen bewerken, zowel onderling als met partners. Onderdeel van dit blok is de beveiligde mailvoorziening.

Protected Core Network - BR-010

Het Protected Core Network (PCN) blok realiseert alle componenten om veilig en vertrouwd informatie te kunnen versturen. Het is bedoeld om virtueel netwerken te maken en te koppelen. Door de hoogste niveaus van NAVO-encryptiestandaarden (FMN-standaarden) te gebruiken kan snel en eenvoudig federatief met NAVO-partners worden samengewerkt.

Local Area Network - BR-011

Dit blok realiseert alle componenten om snel, veilig en vertrouwd lokale netwerken in te kunnen zetten.

Internet op de Legering - BR-012

Dit blok realiseert internettoegang, TV, radio en beldiensten in legeringsgebouwen van Defensie voor privégebruik. De internettoegang is een internetverbinding bij de serviceprovider en is niet te relateren naar Defensie.

Welfare - BR-013

De Welfare service levert bij uitzendingen en missies internettoegang, TV, streaming, radio en beldiensten voor privégebruik op schepen en basissen via commerciële satellietverbindingen.

Multi-Tenant DC LAN - BR-014

Het Multi-Tenant DCLAN is een virtuele netwerkscheiding in plaats van een fysieke netwerkscheiding. Hiermee kunnen meerdere defensieorganisaties parallel gebruikmaken van een gedeelde infrastructuur. De scheiding is dusdanig robuust dat de veiligheid van elk netwerk kan worden gewaarborgd.

Private Cloud Platform - BR-015

Het Private Cloud Platform levert een betrouwbaar, veilig, schaalbaar basisplatform voor het hosten van IT-toepassingen. Defensie kan hiermee nieuwe toepassingen invoeren die binnen de huidige IT niet ondersteund kunnen worden. Hierbij valt te denken aan de toepassing van *big data* en AI-toepassingen die significante eisen stellen aan de onderliggende datacentercapaciteit.

Storage Services - BR-016

Het blok Storage Services levert verschillende soorten opslagruimten voor onder andere deelbare bestanden, back-ups en archivering. Hiermee is Defensie in staat de groeiende hoeveelheid data effectief, betrouwbaar en efficiënt op te slaan.

Infrastructure as a Code - BR-017

Infrastructure as a Code is een voorziening die ervoor zorgt dat IT-diensten snel, foutloos en gecontroleerd uitgerold en aangepast kunnen worden.

IT Service Management - BR-018 – *Dit blok is vervangen door Project Beheer Processen*

IT Service Management biedt de *tooling* en bijhorende procedures om de Service Level Agreements te bewaken, sturen en rapporteren, inclusief de mogelijkheden om daarbij samen te werken met andere dienstverlenende partijen inclusief NAVO. Daarbij wordt een Self Service Portaal geleverd, welke gebruikt wordt om diverse IT en non-IT dienstverlening te bestellen.

IT Operational Management - BR-019

Dit blok levert alle componenten om de volledige Defensie IT, zowel statisch als ontplooid, 24/7 te kunnen bewaken op verstoringen. Hierdoor worden verstoringen sneller opgemerkt en waar mogelijk automatisch opgelost, zodat de IT-beheerorganisatie zich kan focussen op de meer complexe verstoringen.

Yellow Domain - BR-020

Het Yellow Domain is een speciaal rubriceringscompartiment. Dit omvat een geïntegreerde IT-managementomgeving, alsmede het Security Operations Center. Hiermee wordt de mogelijkheid geboden een totaaloverzicht te verkrijgen van de operationele en security status van het complete IT-landschap van Defensie.

Security Operations Center - BR-021

Dit blok realiseert alle componenten om de volledige Defensie IT (statisch en ontplooid) 24/7 te kunnen bewaken op security bedreigingen. Hiermee krijgen medewerkers snel en helder overzicht van alle complexe dreigingen die spelen zodat zij de juiste acties kunnen nemen via de Security Response Teams. Door automatisering worden simpele bedreigingen automatisch opgelost.

Identity & Access Management - BR-022

Identity & Access Management (IAM) beheert de digitale identiteit van defensiemedewerkers. Autorisaties van gebruikers voor informatiesystemen worden hiermee automatisch verstrekt én ingenomen op basis van diens bevoegdheden. Hiermee wordt de basis gelegd voor Attribute Based Access Control.

Information Exchange Gateway (IEG) - BR-023

Dit blok realiseert alle componenten om gebruiksvriendelijk, maar streng gecontroleerd, informatie tussen rubriceringscompartimenten uit te wisselen.

IT Toegangscontrole - BR-024

De IT-toegangscontrolefunctie levert gecontroleerd toegang tot data in het datacenter en voorkomt dat data ongecontroleerd het datacenter kan verlaten. Alleen bevoegde personen met geautoriseerde apparaten krijgen toegang tot data in het juiste rubriceringscompartiment.

Twin datacenter - BR-025

Het twin datacenter is het primaire datacenter van Defensie. De faciliteit bestaat uit twee onafhankelijke datacenters die door middel van een snelle netwerkverbinding synchroon gegevens kunnen uitwisselen. Dit biedt een zeer hoge bescherming tegen verstoringen en reduceert het risico op dataverlies tot nagenoeg nul. Het datacenter is ontworpen voor zowel LGI als HGI.

Uitwijk DC - BR-026

Het uitwijkdatacenter wordt gerealiseerd om het risico op de uitval van het twin datacenter verder te mitigeren. Dit uitwijkdatacenter borgt de beschikbaarheid van kritische IT-diensten door extra beschermende maatregelen. Het twin datacenter en het uitwijkdatacenter zijn middels beveiligde netwerken onderling verbonden.

Camp New Amsterdam (CNA) - BR-027

Doordat de nieuwe datacenters pas later beschikbaar komen, wordt Camp New Amsterdam (CNA) als tijdelijk startlocatie voor GrIT gebruikt. Hier is tijdelijke infrastructuur aangelegd om met GrIT te kunnen starten.

Operationele Compartimenten - BR-028

Het blok Operationele Compartiment (OC) is een centrale IT-voorziening (backend) ter ondersteuning van ontplooide eenheden. Deze centrale voorziening ondersteunt overal ter wereld eenheden met HGI- en LGI-ondersteuning.

Modules Ontplooid - BR-029

De Modules Ontplooid bieden lokale infrastructuur, basis IT-toepassingen en eenheidspecifieke applicaties voor missies of oefeningen. De modules zijn ontworpen om goed tegen stof, trillingen, temperatuurverschillen en vocht bestand te zijn en compact en hanteerbaar genoeg te zijn voor inzet in een ontplooide situatie.

Information Management - BR-030

Het blok Information Management levert de diensten voor het verwerken van informatie en bestanden en deze zowel vindbaar als veilig te maken door, waar mogelijk, automatische toevoeging van metadata, zoals rubricering.

Enterprise Integration Services – BR-031

De Enterprise Integration Service (EIS) zorgt voor de uitwisseling van gegevens tussen verschillende processen en applicaties. Door gegevens geautomatiseerd in een uniform format te zetten, kunnen ze door verschillende applicaties worden gebruikt en neemt de betrouwbaarheid en veiligheid van de gegevensuitwisseling toe.

Data Analytics & Visualisatie & Geo – BR-032

Dit blok levert de capaciteiten voor het verzamelen, verwerken en analyseren van grote hoeveelheden data, het beheer van (informatie op) kaarten en de presentatie van deze informatie.

Enterprise Search & Language Support - BR-033

Dit blok realiseert een krachtige en flexibele zoekmachine, waardoor goed kan worden gezocht binnen de systemen van Defensie en van externe partners. Ook worden diensten voor het vertalen van tekst gerealiseerd.

Wegwerken knelpunten in Huidige IT - BR-034

Om de Defensieapplicaties te kunnen migreren dienen een aantal knelpunten door de uitvoering van dit blok te worden opgelost.

Ontmantelen Defensie Applicaties (ODA) - BR-035

Het blok Ontmantelen Defensie Applicaties ruimt applicaties op die niet langer benodigd zijn voor de bedrijfsvoering.

MKA Hooggerubriceerd Informatiedomein (HGI) - BR-036

Dit Migratie Keep Applicaties (MKA)-blok migreert de applicaties uit het Hoog Gerubriceerde Informatiedomein (HGI) waarbij de continuïteit gewaarborgd blijft.

MKA Ontplooid - BR-037

Dit Migratie Keep Applicaties (MKA)-blok zorgt voor het beschikbaar stellen van de applicaties voor het Ontplooide domein, waarbij de continuïteit gewaarborgd blijft.

MKA LANTEK - BR-038

Dit Migratie Keep Applicaties (MKA)-blok migreert de LANTEK back-end applicaties waarbij de continuïteit gewaarborgd blijft. Lantek applicaties bevinden zich op Technische Werkplekken, waar afwijkende rechten nodig zijn voor bijvoorbeeld de aansturing van specifieke rand- of meetapparatuur.

MKA Confi - BR-039

Dit Migratie Keep Applicaties (MKA)-blok migreert de MULAN Confi applicaties waarbij de continuïteit gewaarborgd blijft.

MKA Laaggerubriceerd Informatiedomein - BR-040

Dit Migratie Keep Applicaties (MKA)-blok migreert de applicaties uit het Laag Gerubriceerde Informatiedomein (LGI) waarbij de continuïteit gewaarborgd blijft.

MKA KMAR - BR-041

Dit Migratie Keep Applicaties (MKA)-blok migreert de applicaties van de KMAR waarbij de continuïteit gewaarborgd blijft.

MKA Medisch - BR-042

Dit Migratie Keep Applicaties (MKA)-blok migreert de applicaties uit het Medische Informatiedomein waarbij de continuïteit gewaarborgd blijft.

MKA Hoogcomplex - BR-043

Dit Migratie Keep Applicaties (MKA)-blok migreert de hoogcomplexe applicaties (zoals SAP en Peoplesoft), waarbij de continuïteit gewaarborgd blijft.

Bijlage B *Lijst van begrippen en afkortingen*

AcICT	Adviescollege ICT-toetsing
ADR	Auditdienst Rijk
AP	Activiteitenplan
BIT	Bureau ICT-toetsing
CIO	Chief Information Officer
DBB	Defensie Beveiligingsbeleid
DMO	Defensie Materieel Organisatie
GES	Generieke Services
GIS	Generieke Infrastructuur Services
GrIT	Grensverleggende IT
HGI	Hoog Gerubriceerde Informatie
IMS	IT Operations
JIVC	Joint Informatievoorzienings Commando
LGI	Laag Gerubriceerde Informatie
MKA	Migratie Keep Applicaties
PB	Programma Board
PDC	Producten- & Dienstencatalogus
QA	Quality Assurance
SOC	Security Operations Center
TBS	Terbeschikkingstelling of exploitatie
TO	Technisch Ontwerp
TITAAN	Theatre Independent Tactical Adaptive Armed Forces Network
UP	Uitvoeringsplan

Ministerie van Defensie
Oktober 2022