HASKONINGDHV NEDERLAND B.V.
Laan 1914 no.35
3818 EX Amersfoort
Netherlands

+31 88 348 20 00 T
+31 33 463 36 52 F
info@rhdhv.com E
royalhaskoningdhv.com W

Bestuurstaf / Hoofddirectie Bedrijfsvoering
Directie Monitoring & Beheer /
Veiligheidsmanagement
Ministerie van Defensie
T.a.v. ir. A.J. de Waard
Kalvermarkt 32
2511 CB | 's-Gravenhage

| | | |
|---|---|---|
| Datum: | 7 oktober 2015 | Contact: |
| Uw kenmerk: | | Telefoon: |
| Ons kenmerk: | IEMBD7650L001F01 | E-mail: |
| Classificatie: | | |
| Bijlagen: | 1 | |

**Oplevering definitief rapport**

Geachte heer de Waard,

Hierbij ontvangt u onze definitieve rapportage Onderzoek bedrijfsveiligheid Defensie.

Ik hoop hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Senior Adviseur
Industry, Energy and Mining

RAPPORT

# Onderzoek bedrijfsveiligheid Defensie

Klant: Ministerie van Defensie

Referentie: IEMBD7650-102-100R001F02

Versie: 02/Finale versie

Datum: 7 oktober 2015

Royal HaskoningDHV
Enhancing Society Together

HASKONINGDHV NEDERLAND B.V.

Postbus 1132
3800 BC Amersfoort
Netherlands
Industry, Energy and Mining
Trade registration number: 56515154

+31 88 348 20 00 T
+31 33 463 36 52 F
info@rhdhv.com E
royalhaskoningdhv.com W

Titel document: Onderzoek bedrijfsveiligheid Defensie

Ondertitel: Bedrijfsveiligheid Defensie
Referentie: IEMBD7650-102-100R001F02
Versie: 02/Finale versie
Datum: 7 oktober 2015
Projectnaam: Onderzoek bedrijfsveiligheid Defensie
Projectnummer: BD7650-102-100
Auteur(s):

Opgesteld door: _____

Gecontroleerd door: _____

Datum/Initialen: _____

Goedgekeurd door: _____

Datum/Initialen: _____

Classificatie

Royal HaskoningDHV

# Inhoud



# Bijlagen

# Managementsamenvatting

In opdracht van de Hoofddirectie Bedrijfsvoering van het Ministerie van Defensie heeft Royal HaskoningDHV een onderzoek uitgevoerd naar bedrijfsveiligheid bij Defensie.

Het onderhavige rapport geeft antwoord op de onderzoekvragen omtrent het bereiken van eerdere doelstellingen bedrijfsveiligheid, het niveau van bedrijfsveiligheidbewustzijn bij Defensie, en of de onderhavige verbeterplannen leiden tot de realisatie van de gewenste doelen. Tot slot worden er aanbevelingen gedaan. Onder bedrijfsveiligheid worden in dit rapport alle veiligheidsaspecten verstaan, die relevant zijn in het kader van bedrijfsvoering en inzet van Defensie. Het onderwerp milieu valt hierbuiten.

De algemene conclusie is dat is de eerdere doelstellingen bedrijfsveiligheid in het beste geval voor een deel zijn gerealiseerd of later dan gepland zijn gerealiseerd.

Waar doelstellingen wel bereikt zijn lijkt dit vooral samen te hangen met continuïteit in de bezetting en beschikbaarheid van expertise. Dit lijkt samen te gaan met het belang dat men aan bedrijfsveiligheid hecht. Daarbij valt op dat dit vooral bedrijfsveiligheid betreft dat dichtbij de ‘kerntaak’ van Defensie ligt, en een hoogrisico karakter kent, zoals vliegveiligheid.

Waar doelstellingen niet of onvoldoende bereikt zijn, geldt in feite het tegenovergestelde hiervan. Het onderwerp bedrijfsveiligheid – en dan met name de bedrijfsveiligheid die verder van de ‘kerntaken’ ligt met minder in het oog springende risico’s - stond – voordat het Chroom-6 dossier in de publiciteit kwam - voorheen niet altijd bovenaan de agenda van de bedrijfsvoering zoals blijkt uit interviews en documenten. Ook het ontbreken van een duidelijk ambitieniveau, het ontbreken van een effectief monitoringsysteem en te weinig scholing met betrekking tot het thema bedrijfsveiligheid om de bewustwording te vergroten, heeft het behalen van de doelen belemmerd. Ook speelt het feit dat de ‘softe’ organisatiekenmerken (zoals leiderschap, communicatie en bewustzijn) in het veiligheidsbeleid onderbelicht zijn een duidelijke rol.

Uit de serie plannen en blauwdrukken die de afgelopen jaren het licht zagen blijkt dat het lastig was het niveau van aandacht en bewustzijn op te voeren. Het beeld dat wij kregen is dat er, juist op het moment dat dit begon te lukken, een golf van bezuinigingen en daarmee samenhangende reorganisaties over de Defensie organisatie kwam. De prille kiemen van een meer structureel bedrijfsveiligheidsbeleid ondervonden daarmee een ernstige tegenslag. Voorbeeld hiervan is de vertraging in het uitvoeren van risico-inventarisaties en de gestage afname van het aantal veiligheidsexperts.

Kijkend naar bedrijfsveiligheidbewustzijn in de breedste zin van het woord laat de organisatie een aantal ongeschreven regels zien die de effectiviteit van de beheersing van bedrijfsveiligheid in positieve maar ook in negatieve zin beïnvloeden. Één van de ongeschreven regels kan worden omschreven als: ‘Can do / fix it’. Deze staat voor de regel dat men tot het uiterste wil gaan om een gegeven opdracht uit te voeren. Dit mes snijdt aan twee kanten. Enerzijds staat het voor vindingrijkheid om onder gegeven moeilijke omstandigheden toch op een verantwoorde wijze het doel te bereiken. Anderzijds kan dit ook leiden tot improvisatie en daarmee afwijken van richtlijnen (meer risico nemen).

“We willen niet graag teleurstellen uit een groot gevoel van verantwoordelijkheid”, is een ongeschreven regel die in het verlengde van de hierboven beschreven regel ligt. Enerzijds helpt dit om de doelen te bereiken, anderzijds kan dit in de hand werken dat medewerkers (te) makkelijk “ja” zeggen terwijl zij weten dat er bijvoorbeeld te weinig capaciteit is om de opdracht succesvol of op een verantwoorde manier af te ronden.

Het effect van ongeschreven regels op bedrijfsveiligheid, het nemen van risico's en bewustwording worden nog te weinig expliciet besproken. Er is op alle niveaus weinig dialoog of expliciete bespreking van de dilemma's die ze met zich meebrengen. Gevolg: de ongeschreven regels hebben nog veel onvoorziene effecten op het veiligheidsbewustzijn en de praktijk. Pas wanneer ongeschreven regels in de pas lopen met geschreven regels, is er sprake van een effectieve veiligheidscultuur.

Het algemene beeld is dat de risicobeheersing van bedrijfsveiligheid op een overwegend 'reactief' niveau plaatsvindt, met enkele uitzonderingen waar zaken op een meer gestructureerd (calculatief) niveau geregeld zijn. Voor een aantal aspecten van bedrijfsveiligheid zoals vliegveiligheid is binnen onderdelen een minimaal proactief niveau bereikt. Dit toont aan dat Defensie zeer goed in staat is op deze niveaus te opereren, maar dat ze deze benadering nog niet heeft kunnen toepassen op alle aspecten van bedrijfsveiligheid.

Om een duurzame verbetering van bedrijfsveiligheid te verkrijgen adviseren wij het volgende:

*Beleid / doel en taakstellingen*

1. Zet bedrijfsveiligheid 'op de agenda' door het integraal onderdeel te maken van alle andere prestatiegebieden en daarvoor op gelijke wijze ambities en doelstellingen te formuleren. Daarbij hoort onder meer een streefcijfer met betrekking tot het verminderen van het aantal ongevallen, dat gebaseerd is op een betrouwbare registratie van de optredende ongevallen. Teneinde commitment te verkrijgen is het raadzaam om in de vorm van workshops gemeenschappelijk het ambitieniveau te bepalen. Dit niveau mag variëren voor de korte en lange termijn en rekening houden met het niveau waarop individuele onderdelen zich op dit moment bevinden.

2. Werk ambities en doelstellingen uit naar acties (en leg een verband met reeds vastgestelde acties) en zorg voor systematisch voortgangsrapportage (zie uitwerking hieronder) Zie punt 1.7, 1.8 en 2.1 van de Nota 'Inrichting en onderhouden van het Bedrijfsveiligheidhuis Defensie'.

3. Ontwikkel een (in eerste instantie eenvoudig) KPI – dashboard. Cascadeer deze door alle lagen van de organisatie; denk aan KPI's 'op lagging niveau (incidenten) en leading niveau (bijvoorbeeld inspecties uitgevoerd conform planning, uitgevoerde trainingen, gerealiseerde verbetermaatregelen etc.). Op deze manier wordt de voortgang van prestaties en verbeteracties systematisch en transparant bijgehouden.

*VMS DEF (Implementatie en Monitoring)*

4. Laat de eenheden naar eigen inzicht (maatwerk) het VMS implementeren, op basis van het VMS Def als kapstok. Zorg voor invulling van de rol hierbij van het hoger management inclusief de SG en de BS in het aansturen en monitoren van het veiligheidsmanagement en de continue verbetering daarvan. Dit verduidelijkt de strategie en verhoogt de druk op de delen van de organisatie die nog niet gereed zijn met opzet en implementatie van het VMS op alle niveaus. Geef daarvoor de hoofdlijnen en versterk en stroomlijn het proces van auditing en review. Vermijdt detailvoorschriften, tenzij eenheid overschrijdende procedures mogelijk en zinvol zijn, in dat geval kan men zoveel mogelijk gezamenlijke procedures opstellen of 'Defensie Guidelines' hanteren.

5. Versterk het toezicht op implementatie en effectiviteit van het VMS op alle niveaus en introduceer daarvoor bijvoorbeeld een, pragmatisch, eenduidig systeem van '(zelf-)beoordeling' waarmee de 'volwassenheid' van het VMS Def aan de hand van een puntenschaal kan worden beoordeeld. Neem in dit systeem de "softe kant" van het veiligheidsmanagement op, te weten: leiderschap, communicatie, bewustzijn. Zo beschikt de organisatie over een beeld van het 'volwassenheidsniveau'

en de kwaliteit van de implementatie van het veiligheidsmanagement en is er tegelijkertijd ook een duidelijk verwachtingskader beschikbaar. Dit in aansluiting op de aanwijzing HDBV – 005: monitoring en toezicht.

6. Overweeg certificering van het Defensie managementsysteem voor bedrijfsveiligheid volgens een voor defensie geschikte norm verplicht te stellen. Hiermee wordt het proces van directie-beoordeling, doelen stellen versterkt en werkt een uniforme aanpak in de hand.

*Veiligheidsbewustzijn*

7. Verbeter de interactie tussen lijn en staf. Dit kan door meer aandacht te besteden aan veiligheidsmanagement in de opleiding van de lijn (zie onderstaande) en door het denken op systeemniveau bij de staf te versterken. Zie punt 1.9 van de Nota 'Inrichting en onderhouden van het Bedrijfsveiligheidshuis Defensie'.

8. Borg kennis over bedrijfsveiligheid in de kaderopleidingen( voor het lijnmanagement). Denk hierbij aan kennisoverdracht over de werking van het managementsystemen en integraal risicomanagement, maar ook over voorbeeld -rol van de lijn, de invloed van ongeschreven regels op het functioneren van managementsystemen, effectieve leiderschapsstijlen en het beoogde ambitie niveau. Zie punt 1.9 van de Nota 'Inrichting en onderhouden van het Bedrijfsveiligheidshuis Defensie'.

9. Naast de aanbevelingen in het voorgaande achten we het noodzakelijk het bewustzijn ten aanzien van bedrijfsveiligheid te bevorderen op alle lagen van de organisatie, door de stijl van leidinggeven en de heersende 'ongeschreven' regels te plaatsen in het perspectief van een veilige operatie. Identificeer en bespreek de stijl van leidinggeven en de 'ongeschreven regels' op alle niveaus in de organisatie en ga de dialoog aan over wat ze betekenen in het licht van veiligheid, bijvoorbeeld aan de hand van workshops met een tool als 'Understanding your culture' uit het programma 'Winning Hearts and Minds'. Zie ook punt 1.1 van de Nota 'Inrichting en onderhouden van het Bedrijfsveiligheidshuis Defensie'.

*Toereikendheid bedrijfsvoeringorganisatie*

10. Zorg voor voldoende capaciteit van specialisten op het gebied van bedrijfsveiligheid.

11. Benut de positieve kanten van het rouleringssysteem – zoals uitwisseling van ervaringen en best practice – en voor uitwisseling tussen de onderdelen ook op het niveau onder de Bestuursstaf om 'goede gewoontes', die in verschillende onderdelen zijn ontwikkeld, op een natuurlijke manier tot gemeengoed te maken.

# 1 Inleiding

## 1.1 Aanleiding

Defensie streeft een verdere verbetering na van de zorg voor veiligheid, gezondheid en milieu in al haar werkzaamheden en operaties. Als startpunt wenst de organisatie inzicht te verkrijgen in de effectiviteit van het tot nu toe gevoerde bedrijfsveiligheidsbeleid en de geleverde inspanningen op dit terrein, en in mogelijke verbeteringen daarin.
Ten aanzien van de terminologie moet in dit rapport onder bedrijfsveiligheid worden verstaan 'veilig en gezond werken en de zorg voor de arbeidsomstandigheden'. De bredere definitie waarbij Defensie ook het aspect 'milieu' tot bedrijfsveiligheid rekent, is in dit rapport niet van toepassing.

## 1.2 Onderzoeksvraag

Defensie heeft opdracht gegeven aan Royal HaskoningDHV de volgende onderzoeksvragen te beantwoorden:

1. Vragen met betrekking tot doelstellingen:
   a. In welke mate zijn eerdere doelstellingen bedrijfsveiligheid bereikt?
   b. Wat zijn de oorzaken in de gevallen waarin de doelstellingen niet zijn bereikt?
   c. Welke aanbevelingen zijn er om toekomstige doelstellingen wel te realiseren?

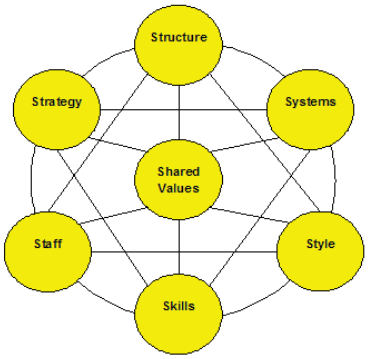
2. Vragen met betrekking tot het bedrijfsveiligheidsbewustzijn
   a. Wat is het huidige niveau van bedrijfsveiligheidsbewustzijn bij Defensie?
   b. Is dit niveau voldoende voor een verantwoorde bedrijfsvoering?
   c. Wat zou het niveau moeten zijn?
   d. Welke aanbevelingen zijn er om het niveau van bedrijfsveiligheidbewustzijn te verhogen, als blijkt dat dit momenteel te laag is

3. Vragen met betrekking tot verbeterplannen:
   a. Zullen de voorliggende verbeterplannen op het gebied van bedrijfsveiligheid van Defensie leiden tot de realisatie van de gewenste doelen?
   b. Indien niet het geval, welke verbetersuggesties zijn er op basis van o.a. de bevindingen over vragen 1 en 2 om de gewenste doelen wel te bereiken?

Onder bedrijfsveiligheid verstaan we in dit rapport alle veiligheidsaspecten die relevant zijn in het kader van bedrijfsvoering en inzet van Defensie. Het onderwerp milieu valt hierbuiten.

## 1.3 Aanpak en opzet van het onderzoek

Om de onderzoeksvragen met betrekking tot het bereiken van doelstellingen en het niveau van bedrijfsveiligheidbewustzijn in de volle breedte te beoordelen en om advies te geven over maatregelen voor verbetering, heeft Royal Haskoning DHV het "**7S Frameworkmodel**" van McKinsey (zie figuur 1.1 7s frameworkmodel) gebruikt in combinatie met de indeling in 'volwassenheidsniveaus' van het programma **'Winning Hearts en Minds'** (zie figuur 1.2hearts and minds'). De combinatie van deze modellen geeft een goed analysekader voor de beantwoording van de onderzoeksvragen.




*Figuur 1.1 7S Frameworkmodel*


*Figuur 1.2Hearts and Minds*

Het 7S-model is een systeem om een organisatie en haar prestaties te analyseren. De zeven 'S'-elementen zijn verdeeld in drie 'harde'(strategie, structuur en systemen) en vier 'zachte'(stijl, significante gemeenschappelijke waarden, sleutelbekwaamheden en staf) elementen. De elementen beïnvloeden elkaar en de 'shared values' vormen de basis voor de kwaliteit van de andere factoren. McKinsey wijst op het belang van de interactie tussen de organisatie-elementen. Een succesvolle organisatie zal deze sleutelelementen bekijken als een soort van kompassen die – om de effectiviteit van het beleid te maximaliseren - alle in eenzelfde richting zullen moeten wijzen.

Elke S is beïnvloedbaar. Staf, Strategie, Structuur en Systemen kunnen vaak op korte termijn worden veranderd of bijgesteld. De drie andere elementen worden door McKinsey traag-variabelen genoemd. Veranderingen in Stijl, Sleutelbekwaamheden en Shared values (gedeelde waarden /cultuur) nemen meer tijd in beslag. Meer in detail kunnen de elementen als volgt beschreven worden:

1. Strategie
   Hoe komt bedrijfsveiligheid aan de orde als onderdeel van visie, missie en strategie van Defensie en hoe wordt hierover gecommuniceerd.
2. Structuur
   Hoe is de organisatie rond het onderwerp bedrijfsveiligheid ingericht, hoe zijn de taken en verantwoordelijkheden belegd en hoe is de samenwerking en kennisuitwisseling tussen onderdelen geborgd.
3. Systemen
   Hoe is het veiligheidsmanagementsystemen (VMS DEF) ingericht en geïmplementeerd, hoe wordt dit systeem onderhouden en hoe functioneert de 'plan-do – check act' cyclus. Wat is de kwaliteit van risicoanalyses (RI&E), wat is de voortgang van verbeterplannen en uitvoeringsprogramma's, welke KPI's worden gehanteerd voor veiligheid en wat is de kwaliteit van registratie en onderzoek van incidenten, van risico-analyses.
4. Stijl
   Wat is de kwaliteit van leiderschap en betrokkenheid in termen van voorbeeldgedrag, daadkracht, sturen op gewenste safety performance en doelen, toezicht en handhaving van veiligheidsvoorschriften. En wat is de kwaliteit van communicatie en besluitvorming over operationele dilemma's en problemen en de aandacht voor deze aspecten in training en coaching van het management.

5 Sleutelbekwaamheden
Welke kennis, bekwaamheden en competenties zijn met betrekking tot bedrijfsveiligheid - herkenbaar aanwezig en wat is het leervermogen van de organisatie bij nieuwe uitdagingen.

6 Staf:
De factor staf gaat over het personeel binnen het bedrijf. Welke rol speelt het aspect veiligheid in het rekruterings- en selectiebeleid en het personeelsbeleid.

7 Shared Values / gemeenschappelijke waarden
De shared values vertegenwoordigen de bedrijfscultuur, de waarden en normen maar ook de ongeschreven regels die binnen een organisatie heersen en zijn in grote mate bepalend voor de kwaliteit van de andere aspecten.

In het kader van dit onderzoek gebruiken we tevens het 'Hearts and Minds' model (figuur 1.2) om ook de shared values goed te duiden. Het onderscheidt 5 niveaus van 'veiligheidsbewustzijn' van een organisatie:

- Pathologisch: veiligheid moet wijken voor alle andere bedrijfsdoelen, zoals winst en marktpositie.
- Reactief: veiligheid is van belangrijk: 'we doen er veel aan telkens wanneer iets mis gaat"
- Calculatief: men gaat ervan uit dat regels en systemen voldoende zijn om ongevallen te voorkomen en is erg gericht op kwantitatieve informatie en afwegingskaders.
- Proactief: men realiseert zich dat regels niet voldoende zijn om ongevallen te voorkomen, maar dat het ook een kwestie is van actieve betrokkenheid en 'mindset' van management en personeel.
- Generatief: hier heeft de organisatie de typische 'high reliability organization' kenmerken: alert zijn ook op kleine fouten, niet simplificeren, in contact blijven met de operationele praktijk, borgen van veerkracht en zoveel mogelijk gebruik maken van aanwezige expertise en praktijkervaring.

Onze stelling is dat het bereiken van de doelstellingen bedrijfsveiligheid in overwegende mate afhankelijk is van het functioneren van de 7 elementen met als kern de gemeenschappelijke waarden ofwel het bedrijfsveiligheidbewustzijn. De verdere operationalisering van het onderzoek bestaat uit een nadere uitwerking van vragen betreffende de 7 elementen in combinatie met de 5 niveaus van het model van Hearts and Minds.

De gegevens zijn verzameld via documenten en een serie interviews met een dwarsdoorsnede van personen in de gehele Defensieorganisatie. De selectie van documenten en te interviewen personen is hoofdzakelijk door Defensie uitgevoerd. In totaal zijn 44 functionarissen uit de bestuursstaf en alle defensieonderdelen geïnterviewd, verdeeld over het hoger management, het middelmanagement en staf, zie bijlage 2. Tevens zijn korte rondgangen uitgevoerd bij o.a. Marine basis Den Helder.

Hoofdstuk 2 bevat onze bevindingen, conclusies en aanbevelingen.

Bijlagen 1 en 2 bevatten een overzicht van geraadpleegde documenten en geïnterviewde personen.

# 2 Beantwoording van de onderzoeksvragen

In dit hoofdstuk beantwoorden we de onderzoeksvragen. Per vraag vermelden we onze bevindingen, onze beoordeling en conclusies daarover en de daarop gebaseerde aanbevelingen.

Onze beoordeling is geformuleerd in termen van de 5-punts schaal van het Hearts and Minds model, dat de eerder beschreven 5 niveaus van 'veiligheids-volwassenheid' van een organisatie onderscheidt.

## 2.1 Onderzoeksvraag 1 a: In welke mate zijn eerdere doelstellingen bedrijfsveiligheid bereikt?

*Bevindingen:*

- Op verschillende momenten zijn er verschillende sets doelstellingen voor bedrijfsveiligheid geformuleerd. Er is een reeks nota's waarin doel- en taakstellingen en kaders op het gebied van bedrijfsveiligheid zijn aangegeven, onder andere: Doel- taakstellingen 2009, 2011 en blauwdrukken. Aan de realisatie hiervan wordt momenteel gewerkt.
- Er heeft tot voor kort geen structurele voortgangscontrole plaatsgevonden op de realisatie van doelstellingen. Binnen een aantal individuele afdelingen en onderdelen is dit wel gebeurd, maar voor Defensie als totaal ontbreekt een 'dashboard' waaruit de voortgang kan worden afgelezen. In 2011 zijn de volgende hoofddoelstellingen geformuleerd:
  - Doelstelling 1: Aantoonbaar verbeteren van inrichting en werking Veiligheidsmanagementsysteem Defensie.
  - Doelstelling 2: Opzet database (RIAS) en beschikken over geactualiseerde risicoanalyses voor de meest kritieke processen.
  - Doelstelling 3: Vaststellen en uitvoeren van verbetermaatregelen

Beoordeling en conclusie

- Voor de bovenstaande doelstellingen uit 2011 constateren we - voor zover door ons te beoordelen – dat elk van deze doelstellingen in het beste geval deels of later dan gepland gerealiseerd is.

## 2.2 Onderzoeksvraag 1 b: Wat zijn de oorzaken in de gevallen waarin de doelstellingen niet zijn bereikt? En

## Onderzoeksvraag 1 c: Welke aanbevelingen zijn er om toekomstige doelstellingen wel te realiseren.

Deze vragen beantwoorden we beide in het onderstaande. Oorzaken die bijgedragen hebben aan de situatie waarin doelstellingen niet zijn bereikt, zijn door ons gerelateerd aan het functioneren van de kernelementen van de organisatie: strategie, systemen, organisatiestructuur, staf en sleutelbekwaamheden. Per element geven we onze bevindingen, conclusies en aanbevelingen.

*Bevindingen in de relatie tot de strategie*
Dit onderdeel beschrijft bedrijfsveiligheid als onderdeel van visie, missie en strategie van Defensie en hoe hierover wordt gecommuniceerd.

- Er is een reeks nota's waarin doel- en taakstellingen en kaders op het gebied van bedrijfsveiligheid zijn aangegeven: onder andere: Doel- en taakstellingen 2009, 2011 en blauwdrukken. De hierin geformuleerde doelen zijn vooral 'instrumenteel' geformuleerd (in termen van acties). Het 'waarom' ofwel het uiteindelijk te bereiken resultaat van de benoemde acties wordt echter niet altijd duidelijk. We hebben geen informatie aangetroffen over het gewenste ambitieniveau ("stip aan de horizon") en strategie met betrekking tot bedrijfsveiligheid en de wijze waarop doelen daarvan zijn afgeleid.
- Niet alle benoemde doelen zijn 'smart' geformuleerd of naar KPI's vertaald, zodat het bereiken ervan niet altijd objectief vastgesteld kan worden. Vooralsnog ontbreekt het aan een uitontwikkeld "dashboard" waarmee het Veiligheid Managementsysteem Defensie (VMS) Def op corporate of BS en lagere niveaus op haar functioneren en effectiviteit, gemonitord kan worden. Binnen een aantal organisatieonderdelen zien we hier overigens wel goede voorbeelden van of aanzetten voor, zoals het monitorsysteem van CLAS Matlogco.
- Sinds 2014 zijn diverse verbetermaatregelen op beleidsniveau doorgevoerd. In interviews is aangegeven, dat monitoring en control daarvan wordt verbeterd. Een risk board is in ontwikkeling, zie onder andere de Nota: Monitoring & Toezicht Jaarplan HDBV 2015 en de Nota Inrichten en onderhouden van het Bedrijfsveiligheidhuis Defensie 2014.
- Vanuit de BS meldt men een zichtbaar toegenomen committment van de top van de organisatie, het onderwerp komt aan de orde in de juiste fora en er is een beginnende controle op voortgang van acties en bereiken van geformuleerde doelen. Men spreekt het streven uit om een meer proactief beleid te voeren en wil men af van de 'risico-regel reflex'. Men is zich ervan bewust dat de organisatie 'arbo regels' in het verleden beschouwde als 'iets van buiten'. Voldoen aan de wet' lijkt daarmee praktisch gezien, impliciet de eerste ambitie voor de komende tijd.
- Geïnterviewden signaleren dat de strategie van bezuinigen op ondersteunende diensten en minder op operationele capaciteit een prioriteit is, die uiteindelijk vroeg of laat ook de operationele inzetbaarheid aantast (zoals dezer dagen ook is aangegeven in een rapport van de Algemene Rekenkamer – Verantwoordingsonderzoek 2014). Dit proces wordt in de veiligheidskunde 'drift into failure' genoemd. Dit is een geleidelijk proces waarvan de gevolgen lang verborgen blijven, maar uiteindelijk grote gevolgen hebben, ook voor het niveau van bedrijfsveiligheid. Als voorbeeld noemt met het' Chroom-6 dossier'. Om goed voorbereid te zijn op vragen en aantijgingen blijkt hoe belangrijk het is om alle gegevens centraal beschikbaar te hebben en toegankelijk. Hier is ruimte voor verbetering.

*Beoordeling en conclusies*

- Op het niveau van strategie en beleid met betrekking tot het aspect bedrijfsveiligheid staat Defensie overwegend op reactief niveau, op sommige plaatsen op calculatief niveau. Wel duiden de huidige initiatieven om bedrijfsveiligheid beter te borgen in de organisatie op een groei naar tenminste 'calculatief' niveau.
- Door het ontbreken van een duidelijk geformuleerd ambitieniveau is het lastig om verbeterstappen te formuleren anders dan het opzetten en formeel implementeren van een systeem: het VMS Def. Defensie lijkt expliciet vooral te streven naar 'Het voldoen aan wet', maar daarmee riskeert Defensie:
  - gebrek aan te focus op de grote risico's, en op nieuwe of onbekende risico's;
  - te weinig aandacht voor continu verbeteren;
  - en het verwisselen van doel en middel (voorbeeld: RIE document als doel en niet de inhoud van de RIE als middel om beheersing van risico's te verbeteren).

*Aanbevelingen*

- Zet bedrijfsveiligheid 'op de agenda' door het integraal onderdeel te maken van de bedrijfsvoering en van alle andere prestatiegebieden en daarvoor op gelijke wijze ambities en doelstellingen te formuleren. Daarbij hoort o.a. een streefcijfer m.b.t. het verminderen van het aantal ongevallen wat gebaseerd is op een betrouwbare registratie van de optredende ongevallen. Teneinde commitment te verkrijgen is het raadzaam om bijvoorbeeld in de vorm van workshops, met de belangrijkste stakeholders. gemeenschappelijk het ambitieniveau te bepalen. Dit niveau mag variëren voor de korte en lange termijn en rekening houden met het niveau waarop individuele onderdelen zich op dit moment bevinden. Verder is het van belang om uitvoerende taken m.b.t. bedrijfsveiligheid zo veel mogelijk in de lijn te beleggen.
- Werk ambities en doelstellingen uit naar acties (en leg een verband met reeds vastgestelde acties) en zorg voor systematisch voortgangsrapportage (zie uitwerking hieronder). Zie punt 1.7, 1.8 en 2.1 van de Nota 'Inrichting en onderhouden van het bedrijfsveiligheidshuis Defensie'.

*Bevindingen in de relatie tot het systeem*

Dit onderdeel beschrijft hoe het veiligheidsmanagementsysteem (VMS DEF) is ingericht en geïmplementeerd, hoe dit systeem wordt onderhouden en hoe de 'plan-do – check act' cyclus functioneert: wat is de kwaliteit van risicoanalyses (RI&E), wat is de voortgang van verbeterplannen en uitvoeringsprogramma's, welke KPI's worden gehanteerd voor veiligheid en wat is de kwaliteit van registratie en onderzoek van incidenten en van risicoanalyses.

- Conform de Nota's over doel- en taakstellingen heeft ieder defensieonderdeel de vrijheid gekregen om het VMS Def specifiek te maken van voor haar organisatiekenmerken. Zo wordt bijvoorbeeld het ISRS model gehanteerd bij DMO Munitiebedrijf, Personeel Risico Management bij de Landmacht en de NTA 8620 bij de luchtmachtbasis Eindhoven. Daar werkt men aan de opzet van een geïntegreerd managementsysteem voor 10 compliance gebieden, waaronder bedrijfsveiligheid.
- De implementatiegraad van het VMS verschilt per organisatieonderdeel. Bijvoorbeeld: bij DMO is dit jaar voor het eerst een directiebeoordeling opgesteld. Bij andere defensie onderdelen zoals Luchtmacht of KMar loopt de cyclus: directiebeoordeling - opstellen jaardoelstellingen al enige jaren. Dit wisselend beeld wordt bevestigd door een aantal externe onderzoeken (auditrapporten en ILT rapport) laten nog diverse tekortkomingen zien ten aanzien van de werking van het VMS.
- Met betrekking tot de implementatie van de in het VMS beschreven processen en met name het proces van risico-inventarisatie tot en met risicobeheersing, dat het hart vormt van een VMS, is een soort 'vicieuze cirkel' waarneembaar: Het opstellen van risico-inventarisaties en evaluaties (RIE's) -

inclusief toetsing door CEAG) is bij veel onderdelen nog niet voltooid. Dit wijt men veelal aan capaciteitsgebrek door de recente bezuinigingen en reorganisaties. Gevolg is dat RIE's niet beschikbaar, onvolledig of wellicht onjuist zijn en dat de daarop te stoelen verbeterplannen (plan van aanpak) ontbreken of een verkeerde prioriteitstelling of maatregelen bevatten. Wanneer er wel een plan van aanpak is wordt de uitvoering hiervan en het nemen van beheersmaatregelen vaak vertraagd door de centralisering of uitbesteding van diensten. Daarbij kwam bij verschillende interviews aan de orde dat sommige onderdelen het uitvoeren van RIE's als doel lijken te zien en niet als middel: men denkt klaar te zijn als de RIE rapportages beschikbaar zijn terwijl men dan juist aan de slag moet met de inhoud ervan.

- Inspectie en toezicht op implementatie en effectiviteit van maatregelen vanuit verschillende lagen in de organisatie varieert sterk en is niet altijd geborgd, omdat een deel van deze taken (bijvoorbeeld inspecties en keuringen van materieel en gebouwen) is gecentraliseerd. Door capaciteitsgebrek of gebrek aan specifieke expertise bij centrale of ingehuurde diensten schiet dit proces soms tekort. Een aantal geïnterviewden gaf aan dat zij in de huidige situatie het 'systeemtoezicht' vanuit bijvoorbeeld BS onvoldoende vinden om vast te stellen of risico's beheerst zijn, zeker ook waar externe dienstverleners een rol spelen.
- Ook het proces van melding en onderzoek van incidenten varieert sterk in kwaliteit. Ongevallen worden over het algemeen gemeld, maar de melding van bijna ongevallen en gevaarlijke situaties is nog niet overal een routine. Voor onderzoek van meldingen is een cursus opgezet, maar door het rouleren van functies is niet geborgd dat betrokken functionarissen deze ook hebben gevolgd. De database waarin meldingen worden geregistreerd, maakt geen uitgebreid scala van analyses mogelijk. Sommige eenheden gebruiken daarom 'workarounds' om toch trendanalyses te kunnen maken, wat tot nauwkeuriger inzicht leidt, maar wel weer extra inspanning vergt. Ook op BS niveau worden trendanalyses uitgevoerd, maar dit leidt nog niet tot een duidelijk verbeterprogramma.
- Het 'operational risk management' bij de actieve inzet van schepen of vliegtuigen lijkt een meer proactief en geborgd proces, mede doordat men zich bewust is van de grote en manifeste risico's die hier spelen. Risico's mijden is hier in veel gevallen geen optie, het gaat hier om bewust nemen en managen van risico's. Risico's worden voortdurend expliciet gecheckt, beoordeeld en beheerst. Het 'opwerken' naar operationeel niveau van schepen bijvoorbeeld loopt via een 6-tal 'operational readiness checks' waarmee objectief wordt aangetoond wat het prestatieniveau van schip en bemanning is.
- Bij daadwerkelijke inzet geeft men aan te werken met een zorgvuldig proces van risicoanalyse, briefing, debriefing en evaluatie. Of, zoals in een interview werd gezegd: 'er is geen democratischer organisatie dan de krijgsmacht: tijdens inzet moet je de opdracht uitvoeren maar in de voorbereiding mag iedereen meepraten en na afloop mag iedereen zijn zegje doen'. Expliciete aandacht voor bedrijfsveiligheid voorafgaand aan en tijdens inzet verschilt wel per onderdeel, niet altijd wordt hierbij bijvoorbeeld veiligheidskundige expertise structureel ingeschakeld.

*Beoordeling en conclusies*

- De werking van het systeem is overwegend reactief, voorbeelden van een proactieve aanpak zijn te vinden op specifieke situaties zoals inzet en vliegveiligheid, maar dit heeft nog weinig 'spin off' naar andere aspecten van bedrijfsveiligheid.
- VMS DEF heeft duidelijk richting gegeven aan de inrichting van VMS op het niveau van de onderdelen. Maar de grote variatie in benaderingen doet vermoeden dat men weinig uitwisselt. De PDCA cyclus is niet overal in voldoende mate gesloten:
- Er zijn veel plannen, maar deze zijn niet altijd concreet of gebaseerd op een goede risicobeoordeling.

- Uitvoering van plannen - de ‘do’ - fase loopt regelmatig vertraging op door organisatorische problemen.

- Monitoring en toezicht - de ‘check’ fase - is een onvoldoende uniform proces waarbij soms criteria voor beoordeling ontbreken. In principe is onderkend dat eerste- tweede- en derdelijns toezicht nodig is (in andere termen, product, proces en systeem toetsen), maar we zien een gebrek aan capaciteit (zowel kwalitatief als kwantitatief) om toets- en toezichtstaken op een voldoende niveau uit te voeren. Dit geldt ook voor onderzoek en (trend-) analyse van incidenten.
- Het verbeterproces - de ‘act’ of ‘adjust’ fase - is vooral reactief van aard: oplossen van problemen zonder dat structurele oorzaken echt worden aangepakt. Hierdoor is er nog geen sprake van een systeem dat het continu verbeteren van de organisatie faciliteert. Zie de ervaringen rond het Chroom-6 dossier en het asbest dossier.

*Aanbevelingen*

- Laat de eenheden naar eigen inzicht (maatwerk) het VMS implementeren, op basis van het VMS Def als kapstok. Zorg voor invulling van de rol van de top van de organisatie inclusief de SG en de BS in het aansturen en monitoren van het veiligheidsmanagement en de continue verbetering daarvan. Dit verduidelijkt de strategie en verhoogt de druk op de delen van de organisatie die nog niet gereed zijn met opzet en implementatie van het VMS op alle niveaus. Geef daarvoor de hoofdlijnen en stroomlijn het proces van auditing en review (zie uitwerking hieronder). Vermijdt detailvoorschriften, tenzij eenheid overschrijdende procedures mogelijk en zinvol zijn, in dat geval kan men zoveel mogelijk gezamenlijke procedures opstellen of ‘Defensie Guidelines’ hanteren.
- Ontwikkel een (in eerste instantie eenvoudig) KPI – dashboard. Cascadeer deze door alle lagen van de organisatie; denk aan KPI’s ’op lagging niveau (incidenten) en leading niveau (bijvoorbeeld inspecties uitgevoerd conform planning, uitgevoerde trainingen, gerealiseerde verbetermaatregelen etc.). Op deze manier wordt de voortgang van prestaties en verbeteracties systematisch en transparant bijgehouden. Wees er alert op dat de KPI een middel blijft en geen doel op zich wordt.
- Versterk het toezicht op implementatie en effectiviteit van het VMS op alle niveaus en introduceer daarvoor een, pragmatisch, eenduidig systeem van ‘(zelf-)beoordeling’ waarmee de ‘volwassenheid’ van het VMS Def aan de hand van een puntenschaal kan worden beoordeeld. Neem in dit systeem de “softe kant” van het veiligheidsmanagement op, te weten: leiderschap, communicatie, bewustzijn. Zo beschikt de organisatie over een beeld van het ‘volwassenheidsniveau’ en de kwaliteit van de implementatie van het veiligheidsmanagement en is er tegelijkertijd ook een duidelijk verwachtingskader beschikbaar. Dit in aansluiting op de aanwijzing HDBV – 005: monitoring en toezicht.
- Overweeg certificering van het Defensie managementsysteem voor bedrijfsveiligheid volgens een voor defensie geschikte norm verplicht te stellen. Hiermee wordt het proces van directie-beoordeling, doelen stellen versterkt en werkt een uniforme aanpak in de hand.

*Bevindingen in de relatie tot structuur*

Dit onderdeel beschrijft hoe de organisatie bedrijfsveiligheid ingericht, hoe de taken en verantwoordelijkheden zijn belegd en hoe de samenwerking en kennisuitwisseling tussen onderdelen is geborgd

- De lijn ‘is verantwoordelijk’ in formele zin, maar in de praktijk wordt het initiatief veelal genomen door de specialisten. Soms kan dat leiden tot een afwachtende houding van de lijn. Het competentieniveau en de bezetting van de veiligheidsstaf wisselt. Er zijn maar enkele onderdelen die erin geslaagd zijn de bezetting ondanks de druk om te bezuinigen op peil te houden. In een aantal gevallen mist men een stafadviseur met een ‘helikopterview’ die kan meedenken bij het effectief implementeren van het VMS

Def. Daarnaast is de positie van de veiligheidstaf niet altijd eenduidig qua niveau in de organisatie, en qua rol: soms ‘controleur’, soms adviseur.

- De overgang naar een procesgerichte organisatie heeft geleid tot het gevoel dat niemand verantwoordelijk is voor het eindresultaat op gebied van veiligheid. ‘De lijn is ervan’ - is formeel wel verantwoordelijk maar niet altijd bevoegd - want afhankelijk van andere organisatieonderdelen om te inspecteren, te onderhouden en verbetermaatregelen te nemen (centralisering diensten, zoals o.a. Rijks Vastgoed Beheer en ook het marginaal invullen van rollen binnen bijvoorbeeld Wapensysteemmanagement en Assortimentsmanagent). Dit kan dan weer aangewend worden als excuus voor achterlopen of leidt tot ‘workarounds’.
- Bij sommige onderdelen (bijvoorbeeld de Divisie Facilitair & Logistiek) zijn verantwoordelijkheden duidelijk belegd op alle niveaus en ziet management veiligheid als integrale verantwoordelijkheid. Daar staat veiligheid op de agenda van het MT, worden acties systematisch opgevolgd, loopt management veiligheidsrondes, en is er betrokkenheid van de medezeggenschapsraad. Maar ook daar is vaak de PDCA cyclus nog niet echt ‘rond’ door gebrek aan tijd en budget. Het systeem ‘staat’, maar werkt nog niet goed.
- Ook luchtmachtonderdelen zijn bezig compliance management strakker te regelen. Men heeft vastgesteld dat dit te laag in de organisatie is belegd. Men heeft dit naar het niveau van de plaatsvervangende commandant getrokken. Per gebied is een compliance officer benoemd die als procesbeheerder functioneert.
- Bij de Marine heeft men in de aanpak van de risicobeheersing, een onderscheid gemaakt tussen hoog- en laagrisico processen. Voor beheersing van de hoog-risicoprocessen is een hoger veiligheidskundige toegewezen ten einde dit proces optimaal te bedienen.
- In functieprofielen of persoonlijke doel- en taakstellingen van de lijn is bedrijfsveiligheid geen expliciet aandachtspunt of prestatiegebied.
- Structuren voor overleg en communicatie variëren per onderdeel. Op BS niveau is recent de eerder opgerichte Veiligheidsraad weer actief geworden en wordt het onderwerp bedrijfsveiligheid sinds kort aangestuurd vanuit de HDBV en besproken in het bedrijfsvoeringoverleg, waar onder meer de plaatsvervangend commandanten van de defensieonderdelen zitting in hebben.
- Communicatie rond het onderwerp veiligheid varieert sterk. Sommige onderdelen hebben een safety bulletin. Maar gestructureerde communicatiecampagnes rond dit onderwerp zijn we niet veel tegengekomen. Zie verder ook het aspect ‘opleiding’ onder ‘staf’. In de locatie van de BS is een ‘poll’ gedaan om de kennis van het ontruimingsplan te toetsen. Men ziet het ook daar als een uitdaging om het bewustzijn rond dit onderwerp op peil te houden.

*Beoordeling en conclusies*

- Het element ‘structuur’ functioneert overwegend reactief, hoewel sommige onderdelen de organisatie en verantwoordelijkheden op calculatief niveau geregeld hebben. Echter het effect hiervan is vaak nog niet zichtbaar omdat de PDCA cyclus wel ‘geregeld’ is, maar nog niet functioneert of effect oplevert (zie de beoordeling in relatie tot het systeem).
- Formeel is men zich ervan bewust dat dit hoort bij de verantwoordelijkheden van de lijn (de lijn ‘is ervan’), maar dit wordt deels ondermijnd door de centralisering van diensten, de daarmee samenhangende afhankelijkheid van derden en door een gebrek aan (competente) ondersteuning en opleiding. Dit kan ertoe leiden dat de lijn een gebrek aan bevoegdheden ervaart.

*Aanbevelingen*

- Invoering van de aanbevelingen onder het vorige hoofdstuk ‘systeem’ zullen ook leiden tot verbetering in de structuur van de organisatie.
- Versterk, bij de implementatie van het VMS DEF de taken en verantwoordelijkheden van het management. Maak duidelijk onderscheid tussen de adviestaken van de staf en de uitvoerende taken van het management.

*Bevindingen in de relatie tot Staf*

Dit onderdeel beschrijft het aspect veiligheid in het rekruterings- en selectiebeleid en het personeelsbeleid.

Belangrijk kenmerk van het personeelsbeleid bij Defensie is het rouleren van militair personeel. Dit heeft te maken met de vereiste opbouw van kennis en ervaring en de cyclus van bevordering in rangen. Voordeel is dat iedereen ‘onderaan’ begint en daardoor de praktijk en de routines van de organisatie in het DNA heeft. Nadeel kan zijn dat opgebouwde kennis en ervaring, specifiek voor het betreffende organisatiedeel, wegvloeit en steeds opnieuw moet worden opgebouwd. Uit de interviews kwam naar voren dat dit voor het aspect veiligheid nadelige gevolgen kan hebben. Men ondervangt dit op een aantal plekken door medewerkers een tweede termijn te geven of door burgerpersoneel in te zetten. Wel signaleren we weinig 'kruisbestuiving', onderdelen integreren voornamelijk alleen op het niveau van de Bestuursstaf. Er is weinig of geen ‘georganiseerde’ uitwisseling of roulatie tussen de onderdelen op lagere niveaus. Wanneer dit wel zou gebeuren zou dit de kennisuitwisseling kunnen bevorderen. Bij enkele onderdelen werken medewerkers uit verschillende onderdelen (zoals luchtmacht en landmacht bij DGLC), hier lijkt dit een positief effect te hebben

- Tenslotte is ook het afvloeien van binnen Defensie opgeleide specialisten onvermijdelijk, maar soms wel lastig voor de organisatie gezien het gewenste behoud van kennis en ervaring.

*Beoordeling en conclusie*

- Het element ‘staf’, in de zin van het vasthouden van kennis en ervaring beweegt zicht overwegend op een reactief-calculatief niveau.
- De uitspraak “bedrijfsveiligheid behoeft “continuïteit” is meermaals gevallen. Het borgen van risico’s vraagt een opbouw van kennis en inzicht in de historie van maatregelen, bij specialisten maar ook bij leidinggevenden. Het tekort aan capaciteit en het rouleren van militair personeel lijkt de effectiviteit van het veiligheidsbeleid bij sommige onderdelen tegen te werken en dringt de organisatie in een reactieve positie.

*Aanbeveling*

- Zorg voor voldoende capaciteit van specialisten op het gebied van bedrijfsveiligheid. Het verdient daarnaast aanbeveling vooraf te onderzoeken wat de minimale capaciteit dient te zijn om het gewenste niveau van bedrijfsveiligheid te kunnen bereiken.
- Benut de positieve kanten van het rouleringssysteem – zoals uitwisseling van ervaringen en best practice – en voor uitwisseling tussen de onderdelen ook op het niveau onder de Bestuursstaf om ‘goede gewoontes’, die in verschillende onderdelen zijn ontwikkeld, op een natuurlijke manier tot gemeengoed te maken. Overweeg, in het verlengde van het bovenstaande advies, een defensiebreed personeelsbeleid voor bedrijfsveiligheidspersoneel te ontwikkelen, waarbij een loopbaanbeleid wordt ontwikkeld dat voorziet in roulatie over de defensieonderdelen heen.

*Bevindingen in relatie tot sleutelbekwaamheden*

Ten aanzien van het element Sleutelbekwaamheden wordt beschreven: kennis, bekwaamheden en competenties met betrekking tot bedrijfsveiligheid en het leervermogen van de organisatie bij nieuwe uitdagingen.

- Meerdere geïnterviewden geven aan dat men het veiligheidsbewustzijn (herkennen van specifieke gevaren) bij zowel uitvoerenden als leidinggevenden als te laag ervaart. Er zijn wel trainingen en opleidingen aangetroffen die aandacht besteden aan bedrijfsveiligheid, maar deze trainingen maken niet altijd onderdeel uit van het reguliere opleidingsprogramma. Het is niet overal geborgd dat deze trainingen op alle functieniveaus systematisch aan bod komt, onder meer door tijd- en capaciteitsbeperkingen.
- Positieve voorbeelden zijn een 5-daags opleidingsprogramma voor het management over veiligheid en milieu, bij de Marine en veiligheid & milieu als vast onderdeel van de kaderopleiding bij KMar. Bij Matlogco dient het personeel de basis veiligheidsopleiding VCA (Veiligheids Checklist Aannemers) te volgen.
- Het motto 'train as you fight, fight as you train' geeft aan dat voor een optimaal niveau van competentie bij inzet een zo realistisch mogelijke training nodig is en men zich tijdens de inzet moet houden aan de routines die tijdens de training zijn ingeslepen. Dit kan leiden tot het dilemma dat men bij trainingen ver moet gaan in het nemen van risico's, maar dat dit niet tot onverantwoorde situaties mag leiden. Omdat dit zo'n expliciet dilemma is, lijkt de militaire organisatie bij uitstek competenties te hebben ontwikkeld om deze grens telkens weer te vinden. Bij CZSK noteerden we het volgende citaat: *Kritisch kijken zit in ons DNA, luister naar je onderbuik: praat erover, stel de actie uit als je het niet vertrouwt. In training zien we erop toe dat men dit oppikt; je kan het niet dichtregelen' het moet uit de mensen zelf komen, het is een fijn gevoel als ze heel kritisch zijn.*

*Beoordeling en conclusie*

- Het element 'sleutelbekwaamheden' beweegt zicht overwegend op een reactief niveau, met uitzondering van de aandacht voor veiligheid bij operationele trainingen.
- Door het ontbreken van een structureel opleidings- en communicatieprogramma rond bedrijfsveiligheid lijkt het kennisniveau en daarmee het veiligheidsbewustzijn op dit thema met name in de lijn nog laag. Dit kan het op de juiste waarde inschatten van risico's beïnvloeden.
- De communicatie tussen lijn en (expert-) staf verloopt vaak stroef. Men spreekt elkaars taal niet, wat kan leiden tot misverstanden en niet optimaal functioneren van veiligheidsmanagement en het verbeterproces. Managers missen een 'helikopterview' bij de staf, staf heeft soms het gevoel tegen dovemansoren te praten.

*Aanbevelingen*

- Verbeter de interactie tussen lijn en staf. Dit kan worden opgelost door meer aandacht voor veiligheidsmanagement in de opleiding van de lijn (zie onderstaande) en door het denken op systeemniveau bij de staf te versterken. Zie ook punt 2.4 van de Nota 'Inrichting en onderhouden van het Bedrijfsveiligheidshuis Defensie'.
- Borg kennis over bedrijfsveiligheid in de kaderopleidingen (voor het lijnmanagement). Denk hierbij aan kennisoverdracht over de werking van het managementsystemen en integraal risicomanagement, maar ook over voorbeeld -rol van de lijn, de invloed van ongeschreven regels op het functioneren van managementsystemen, effectieve leiderschapsstijlen en het beoogde ambitie niveau. Zie punt 1.9 van de nota actieplan Inrichten en onderhouden van het bedrijfsveiligheidshuis Defensie.

## 2.3 Vragen met betrekking tot het bedrijfsveiligheidbewustzijn

Het bedrijfsveiligheidsbewustzijn kenschetsen we aan de hand van de elementen ‘stijl’ en ‘shared values’ ofwel de gemeenschappelijke waarden van de organisatie.

Het element ‘stijl’ betreft kwaliteit van leiderschap en betrokkenheid in termen van voorbeeldgedrag, daadkracht, sturen op gewenste safety performance en doelen, toezicht en handhaving van veiligheidsvoorschriften.
Het element ‘gemeenschappelijke waarden’ vertegenwoordigt de bedrijfscultuur, de waarden en normen die binnen een organisatie heersen en die in grote mate bepalend zijn voor de kwaliteit van de andere aspecten.

### 2.3.1 Onderzoeksvraag 2 a: Wat is het huidige niveau van bedrijfsveiligheidbewustzijn bij Defensie?:

*Bevindingen*
*Ten aanzien van het element stijl zien we het volgende:*

- De organisatie wordt in principe gekenmerkt door een sterke hiërarchie, waarbij het motto ‘opdracht is opdracht centraal staat. Tegelijkertijd lijkt management zich bewust van de noodzaak een ‘open cultuur’, waarin vragen en zorgen geuit kunnen worden. Dit lijkt – een aantal goede voorbeelden daargelaten – in de praktijk echter niet voor alle aspecten van bedrijfsveiligheid te zijn gerealiseerd
- Daarnaast is ‘niet werken met de lange schroevendraaier’ een motto dat een nieuwe stijl van leidinggeven binnen de Bestuursstaf en hogere leiding moet ondersteunen. Hiermee geeft men aan wel het ‘wat’, maar niet het ‘hoe’ te willen bepalen. Waar men in het verleden gewend was zich met details bezig te houden, gaat de nieuwe visie en opzet van de organisatie uit van management op afstand in plaats van micromanagement. Dit geeft de ‘werkvloer’ meer invloed maar ook meer verantwoordelijkheid, ook ten aanzien van bedrijfsveiligheid.

*Ten aanzien van de gemeenschappelijke waarden zien we het volgende:*

- De hiervoor behandelde elementen zijn in grote mate bepalend voor het niveau van beheersing van veiligheidsrisico’s in de organisatie. Maar op de achtergrond drukken ook de ‘ongeschreven regels’, de cultuur en gewoonten van de organisatie en haar leden een belangrijke stempel op het uiteindelijke resultaat van deze inspanning. Een aantal van deze ongeschreven regels kwam in de interviews meermalen aan de orde. Onderstaand geven we de meest in het oog springende ongeschreven regels en de wijze waarop ze de zorg voor veiligheid kunnen beïnvloeden.
- ‘Can do/ fix it’ staat voor de regel dat men tot het uiterste wil gaan om een gegeven opdracht uit te voeren. Dit mes snijdt aan twee kanten. Enerzijds staat het voor vindingrijkheid om onder gegeven moeilijke omstandigheden toch op een verantwoorde wijze het doel te bereiken. Anderzijds kan dit ook leiden tot improvisatie en daarmee afwijken van richtlijnen (meer risico nemen). Van beide uitwerkingen zijn voorbeelden de revue gepasseerd.
- ‘We willen niet graag teleurstellen uit een groot gevoel van verantwoordelijkheid’, is een ongeschreven regel die in het verlengde hiervan ligt. Enerzijds helpt dit om de doelen te bereiken, anderzijds kan dit in de hand werken dat medewerkers (te) makkelijk “ja” zeggen terwijl zij weten

dat er bijvoorbeeld te weinig capaciteit is om de opdracht succesvol of op een verantwoorde manier af te ronden.

- Meerdere geïnterviewden geven aan dat men het veiligheidsbewustzijn (herkennen van specifieke gevaren) bij zowel uitvoerenden als leidinggevenden als te laag ervaart, zie ook hoofdstuk 2.2:bevindingen in relatie tot sleutelbekwaamheden.
- 'Esprit de corps' staat voor de noodzaak om een sterk teamgevoel te hebben bij de uitvoering van bijzondere taken. Dit kan haaks staan op de procesgerichte inrichting van de organisatie: niet alle processen draaien meer om het 'team' of het eindproduct, het team staat niet meer centraal, maar riskeert een radertje in een kluwen van processen te worden.
- "Het hoeft niet altijd beter, het moet ook werkbaar blijven' geeft de vrees weer voor het star vasthouden aan arbo-regels. Met name degenen die dicht bij training en inzet zitten gaven ons tal van voorbeelden om aan te tonen dat het niet altijd mogelijk is om aan regels te voldoen die in de burgermaatschappij normaal zijn. Als mensenlevens op het spel staan ontkomt men er niet aan keuzes te moeten maken. Afwijken van regels gebeurt volgens de meeste geïnterviewden wel op basis van zeer strikte risicobeoordeling

*Beoordeling en conclusie*

- Uit onze bevindingen ten aanzien van de andere elementen en de beoordeling daarvan aan de hand van het 'Hearts and Minds' model, wordt zichtbaar dat de bedrijfscultuur rond het aspect veiligheid in beweging is, maar zich vooralsnog overwegend op een reactief niveau bevindt.
- De grote invloed van ongeschreven regels is dat ze vaak niet openlijk ter discussie staan of worden besproken. Toch kunnen ze het bereiken van de doelstellingen in het kader van bedrijfsveiligheid sterk beïnvloeden, zowel in positieve als negatieve zin. Het effect van de stijl van leidinggeven en de ongeschreven regels op bedrijfsveiligheid en het nemen van risico's wordt nog te weinig expliciet besproken. Met name de – soms grote - verschillen tussen de manier waarop onderdelen omgaan met het aspect bedrijfsveiligheid en tussen de aandacht voor veiligheid bij training en inzet enerzijds en bij andere activiteiten anderzijds, maken duidelijk dat een expliciete dialoog met betrekking tot de gedeelde waarden rond dit aspect ontbreekt. Dit bemoeilijkt het formuleren van een consequente en samenhangende ambitie en strategie op dit terrein en leidt ertoe dat de ongeschreven regels onvoorziene effecten hebben op het veiligheidsbewustzijn en de praktijk. Pas wanneer ongeschreven regels in de pas lopen met geschreven regels, is er sprake van een effectieve veiligheidscultuur.

### 2.3.2 Onderzoeksvraag 2 b: Is dit niveau voldoende voor een verantwoorde bedrijfsvoering?
### Onderzoeksvraag 2 c en 2 d: Wat zou het niveau moeten zijn en welke aanbevelingen zijn er, indien van toepassing.

- Zoals blijkt uit onze eerdere conclusies is dit 'reactieve' niveau onvoldoende om tot een blijvend verantwoord niveau van veiligheidszorg in de bedrijfsvoering te komen. Afhankelijk van de aard en de omvang van de risico's zal de organisatie zeker op een calculatief of bij voorkeur proactief niveau moeten gaan acteren.

*Aanbevelingen*

- Naast de aanbevelingen in het voorgaande achten we het noodzakelijk het bewustzijn ten aanzien van bedrijfsveiligheid te bevorderen op alle lagen van de organisatie door de stijl van leidinggeven en de heersende 'ongeschreven' regels te plaatsen in het perspectief van een veilige operatie. Identificeer en bespreek de stijl van leidinggeven en de 'ongeschreven regels' op alle niveaus in de organisatie en ga de dialoog aan over wat ze betekenen in het licht van veiligheid, bijvoorbeeld aan de hand van workshops met een tool als 'Understanding your culture' uit het programma 'Winning Hearts and Minds'. Zie ook punt 1.1 van de nota Inrichten en onderhouden van het Bedrijfsveiligheidshuis Defensie.
- Borg kennis over bedrijfsveiligheid in de kaderopleidingen. Denk hierbij aan kennisoverdracht over de werking van het managementsystemen en integraal risicomanagement, maar ook over voorbeeld- rol van de lijn, de invloed van ongeschreven regels op het functioneren van managementsystemen, effectieve leiderschapsstijlen en het beoogde ambitie niveau. Zie ook hoofdstuk 2.2:bevindingen in relatie tot sleutelbekwaamheden.

## 2.4 Onderzoeksvragen met betrekking tot ten aanzien van de meest recente verbeterplannen

### 2.4.1 Vraag 3 a: Zullen de voorliggende verbeterplannen op het gebied van bedrijfsveiligheid van Defensie leiden tot de realisatie van de gewenste doelen?

- De Nota 'Inrichting en onderhouden van het Bedrijfsveiligheidshuis Defensie' bevat een vrij complete set aan concrete afspraken, maar we missen vooral een expliciete vaststelling van het ambitieniveau.

### 2.4.2 Vraag 3 b: Indien niet het geval, welke verbetersuggesties zijn er op basis van o.a. de bevindingen over vragen 1 en 2 om de gewenste doelen wel te bereiken?

- Bij de beantwoording van vragen 1 en 2 hebben we in hoofdstuk 2 een elftaltal verbetersuggesties aangegeven.

  In onderstaande tabel geven we – op basis van ervaringen met verandertrajecten in vergelijkbare complexe organisaties - een globale indicatie met betrekking tot de volgorde en de doorlooptijd van elk van deze aanbevelingen. Voor alle aanbevelingen geldt dat een gefaseerde aanpak nodig is: eerste opzet – proefdraaien – evaluatie – fine tuning en brede implementatie. Ook kan deze planning voor bepaalde aanbevelingen per onderdeel wisselen, aan aantal zijn in vele opzicht als verder dan andere.

Tenslotte geldt voor vrijwel elke aanbeveling dat na verloop van tijd een ‘revisie’ nodig is, dat is in deze tabel niet meegenomen.

| | *Aanbeveling* | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|
| | *Beleid / doel en taakstellingen* | | | | |
| 1 | Ambities en doelen | | | | |
| 2 | Acties en voortgang | | | | |
| 3 | KPI Dashboard | | | | |
| | *VMS DEF (Implementatie en Monitoring)* | | | | |
| 4 | VMS DEF op orde | | | | |
| 5 | Versterken Toezicht en beoordeling | | | | |
| 6 | Certificering geschikte norm | | | | |
| | *Veiligheidsbewustwording* | | | | |
| 7 | Interactie lijn / staf verbeteren | | | | |
| 8 | Veiligheid in opleidingen | | | | |
| 9 | Dialoog ongeschreven regels | | | | |
| | *Toereikendheid bedrijfsvoeringorganisatie* | | | | |
| 10 | Zorg voor voldoende capaciteit veiligheidsstaf | | | | |
| 11 | Uitwisseling / roulering | | | | |

# Bijlage 1

# Geraadpleegde documenten

Royal HaskoningDHV

- Nota SG Doel en taakstellingen 2011; 11 maart 2010
- Nota SG Doel en taakstellingen 2009
- Bijlage G - Opdrachten Veiligheidsmanagementsysteem; 19 december 2008
- Werking veiligheidsmanagementsysteem bij de BACK-spelers binnen de BS; 21 januari 2015
- Auditrapport Werking VMS Def; 21 januari 2015
- Rapport quick scan Safety; 28 oktober 2013
- Veiligheidsmanagement bij Defensie
- Bevindingen Toezicht  CZSK ILT 31 maart 2015
- Audit rapportage Lloyd's; 27 januari 2015
- Een blauwdruk voor belegging en verankering; 18 mei 2010
- Nota: Inrichten en onderhouden van het Bedrijfsveiligheidshuis Defensie
- Blauwdruk Bestuur Defensie BACK-bone voor de toekomst Datum 1 augustus 2011
- Besluitenlijst en actiepunten Ketenoverleg Veiligheid, Gezondheid en Milieu; 15 oktober 2014
- Nota: Aanschrijving Management Control; 2011
- Externe DMO rapportage Veiligheidsmanagement; 2014 Q1.doc
- Inspectie rapport ILT marinekazerne Willemsoord; 10 april 2014
- Monitoring & Toezicht Jaarplan HDBV; 3 maart 2015
- Aanwijzing HDBV Monitoring en Toezicht; 1 januari 2015
- Besturen bij Defensie (BBD2013;
- Visie op veiligheidsmanagement (definitief); 29 oktober 2009
- Instellingsbeschikking Veiligheidsraad; 13 mei 2009
- Veiligheidsbeleidsverklaring; december 2008
- Nota CDS uitgangspunten en visie; 10 november 2009
- CLAS Managementrapportage veiligheidsmanagement; 1ste kwartaal 2014
- Notie: MR Q1 2014 BS
- Professionaliseren van het veiligheidsmanagement systeem; 20 oktober 2010
- Betreft Verkennende inspectie Hyperbare Geneeskunde; 2 juli 2014 Inspectie SZW
- Betreft Beschikking inzake boete; 16-10-2014 Inspectie SZW
- Brief inzake arbeidongeval. Betreft Arbeidsongeval d.d. 4 november 20142014 Inspectie SZW
- Brief inzake overtreding  Betreft Eis Arbo Inspectie SZW; 7 januari 2015
- Appreciatie MR Q1 2014
- CLAS Managementrapportage veiligheidsmanagement 1ste kwartaal 2014
- Controle brandveiligheid gebouwen: gebruiksaspecten ILT; maart 2014
- CDC rapportage veiligheidsmanagement; 3 april 2014
- Nota: Veiligheid & milieu rapportage KMar  2013
- VMS Def

# Bijlage 2

# Geïnterviewde personen

| Eenheid | Functie | Rang / Titel | Naam |
|---|---|---|---|
| BS/DBOBS | Directeur Bedrijfsondersteuning BS | | |
| BS/DBOBS | Adviseur Dienstverlening DBOBS | | |
| CDC/OG&K | Directeur Bedrijfsvoering | | |
| CDC/DGO/TGB/CMH | Commandant CMH | | |
| CDC/F&L | Commandant DF&L | | |
| CDC/DGO/TGB/CMH/ZOG | Medewerker Kwaliteit Arbo Veiligheid | | |
| CLAS | PLV Commandant CLAS | Genm. | M.J.H.M. van Uhm |
| CLAS/DGLC | Commandant DGLC | | |
| CLAS/11LMB | C-LUCHTMOBIELE BRIGADE | | |
| CLAS/13LTBRIG/STSTCIE/BRIGST/SIEG1 | HOOFD SECTIE G1 | | |
| CLAS/Matlogco | HOOFD BUREAU KAMB | | |
| CLSK/P-CLSK | Plv Commandant Luchtstrijdkrachten | Genm ir. | E.C.G.J. van Duren |
| CLSK/PLV C-LSK/DP&BV | Directeur Pers. & Bedrijfsvoering | | |
| CLSK/EHV | Commandant Lutra | | |
| CLSK/DHC | C-DHC | | |
| CLSK/VKL/SP&BV/BVLGHD&INT | Hoofd Sie BV & Integrale toetsing | | |
| CLSK/LW/P&BV/BEDR&KWAL | Hoofd Bedrijfsveiligheid & Kwaliteit | | |
| CLSK/LCW/AIBV/SIEIB | Hoofd Sie Integr Bdrfsveiligheid | | |
| CZSK/PCZSK | Plv Commandant Zeestrijdkrachten | SBN | B.W.J. Bekkering |
| CZSK/OPS/NLMF/STC | Commandant STC | | |
| CZSK/MI/MT | Hoofd Afd Maritieme Technieken | | |
| CZSK/OPS/NLMF/STC/SBV | H-V&M | | |
| CZSK/MI/PROG/IV&K | Hfd Bur Int Veiligheid&Kwal | | |
| KMAR/STAF/COGP | PCKMAR | Genm Mr. EMPM | H. van den Brink |
| KMAR/STAF/DPB | DIR DPB | | |
| KMAR/LTC | Commandant LTC | | |
| KMAR/OTCKMAR | Commandant OTCKMAR | | |
| KMAR/DLBE/ST/SIEMATLOG | Hoofd SIE MAT/LOG | I | |
| KMAR/ZUID/ST/SIEMATLOG | Hoofd SIE MATLOG | | |
| DMO | DIRECTEUR | Genm Ir. MA | P.H.T.J.M. Dohmen |
| DMO/MATLOG/WPSN | SC WPSN | | |
| DMO/MATLOG/DMUNB | C-DMUNB | | |
| DMO/JIVC/ST | HFD ST | | |
| DMO/MATLOG/DMUNB/VHMGMT | HFD SIE VHMGMT | | |

| Eenheid | Functie | Rang / Titel | Naam |
|---|---|---|---|
| CDC/F&L/VAM | Voorzitter CMC | | |
| CZSK/MI/MAROST/SBVM | Lid CMC / Wg VKAM | | |
| BS/AL/HDP/Prj PlvHDP | Projectfunctionaris PHDP | . | |
| BS/AL/DS/DAOG | Directeur DAOG | Genm | J.D. Luyt |
| BS/AL/DS/DAOG/AOndOpGerh | Senior Stafofficier Veiligheid | | |
| BS/AL/HDBV | Hoofddirecteur Bedrijfsvoering | SBN (TD) Dr. Ir. | A.J. de Waard |
| BS/AL/DS/DOPS | Directeur DOPS | Genm. | M.A. van der Laan |
| BS/AL/DS/DOPS | Plv. Directeur DOPS | | |
| BS/AL/DS/Dir. Plan. | Directeur Plannen | SBN | R.P. Bauer |
| BS/AL/BSG | plv.Secretaris-Generaal | Mr. | M. Gazenbeek |

With its headquarters in Amersfoort, The Netherlands, Royal HaskoningDHV is an independent, international project management, engineering and consultancy service provider. Ranking globally in the top 10 of independently owned, nonlisted companies and top 40 overall, the Company's 6,500 staff provide services across the world from more than 100 offices in over 35 countries.

## Our connections

Innovation is a collaborative process, which is why Royal HaskoningDHV works in association with clients, project partners, universities, government agencies, NGOs and many other organisations to develop and introduce new ways of living and working to enhance society together, now and in the future.

## Memberships

Royal HaskoningDHV is a member of the recognised engineering and environmental bodies in those countries where it has a permanent office base.

All Royal HaskoningDHV consultants, architects and engineers are members of their individual branch organisations in their various countries.

**royalhaskoningdhv.com**

Royal HaskoningDHV
*Enhancing Society Together*