Risicomanagement en de Nederlandse defensie-industrie.

DE ABDO IN RELATIE TOT HET TOEPASSEN VAN RISICOMANAGEMENT.

S. Boonstoppel
Universiteit Twente | Masterthesis | Versie 1.0 | 11-2022

Bibliografie.

Informatiepagina

Gegevens onderzoek.

Titel:	Risicomanagement en de Nederlandse defensie-industrie.
Ondertitel:	De ABDO in relatie tot het toepassen van risicomanagement.

Gegevens student.

Student:	S. Boonstoppel.

Gegevens opdrachtgevers.

Naam organisatie:	Ministerie van Defensie.
Postadres:	Van Alkemadelaan 786.
Bezoekadres:	Van Alkemadelaan 786.
Postcode:	2597 BC.
Plaats:	Den Haag.

Naam organisatie:	Universiteit Twente.
Faculteit:	Behavioural Management and Social sciences.
Opleiding:	Master Risicomanagement.
Postadres:	Universiteit Twente.
Postbus:	217.
Plaats:	Enschede.
Bezoekadres:	Drienerlolaan 5.
Postcode:	7522 NB.
Plaats:	Enschede.
Telefoonnummer:	+31(0)534899111.

Gegevens begeleiders.

1e begeleider.

Titel, voor- en achternaam:	Dr. ir. M.Th. van Staveren MBA.
E-mail:	Info@vsrm.nl.

2e begeleider.

Titel, voor- en achternaam:	Dr. M. Rajabali Nejad.
E-mail:	M.rajabalinejad@utwente.nl.

Afkortingenlijst

ABDO	Algemene Beveiligingseisen voor Defensieopdrachten.
BI	Bijzondere Informatie.
BIV	Bureau Industrieveiligheid.
BO	Bijzondere Opdracht.
COSO	The Committee of Sponsoring Organizations of the Treadway Commission.
COTS	Commercial-off-the-shelf.
ERM	Enterprise Risk Management.
IRM	Institute of Risk Management.
IIA	Institute of Internal Auditors.
ISO	International Organization for Standardization.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst.
MOBEC	Meldingen & stuurinformatie, Organisatorisch, Bouwkundig, Elektronisch en Communicatie & bewustwording.
OBE	Organisatorisch, Bouwkundig en Elektronisch.
OBER	Organisatorische-, Bouwkundige, Elektronische en Reactieve- maatregelen.
Stg	Staatsgeheim.
TBB	Te Beschermen Belang.
Wiv	Wet op de inlichtingen- en veiligheidsdiensten.

Voorwoord

Voor u ligt de thesis ‘’Risicomanagement en de Nederlandse defensie-industrie’’. Het onderzoek voor deze thesis is uitgevoerd bij defensieorderbedrijven die een bijzondere opdracht uitvoeren voor de Nederlandse krijgsmacht. Deze scriptie is geschreven in het kader van mijn afstuderen aan de opleiding Master Risicomanagement aan de Universiteit Twente en in opdracht van Bureau Industrieveiligheid ,wat ressorteert onder het Ministerie van Defensie.

Het schrijven van deze thesis heeft bijgedragen aan mijn persoonlijke ontwikkeling en ik ben tevreden met het eindresultaat. Door het toepassen van kwalitatief onderzoek, heb ik een goed beeld verkregen wat voor effect de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) heeft op het toepassen van risicomanagement bij defensieorderbedrijven.

Afsluitend wil ik iedereen bedanken voor de fijne samenwerking en het gegeven vertrouwen. In het bijzonder mijn begeleiders en tevens lezers, Dr. ir. M.Th. van Staveren, Dr. M. Rajabali Nejad en alle beveiligingsfunctionarissen die bijgedragen hebben aan dit onderzoek.

Ik wens u veel leesplezier toe.

S. Boonstoppel.

Apeldoorn, november 2022.

Samenvatting

Iedere dag laat de dagelijkse praktijk medewerkers van Bureau Industrieveiligheid zien, dat defensieorderbedrijven, die een bijzondere opdracht uitvoeren voor het ministerie van Defensie, onderhevig zijn aan risico's van binnen- en buitenaf. Om de kroonjuwelen (Te Beschermen Belang) die bij het bedrijf belegd zijn te beschermen, wordt de Algemene Beveiligingseisen voor Defensie (ABDO) contractueel bedongen en gehanteerd. Wanneer volledig en adequaat geïmplementeerd, biedt de ABDO de gewenste bescherming voor de daderprofielen die het ministerie van Defensie kent. Echter kunnen daderprofielen wisselen door tijd, actualiteit en nieuwe politieke- en technologische innovatie. Laatstgenoemde factoren kunnen dan ook invloed hebben op een modus operandi van een daderprofiel, wat betekent dat er mogelijk ongewenste, niet bekende risico's kunnen ontstaan. Gezien laatstgenoemde niet wenselijk is, wil Bureau Industrieveiligheid dat ieder bedrijf dat in de defensie-industrie actief is, risicomanagement hanteert. Het doel van dit onderzoek is om inzicht te krijgen wat voor effect de ABDO heeft op het toepassen van risicomanagement. Hiervoor is de volgende onderzoeksvraag opgesteld: Wat voor effect heeft de ABDO op het toepassen van risicomanagement bij defensieorderbedrijven, waarbij een bijzondere opdracht belegd is? Daarnaast zijn er enkele aanbevelingen gemaakt die in beschouwing genomen kunnen worden ten aanzien van de ontwikkeling van de nieuwe versie van de ABDO.

Om antwoord te kunnen geven op de geformuleerde onderzoeksvraag is er een kwalitatief onderzoek uitgevoerd, gebruikmakende van verschillende soorten literatuur en interviews met beveiligingsfunctionarissen. Uit het literatuuronderzoek is gebleken dat er bij defensieorderbedrijven een verschuiving plaatsvindt, van conventioneel- naar vernieuwend management. Conventioneel management is hoofzakelijk strategisch van aard en vertaald zich niet terug naar de werkvloer, waar er gewerkt wordt aan de kroonjuwelen. Vernieuwend management typeert zich door juist wel iedereen te betrekken en is daarmee enkel niet alleen strategisch aanwezig, maar op ieder zijn eigen niveau. Dit laatste heeft er naar geleid dat voor dit onderzoek verder gebruik gemaakt is van een vernieuwende risicomanagementmethode, namelijk risico gestuurd werken. Door de ABDO te vergelijken met alle bestudeerde literatuur, betreffende dit onderzoek is er inzichtelijk gemaakt dat de ABDO elementen bezit van integrale beveiliging en dat van risicomanagement. Het is gebleken dat dat ABDO voornamelijk operationaliserend van aard is en voldoet aan alle elementen waarmee risicomanagement wordt gedefinieerd. Als laatste zijn beveiligingsfunctionarissen gesproken om zodoende de theoretische resultaten te kunnen vergelijken met de dagelijkse realiteit. De beveiligingsfunctionarissen zijn gekozen middels een selecte steekproef, met inachtneming van de populatie van defensieorderbedrijven die bijzondere opdrachten uitvoeren. Uit de antwoorden is gebleken dat de ABDO een beperkt effect heeft op het toepassen van risicomanagement in de dagelijkse praktijk. Defensieorderbedrijven hanteren de ABDO omdat het contractueel bedongen is en ze rechtswege compliant moeten zijn. Ieder defensieorderbedrijf doet dit op zijn eigen manier en gebruikt zijn eigen risicomanagementmethode. Uit de gesprekken is ook gebleken dat er de wens bestaat, om de ABDO meer te laten aansluiten bij bestaande standaarden- en normkaders.

Op basis van de genoemde bevindingen wordt er dan ook aanbevolen om in de nieuwe versie van de ABDO, de generieke risicoprocesstappen van risico gestuurd werken op te nemen. Dit creëert een eenduidige manier van werken en is er geen ruimte voor eigen interpretatie. Daarnaast is het advies om inzichtelijk te maken hoe de ABDO overeenkomt met andere standaarden- en normkaders, om zodoende de focus te kunnen leggen naar de nog te implementeren, resterende normen. Eventueel vervolgonderzoek zal zich kunnen richten op welke standaarden- en normkaders overeenkomen met de ABDO en wat defensieorderbedrijven beweegt om toch risicomanagement toe te passen zonder contractueel of rechtswege compliant te moeten zijn.

1. Inleiding

Om een rol van betekenis te spelen in de samenwerking met andere landen en een waardevolle bijdrage te leveren aan de veiligheid in Europa heeft Nederland een sterke, stabiele basis nodig. Na jaren van (politieke-) bezuinigingen is er eindelijk weer perspectief op een grotere en sterkere Nederlandse krijgsmacht. Niet alleen omdat de krijgsmacht dit nodig heeft, maar omdat de situatie in de wereld dat van Nederland en Europa vraagt. Om dit te kunnen bewerkstelligen is er een innovatieve, sterke en veilige defensie-industrie nodig, dat in bezit is van kennis, technologie en capaciteit (Ministerie van Defensie, 2021b). Helaas blijkt iedere dag dat buitenstaanders interesse hebben in kennis, materieel, goederen en objecten van het Ministerie van Defensie, kennisinstituten en de Nederlandse defensie-industrie. Onoorbare praktijken en heimelijke middelen worden niet geschuwd om te trachten hierop de hand te leggen. Het is dus begrijpelijk en van essentieel belang om genoemde zaken adequaat te beschermen.

1.1 Beschermen van onze kroonjuwelen

Het Ministerie van Defensie belegd zijn opdrachten bij diverse bedrijven die actief zijn in de zogenaamde defensie-industrie. Het Ministerie van Defensie kiest hiervoor, omdat het zelf niet meer de kennis, technologie en de gewenste capaciteit bezit om zelf te voorzien in deze opdrachten. Te denken valt aan het ontwikkelen van wapensystemen, tot het bouwen van nieuwe onderzeeërs en fregatten voor de Koninklijke Marine. Om een dergelijke opdracht te kunnen uitvoeren krijgen de bedrijven, ook wel defensieorderbedrijven soms gerubriceerde informatie overhandigd of toegang tot een Te Beschermen Belang. Een voorbeeld van een Te Beschermen Belang is bijvoorbeeld een kazerne of een (niet-)operationeel schip van de Koninklijke Marine. Veelal wordt er dan ook gesproken over ‘onze kroonjuwelen’.

Volgens het MIVD Jaarverslag (Ministerie van Defensie, 2021a) blijkt dat buitenlandse actoren regelmatig grote interesse hebben in onze kroonjuwelen. Deze actoren proberen middels diefstal, spionage en andere ongewenste methoden toegang te krijgen of informatie toe te eigenen. Om te voorkomen dat dit gebeurt en om de weerbaarheid van de Nederlandse defensie-industrie te vergroten heeft de wetgever op basis van de wet Inlichtingen en Veiligheidsdiensten 2017 (*wetten.nl - Regeling - Wet op de inlichtingen- en veiligheidsdiensten 2017 - BWBR0039896*, 2022) de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) enkele taken toebedeeld. Eén van die taken is om maatregelen te nemen om de veiligheid en paraatheid van de krijgsmacht te beschermen, waaronder de beveiliging van (bijzondere) informatie (de zogenoemde D-taak). Dit betekent voor de MIVD dat ze maatregelen dienen te treffen om bijzondere informatie, ofwel onze kroonjuwelen, te beschermen. Om aan de genoemde taakstelling te kunnen voldoen heeft de MIVD, Bureau Industrieveiligheid (BIV) opgericht. Bureau Industrieveiligheid stelt zich ten doel om bij te dragen aan de bescherming van defensiebelangen, tegen interne en externe dreigingen op korte en langere termijn, door het tijdig onderkennen en identificeren van dreigingen jegens de defensie-industrie en het op basis hiervan (laten) treffen van maatregelen ter bescherming van de te behartigen belangen. Ofwel betekent dit in de dagelijkse praktijk dat Bureau Industrieveiligheid, bedrijven adviseert en controleert over de wijze hoe ze bijzondere (gerubriceerde) informatie dienen te verwerken, te beschermen en op te slaan.

1.2 Aanleiding

Zoals eerder benoemd heeft de Militaire Inlichtingen- en Veiligheidsdienst en hiermee Bureau Industrieveiligheid de taak toebedeeld gekregen, om maatregelen te nemen om de veiligheid en paraatheid van de krijgsmacht te beschermen, waaronder de beveiliging van bijzondere (gerubriceerde) informatie (Wiv, art 10 lid 2) (*wetten.nl - Regeling - Wet op de inlichtingen- en veiligheidsdiensten 2017 - BWBR0039896*, 2022).

Het is namelijk zo dat men onder alle omstandigheden moet kunnen rekenen op de betrouwbaarheid (beschikbaarheid, integriteit, vertrouwelijkheid) van personeel, informatie, materieel, goederen en objecten. Deze staan echter voortdurend bloot aan dreigingen zoals criminaliteit, extremisme, sabotage, terrorisme en spionage. Economische, strategische militaire en technisch wetenschappelijke spionage vormen een actuele dreiging. Vitale sectoren zoals energie en telecommunicatie, kunnen getroffen worden door (digitale) extremistische of terroristische aanslagen. Het nemen van beveiligingsmaatregelen met een bepaalde mate van gelaagdheid dragen bij aan de weerstand tegen genoemde dreigingen. Gezien de complexheid van deze taak is hiervoor door Bureau Industrieveiligheid, de Algemene Beveiligingseisen voor Defensieopdrachten ontworpen. De eerste professionele versie van de ABDO vindt zijn oorsprong in 2006. Gezien technologische innovaties en daarmee een verandert dreigingsbeeld werd er in 2017 een vernieuwde versie van de ABDO gepresenteerd. In versie 2017 werd voornamelijk hoofdstuk vier, het cyber hoofdstuk enorm uitgebreid met nieuwe beveiligingsnormen. De meest recente versie van de ABDO dateert uit het jaar 2019. De ABDO 2019 wordt dan ook nog dagelijks gebruikt en toegepast door Bureau Industrieveiligheid en de Nederlandse defensie-industrie. De ABDO stelt Bureau Industrieveiligheid in staat om defensieorderbedrijven passende beveiligingsmaatregelen te laten nemen, dit in relatie tot de specifieke (bijzondere) opdracht (BO).

Voordat een defensieorderbedrijf een bijzondere opdracht wil gaan uitvoeren moet het dus contractueel voldoen aan de bijpassende normen die de ABDO stelt. Bureau Industrieveiligheid begeleidt het defensieorderbedrijf in dit proces en wanneer deze voldoet, zal het voor de opdracht in kwestie geautoriseerd worden. Een autorisatie van Bureau Industrieveiligheid is dan ook benodigd om een bijzondere opdracht te kunnen uitvoeren.

1.3 Probleemstelling

De dagelijkse praktijk laat medewerkers van Bureau Industrieveiligheid zien dat de beveiligingsnormen van de ABDO duidelijk en goed te implementeren zijn. Met behulp van Bureau Industrieveiligheid zijn defensieorderbedrijven in staat om tot het gewenste beveiligingsniveau te komen en kunnen daardoor geautoriseerd worden voor de opdracht. De ABDO kent vier hoofdstukken die ieder een ander aandachtsgebied heeft. Wanneer volledig en adequaat geïmplementeerd, biedt de ABDO de gewenste bescherming voor de daderprofielen die het Ministerie van Defensie hanteert. Echter kunnen daderprofielen wisselen door tijd, actualiteit en nieuwe politieke- en technologische innovatie. Laatstgenoemde factoren kunnen dan ook invloed hebben op een modus operandi van een daderprofiel, wat betekent dat er mogelijk ongewenste, niet bekende risico's kunnen ontstaan.

De dagelijkse praktijk laat Bureau Industrieveiligheid dan ook zien dat defensieorderbedrijven onderhevig zijn aan risico's en ongewenste invloeden van binnen- en buitenaf. Om deze reden is het borgen en het bestendigen van de te hanteren ABDO-normen dan ook van vitaal belang. Gezien de mogelijke (nieuwe) risico's, ongewenste invloeden en het vitale belang om de gelaagdheid en daarmee de effectiviteit van reeds geïmplementeerde beheers- en beveiligingsmaatregelen te beschermen is Bureau Industrieveiligheid voornemend om een nieuwe versie van de ABDO te ontwikkelen.

Zoals de reeds gepubliceerde versies van de ABDO laten zien, worden ze altijd ingehaald door de dagelijkse actualiteit, innovaties en daarmee ook risico's. Om genoemde redenen wil Bureau Industrieveiligheid dan ook onderzoeken welk effect de ABDO heeft op het toepassen van risicomanagement bij defensieorderbedrijven.

1.4. Doelstelling

Het doel van de opdracht is om te inventariseren wat voor effect de ABDO heeft op het toepassen van risicomanagement bij een defensieorderbedrijf in de dagelijkse praktijk, zodat er aanbevelingen kunnen worden gemaakt om het toepassen van risicomanagement en daarmee de bescherming van onze kroonjuwelen te bevorderen. Daarnaast zal Bureau Industrieveiligheid alle aanbevelingen in beschouwing nemen ten aanzien van de ontwikkeling van de nieuwe versie van de ABDO. Om dit te kunnen doen zal er als eindproduct op basis van alle relevante onderzoeksresultaten puntsgewijs aanbevelingen gepresenteerd worden.

1.5 Onderzoeksvragen

Gezien de probleemstelling en doelstelling van dit onderzoek is de onderstaande onderzoeksvraag geformuleerd.

Onderzoeksvraag:
Wat voor effect heeft de ABDO op het toepassen van risicomanagement bij defensieorderbedrijven waarbij een bijzondere opdracht belegd is?

Tabel 1: Onderzoeksvraag.

1.5.1 Deelvragen.

Om de geformuleerde onderzoeksvraag te kunnen beantwoorden zijn de onderstaande deelvragen opgesteld. Door gebruik te maken van deelvragen wordt de probleemstelling gespecificeerd en kunnen directe vragen opgesteld worden. Onderstaande deelvragen geven inzicht welke specifieke kennis nodig is om de onderzoeksvraag te kunnen beantwoorden (Verhoeven, 2011).

Deelvraag één:
Welke risicomanagementmethode kan gebruikt worden ter ondersteuning van de ABDO?

Tabel 2: Deelvraag één.

Door het beantwoorden van deelvraag één wordt er inzicht verkregen wat risicomanagement precies is en hoe het zich positioneert in relatie tot de ABDO. Het beantwoorden van deelvraag één is dan ook het startpunt van dit onderzoek.

Deelvraag twee:
Wordt er met de ABDO risicomanagement toegepast bij een defensieorderbedrijf?

Tabel 3: Deelvraag twee.

De resultaten van deelvraag twee geven een duidelijk beeld wat risicomanagement is en hoe een risicomanagementmethode zich verhoudt tot de ABDO. Gezien de onderzoeksvraag zich richt tot de ABDO zal deze diepgaand geanalyseerd worden met behulp van de resultaten van deelvraag één.

Deelvraag drie:
Hoe passen defensieorderbedrijven risicomanagement toe in de dagelijkse praktijk?

Tabel 4: Deelvraag drie.

Met deelvraag drie zal er inzicht verkregen worden hoe het gesteld is met het toepassen van risicomanagement in de dagelijkse praktijk. De resultaten van deelvraag drie zullen naast de uitkomsten van deelvraag één en twee gepresenteerd worden om uiteindelijk antwoord te kunnen geven op de geformuleerde onderzoeksvraag.

2. Theoretisch kader

2.1 Inleiding

In het voorgaande hoofdstuk is de problematiek inzichtelijk gemaakt, is er een doelstelling opgesteld en zijn onderzoeksvragen geformuleerd. In dit hoofdstuk zullen er verdiepingen plaatsvinden die relevant zijn voor dit onderzoek. Allereerst zal er gekeken worden naar de betekenis en definities van de gebruikte termen, om zodoende onduidelijkheden te voorkomen. Termen zoals risico, risicomanagement, beveiliging en integrale beveiliging zullen uitvoerig aan bod komen. Daarnaast zal er gezien het onderwerp van dit onderzoek een verdieping plaatsvinden in de ABDO.

2.2. Theoretische verdieping ten behoeve van deelvraag één

Deze paragraaf en bijhorende sub-paragrafen zullen zich richten op een verdieping van literatuur, wat uiteindelijk gebruikt zal worden voor de beantwoording van deelvraag één. De sub-paragrafen zullen zich dan ook richten op welke risicomanagementmethode gebruikt kan worden ter ondersteuning van de ABDO.

2.2.1 Risico

In het dagelijkse leven komt eenieder wel eens in aanraking met een risico. Echter wanneer iemand over een risico praat, is dit altijd open voor eigen interpretatie. Het is dan ook in het belang voor dit onderzoek om duidelijk te hebben wat een risico precies is en welke definitie van een risico wordt gehanteerd. Er zijn veel bronnen te vinden die het begrip risico definiëren. Onderstaand een opsomming van deze verschillende bronnen en de door hun geformuleerde definitie.

Definities risico.	
Bron:	Definitie van risico:
International Organization for Standardization (ISO) Guide 73.	Effect bij onzekerheid over doelstellingen. Houd er rekening mee dat een effect positief, negatief of een afwijking van het verwachte effect kan zijn. Ook wordt risico vaak beschreven als een gebeurtenis, een verandering in omstandigheden of een gevolg (ISO, 2017).
Institute of Risk Management (IRM).	Risico is de combinatie van de kans op een gebeurtenis en het gevolg ervan. Gevolgen kunnen variëren van positief tot negatief (Institute of Risk Management, z.d.).
Orange Book from HM Treasury.	Onzekerheid over de uitkomst, binnen een bereik van blootstelling, als gevolg van een combinatie van de impact en waarschijnlijkheid van mogelijke gebeurtenissen (Government Finance Function, 2021).
Institute of Internal Auditors (IIA).	De onzekerheid van een gebeurtenis die van invloed kan zijn op het behalen van de doelstellingen. Risico wordt gemeten in termen van gevolgen en waarschijnlijkheid (Chartered Institute of Internal Auditors, 2022).
Dikke van Dale.	Het gevaar van schade of verlies, de gevaarlijke of kwade kans of kansen dat zich bij iets voordoen (Van Dale, z.d.).
Risicogestuurd werken in de praktijk.	Risico is een onzekere gebeurtenis met oorzaken, een kans van optreden en effecten op doestellingen (Van Staveren, 2015).
Risk analysis and the security survey.	De waarschijnlijkheid van de gebeurtenis van een ongewenst incident (Broder & Tucker, 2012).

Veiligheid, Security Risk en Intelligence Management in de 21e eeuw.	Een kans op verlies op schade, vermenigvuldigd met het potentiële effect (impact) dat dit verlies of schade oplevert (kans x effect) (Geraets, 2016).
Ministerie van Defensie, ABDO 2019.	Het product van de kans dat een dreiging zich daadwerkelijk manifesteert en het effect daarvan op het voortzettingsvermogen van defensie, kortweg: risico = kans x effect (ministerie van Defensie, 2021b, mei 19, p. 6).
United States Army.	Waarschijnlijkheid en ernst van verlies in verband met gevaren (Headquarters, Department of the Army, 2021).

Tabel 5: Risico definities.

Zoals bovenstaande tabel laat zien worden er veel verschillende definities gebruikt voor het begrip risico. Veelal hebben de verschillende bronnen het over onzekerheid, een kans van optreden en een gebeurtenis dat een effect dan wel gevolg kan hebben op de doelstellingen die gesteld zijn. Kijkend naar de overeenkomsten van de genoemde definities kan er gesteld worden dat er vier variaties van de term risico zijn.

1. risico als kans op een ongewenste gebeurtenis;

2. risico als gevolg van een dergelijke gebeurtenis;

3 risico als ongewenste gebeurtenis zelf;

4. risico als oorzaak van die gebeurtenis.

Van Staveren (2015) onderschrijft genoemde vier variaties ook. Nadeel van de verschillende variaties is dat men een andere invulling of interpretatie kan geven aan het begrip risico. Het geven van een andere invulling of interpretatie kan bijvoorbeeld resulteren in miscommunicatie tussen stakeholders. Om dit te voorkomen zal er voor dit onderzoek een eenduidige definitie van het begrip risico gehanteerd worden. Van Staveren (2015) brengt diverse risico definities bij elkaar en komt tot de werkdefinitie: Risico is een onzekere gebeurtenis met oorzaken, een kans van optreden en effecten op de doelstelling.

2.2.2 Soorten risico's

Nu er een definitie is gekozen voor het begrip risico kan er worden gekeken wat voor risico's er allemaal bestaan. Wanneer het woord risico wordt genoemd denkt men meestal aan een negatief iets. Echter kunnen risico's zowel positief als negatief van aard zijn. Een voorbeeld van een positief risico is het bewust nemen van risico's door een investeerder om zodoende meer rendement te behalen op zijn investering. Echter is het ook mogelijk dat zijn bewuste risiconeming verkeerd uitpakt en dat een deel of alles van het geïnvesteerde verloren gaat. Positieve risico's worden dan ook wel kansen genoemd en negatieve risico's bedreigingen. Het woord risico geeft dan ook aan dat er onzekerheid is over de toekomst en die kan zowel positief als negatief uitvallen.

Net zoals risico's zowel positief als negatief kunnen uitvallen kunnen risico's ook ontstaan vanuit verschillende oorzaken. Deze oorzaken hangen vaak samen en zijn veelal een combinatie van technische, menselijke of organisatorische aard. Daarnaast zijn er factoren die deze oorzaken versterken en daarmee de escalatie van een risico in gang zetten (Van Staveren, 2015, p. 48).

HOT- RIP factoren.		
H: Human (mens).	O: Organizational (Organisatie).	T: Technological (Techniek).
Oorzaken van risico's.		
R: Regulations (Regulering).	I: Industry (Sector).	P: Politics (Politiek, pers, publiek).

Tabel 6: HOT-RIP factoren (Van Staveren, 2015, p. 48).

Bovenstaand een schema met de zogenaamde HOT- RIP factoren. De zogenaamde HOT- factoren zijn event-triggers en veroorzaken een risico. De zogenaamde RIP- factoren zijn event accelerators. Bij het manifesteren van een risico zorgen de RIP-factoren voor een escalatie van het risico.

Risico's kunnen ook onderscheiden worden op basis van hun aard. Hierbij ontstaan er onder meer strategische en operationele risico's. Strategische risico's hangen voornamelijk samen met de strategische keuzes die een organisatie maakt. Het zijn risico's die nauw verbonden zijn met de missie, visie en strategisch management van een organisatie. Veelal zijn strategische risico's dan ook positief van aard en gericht op waardevermeerdering. Uiteraard kunnen strategische keuzes ook verkeerd uitpakken en niet tot het gewenste resultaat leiden. Operationele risico's zijn gevolgen van falende interne processen, mensen of van externe gebeurtenissen (Blunden & Thirlwell, 2013).

Door de hedendaagse regelgeving en inrichting van organisaties zijn er ook andere risicocategorieën ontstaan. Voor risico's aangaande naleving van wet- en regelgeving spreekt men over compliance risico's. Bij natuurlijke fenomenen zoals natuurrampen of (veelal externe) invloeden zoals een terroristische aanslag en of diefstal wordt er gesproken over veiligheidsrisico's. Financiële risico's ontstaan vanuit financiële ontwikkelingen en bijhorende instrumentarium. Afsluitend zien organisaties verslaglegging ook als een risicocategorie. Bij verslaglegging risico's gaat het om de betrouwbaarheid van de verslaglegging en kunnen de eisen dus verschillen per sector, branche en organisatie (Van der Waal, 2019, p. 22). Dit onderzoek richt zich voornamelijk op operationele- en veiligheidsrisico's. Echter zullen andere risico categorieën ook altijd in mindere mate aanwezig zijn. Defensieorderbedrijven die een bijzondere opdracht gaan uitvoeren dienen vanuit compliance oogpunt te voldoen aan de normen die de ABDO stelt, hier door kunnen er bijvoorbeeld verschillende compliance risico's ontstaan.

Operationele- en veiligheidsrisico's zijn nauw verweven met elkaar. Ze kunnen leiden tot gebeurtenissen die het behalen van de beoogde doelstellingen in gevaar kunnen brengen. Het niet-geautoriseerde gebruik, verlies, beschadiging, openbaarmaking, wijziging van organisatorische activa voor de winst, persoonlijke- of politieke belangen van individuen, groepen of andere entiteiten (zoals statelijke actoren) brengt (ongewenste) nadelige effecten met zich mee en veroorzaakt bijvoorbeeld ook risico's die mogelijke schadelijk kunnen zijn voor mensen. Daarnaast kunnen beide risicocategorieën ook nadelige gevolgen hebben voor het voortbestaan van een onderneming, omgeving, zijn bedrijfsonderdelen, partners en klanten (Talbot & Jakeman, 2009).

Zoals eerder werd beschreven biedt een volledig en adequaat geïmplementeerde ABDO, de gewenste bescherming tegen risico's (middels de vastgestelde daderprofielen) die defensie voor defensieorderbedrijven hanteert. Echter ontstaan door verloop van tijd, omgeving, soort van werkzaamheden en andere denkbare factoren wellicht ook andere, onbekende risico's. Het is dus van belang dat de verschillende risico's continue inzichtelijk gemaakt worden en hiermee gekend worden, gelukkig zijn er verschillende methodes ontwikkeld om dit adequaat te kunnen bewerkstelligen (zie 2.2.4 Risicomanagementmethoden).

2.2.3. Risicomanagement

De betekenis van het woord management is volgens Van Dale (z.d.) het leiden van een bedrijf of instelling. Wanneer dit gecombineerd wordt met het woord risico kan er gesproken worden over het woord risicomanagement. Maar wat is risicomanagement nou eigenlijk? Heeft het wellicht te maken met het managen van risico's? In de voorgaande paragraaf is gedefinieerd dat een risico een onzekere gebeurtenis is met oorzaken, een kans van optreden en dat het effecten heeft op doelstellingen. Doelstellingen worden gemaakt om iets te bereiken, voor defensieorderbedrijven kan bijvoorbeeld een doelstelling zijn om de defensieopdrachten af te ronden binnen een bepaalde begroting of termijn. Om te zorgen dat geformuleerde doelstellingen niet ongewenst beïnvloed kunnen worden kan er risicomanagement toegepast worden. Door het toepassen van risicomanagement kunnen risico's vermeden, gereduceerd, overgedragen of geaccepteerd worden. Samenvattend kan er ook wel gezegd worden dat risicomanagement een bedrijf of organisatie in staat stelt om zijn beoogde doelstellingen te behalen.

Er zijn veel bronnen die ook schrijven over het begrip risicomanagement. Organisaties zoals ISO, Institute of Risk Management, HM Treasury en Londen School of Economics hanteren allemaal een eigen definitie van risicomanagement. Paul Hopkin voegt in zijn boek Fundamentals of Risk Management (Hopkin, 2018) de definities van genoemde organisaties samen en komt tot de definitie; 'risicomanagement is de reeks van activiteiten die binnen een organisatie worden ondernomen om de meest gunstige uitkomst te leveren en de volatiliteit of variabiliteit van die uitkomst te verminderen'. Van Staveren (2015) heeft een andere definitie voor risicomanagement. Volgens van Staveren (2015) is risicomanagement doelgericht, expliciet, gestructureerd, gecommuniceerd en continue omgaan met risico's. Deze definitie geeft in tegenstelling van die van Paul Hopkin (2018), eenvoudig en beknopt aan waar risicomanagement in essentie om draait.

Definitie risicomanagement voor dit onderzoek.
Risicomanagement is doelgericht, expliciet, gestructureerd, communicerend en continue omgaan met risico's.

Tabel 7: Definitie risicomanagement (Van Staveren, 2015).

Gezien de eenvoudigheid en beknoptheid zal de geformuleerde definitie van M. van Staveren (2015) voor eenduidigheid ten behoeve dit onderzoek verder worden gebruikt. Concluderend kan er wel gezegd worden dat de verschillende definities laten zien dat er geen goed of fout is, het is voornamelijk van belang dat alle stakeholders weten wat risicomanagement is en wat daarbij verwacht kan worden.

2.2.4. Risicomanagement in ontwikkeling

Risicomanagement wordt al vele jaren toegepast in verschillende mate en vormen. De eerste pogingen om risico's te beheersen dateert al uit de zeventiende of achttiende eeuw. Japanse rijstboeren maakten afspraken met de koper/afnemer om in een later stadium vooraf vastgestelde hoeveelheden rijst te leveren tegen een vooraf gestelde prijs (Dionne, 2013). Genoemde afspraak gaf de koper en de verkoper beide duidelijkheid, de rijstboer wist hoeveel omzet hij ging genereren en moest produceren en de koper wist precies zijn kosten en de hoeveelheid rijst die hij daarvoor zou krijgen. Hiermee werden risico's voor beide partijen gemitigeerd. Medio 1980 ontstond er een beweging dat er binnen grote Amerikaanse afdelingen werden opgericht die gespecialiseerd waren in financieel risicomanagement. Grote volumes van financiële tegoeden werden verhandeld en moesten beschermd worden tegen ongewenste gebeurtenissen. Desondanks de professionalisering in de jaren 80, vonden er in de jaren negentig diverse schandalen plaats waarbij er sprake was van grote financiële verliezen. Door deze negatieve ervaringen kregen organisaties een ander beeld van risicomanagement, dit resulteerde tot de doorontwikkeling van verschillende risicomethodieken die hedendaags nog toegepast worden (Van der Waal, 2019).

Zoals te lezen heeft risicomanagement al een flinke geschiedenis en daarmee ontwikkeling doorgemaakt. Dit is dan ook de reden dat er voldoende informatie over risicomanagement aanwezig is. Voor dit onderzoek zullen we ons dan ook niet verder richten op de geschiedenis van risicomanagement, maar nemen we vanaf nu enkel de ontwikkelingen en actuele toepassingen van risicomanagement aangaande de afgelopen jaren in beschouwing. Zoals eerder benoemd ontstond er door verschillende gebeurtenissen en ervaringen een andere kijk op risicomanagement. Risicomanagementmethoden werden doorontwikkeld tot de methodes die tegenwoordig veelal gangbaar zijn. Deze methoden noemt men ook wel de conventionele risicomanagementmethoden.

Kenmerken van conventioneel management naar vernieuwend management.		
Wat:	Kenmerken van conventioneel risicomanagement.	Kenmerken van risicogestuurd werken.
1.	Methode is leidend.	Doelen zijn leidend.
2.	Eén doel.	Enkele doelen.
3.	Geld is dominant.	Waarde is dominant.
4.	Standaardisatie.	Variatie.
5.	Variatie minimaliseren.	Variatie benutten.
6.	Onteigenen.	Eigenaarschap.
7.	Schaalvergroting.	Functionele omvang.
8.	Low trust – high tolerance.	High trust – low tolerance.
9.	Afdwingen.	Uitnodigen.
10.	Zeker willen weten.	Onzekerheid toelaten.
11.	Compleet willen zijn.	Keuzes durven maken.
12.	Meer onderzoek vragen.	Beperkingen onderzoek aangeven.
13.	Alleen lineair.	Lineair en cyclisch.
14.	Ontwerpen.	Ontwikkelen.
15.	Statisch.	Dynamisch.
16.	Oorzaak – gevolg.	Interactie.
17.	Uitsluiten van verspilling.	Kleine verspilling accepteren.
18.	Fouten uitsluiten.	Fouten vroegtijdig opmerken.
19.	Kansen op risico's verkleinen.	Gevolgen van risico's verkleinen.
20.	Antwoorden geven.	Vragen stellen.

Tabel 8: Kenmerken conventioneel management naar vernieuwend management (Van Staveren, 2015, p. 33 met referentie aan Wouter Hart (2013).

Bovenstaand tabel laat zien dat bij het toepassen van conventionele risicomanagementmethoden de methode lijdend is. De implementatie van conventioneel risicomanagement vindt plaats op strategisch niveau en richt zich tot het behalen van één doel. Resultaat hiervan is dat risico's op andere niveaus verminderd zichtbaar zijn en personeel een mindere mate van risico-eigenaarschap ervaart. Het is dan ook verklaarbaar dat conventioneel risicomanagement een verandering doormaakt, gezien alle interne- en externe invloeden op organisaties van nu. De klassieke silobenadering wordt dan ook steeds meer losgelaten (Dornberger, Oberlehner & Zadrazil, 2014).

Bij de silobenadering wordt risicomanagement binnen diverse onderdelen van de organisatie los van elkaar uitgevoerd en ontbreekt er een samenhang tussen onderdelen. Hedendaags risicomanagement verschuift dan ook steeds meer naar een andere vorm om zodoende gestructureerd met risico's om te kunnen gaan. Hoofdzakelijke reden hiervan is dat veranderingen in de hedendaagse wereld elkaar steeds sneller opvolgen. Hierbij valt te denken aan technologische ontwikkelingen zoals cyber, Big Data. Maar ook op sociaal gebied door veranderingen in veiligheid door (dreiging van) statelijke actoren en terrorisme.

Daarnaast onderschrijven verschillende onderzoeken dat het beoogde resultaat van het toepassen van conventioneel risicomanagement niet behaald worden. Een voorbeeld, in 2014 is gezamenlijk door Rijksuniversiteit Groningen, Nyenrode School of Accountancy Breukelen, NBA en PwC (2014) het Tweede Nationale Onderzoek Risicomanagement uitgevoerd. Ruim 700 Nederlandse organisaties hebben deelgenomen aan de enquête. Zowel de profit als de non-profit sector scoort gemiddeld met een 4,5 onvoldoende. Maar in de tegelijkertijd uitgevoerde zelfevaluatie beoordelen bestuurders en managers het toepassen van risicomanagement in hun organisatie als ruim voldoende. Hieruit kan dan ook geconcludeerd worden dat conventioneel risicomanagement niet doordringt tot alle niveaus binnen een organisatie.

Ook de medewerkers van Bureau Industrieveiligheid bemerken (diverse accountmanagers van Bureau Industrieveiligheid, persoonlijke communicatie, augustus 8, 2022) in de dagelijkse praktijk dat de kenmerken van vernieuwend management aansluiten bij de uitvoering van een bijzondere opdracht (zie bijlage één). In onderstaande tabel zijn enkele vernieuwende kenmerken geselecteerd die gemotiveerd zullen worden waarom ze meer passend zijn in de huidige dagelijkse praktijk.

Vernieuwend management in de dagelijkse praktijk.		
Wat:	Vernieuwd management:	Motivatie:
1.	Doelen zijn leidend (Van Staveren, 2015, p. 82 naar Wouter Hart (2013).	Risicomanagementmethoden dienen een defensieorderbedrijf te ondersteunen bij het realiseren van de gestelde doelen. Veelal is het hanteren van één risicomanagementmethode niet mogelijk gezien een defensieorderbedrijf aan verschillende voorgeschreven kwaliteits- en compliance richtlijnen moet voldoen.
3.	Waarde is dominant (Van Staveren, 2015, p. 82 naar Wouter Hart (2013).	Met conventioneel risicomanagement werd alles veelal in geld uitgedrukt. Echter is bij een bijzondere opdracht de inschaling van een Te Beschermen Belang van toepassing. Hiervoor wordt er gekeken naar betrouwbaarheid, integriteit en vertrouwelijkheid van personeel, informatie, materieel, goederen en objecten (Ministerie van Defensie, 2021b, p. 6)
6.	Eigenaarschap (Van Staveren, 2015, p. 82 naar Wouter Hart (2013).	Bescherming van een Te Beschermen Belang begint met een breed gedragen en structureel gehandhaafd beveiligingsbeleid, bekrachtigd door het hoogste bestuursorgaan. Het vervolgens opgestelde beveiligingsplan en de implementatie van de adequate beveiligingsmaatregelen vormen de basis voor succesvolle beveiliging. Beveiligingsbewustzijn is van groot belang. Pas als de gehele organisatie, van hoog tot laag, is doordrongen van de waarde van een Te Beschermen Belang, kan een bedrijfscultuur ontstaan waarin een Te Beschermen Belang ook door alle medewerkers als zodanig wordt behandeld (Ministerie van Defensie, 2021b, p. 10).
18.	Fouten vroegtijdig opmerken (Van Staveren, 2015, p. 82 naar Wouter Hart (2013).	Wanneer er fouten gemaakt worden met betrekking tot een bijzondere opdracht dient de opdrachtnemer dit te melden middels de incidentmeldingsprocedure die de ABDO hanteert. De ABDO beschrijft veel maatregelen die moeten bijdragen in het vroegtijdig signaleren van fouten (bijvoorbeeld ieder jaar een security awareness training voor alle betrokken medewerkers om zo de waarde van een bijzondere opdracht te duiden.).

20.	Vragen stellen (Van Staveren, 2015, p. 82 naar Wouter Hart (2013).	Niet alleen bestaande beveiligingsplannen en geformuleerde risicodossiers zijn leidend. Dit is immers al allemaal bekend. Bij vernieuwend risicomanagement gaat het niet om wat je zoekt, maar wat je vindt. Want bij zoeken heb je immers al een beeld naar wat je zoekt (Van Staveren, 2015, p. 92). Door minder gericht te zoeken en te praten met alle stakeholders en risico eigenaren worden er wellicht risico's gevonden die anders niet waren gezien. In de dagelijkse praktijk vertaalt dit zich terug in de taken en werkzaamheden van risico eigenaren, beveiligingsfunctionarissen en (de medewerkers van) Bureau Industrieveiligheid.

Tabel 9: Vernieuwend management in de dagelijkse praktijk.

Zoals alle motiveringen van bovenstaand tabel laten zien past vernieuwend management bij de uitvoering van een bijzondere opdracht en daarmee de ABDO. De accenten van vernieuwend management vragen om een actieve benadering en continuïteit. Het vullen van draaiboeken volstaat niet meer, men moet iedere dag, op ieder niveau actief bezig zijn met het omgaan van risico's. Niet alleen in risicomanagement vindt een verschuiving plaats, maar ook in andere managementgebieden. De meest recente versie van de ISO 9001-norm voor kwaliteitsmanagement onderschrijft dit: leiderschap heeft een geheel eigen hoofdstuk gekregen, en onderwerpen zoals communicatie, mensen betrekken en faciliteren komen ruim aan bod. Het beschrijft niet meer wat je vastlegt, maar dat je het vastlegt wat je zelf nodig acht. De verbinding tussen strategie en de dagelijkse praktijk, tussen management en werkvloer staan dan ook in deze ISO centraal. Net zoals kwaliteitsmanagement vraagt de dagelijkse realiteit voor risicomanagement ook een vernieuwde manier van werken, waarbij zaken zoals doelen, mensen en risico eigenaarschap centraal staan.

2.2.5. Risicomanagementmethoden

Met de voorgaande paragrafen is er bekeken wat een risico betekent, wat risicomanagement is en hoe het zich ontwikkeld van conventioneel risicomanagement naar vernieuwend risicomanagement. Deze paragraaf zal zich richten op bekende en veel toegepaste risicomanagementmethoden in Nederland. Deze methoden zijn voornamelijk een middel om op gestructureerde wijze risico's te inventariseren, te evalueren, er proactief mee om te gaan en te beheersen. Eerst zullen drie meer conventionele risicomanagementmethoden beschreven worden, namelijk de COSO-ERM, ISO 31000 en RISMAN. Afsluitend zal er naast de drie genoemde methoden een vernieuwde manier van werken geïntroduceerd worden en zal ook deze methode inzichtelijk gemaakt worden. Daarbij zal er een verdere onderbouwing plaatsvinden waarom deze methode, net zoals de eerder gemotiveerde vernieuwende kenmerken, meer passend is voor gebruik ter ondersteuning van de ABDO in de dagelijkse praktijk.

2.2.5.1. COSO-ERM.

De geschiedenis van het model Commission of Sponsoring Organizations of the Treadway Commission, ofwel COSO genoemd begint met de introductie van de Foreign Corrupt Practices Act in 1977, die werd opgesteld naar aanleiding van het Watergate-schandaal (1973) ter preventie van omkopingspraktijken in de Verenigde Staten en daarbuiten. De wet eiste dat ondernemingen een goede interne (risico) beheersing moesten hebben. In de opvolgende jaren zijn er verschillende COSO-raamwerken gepresenteerd waarvan de COSO-ERM hedendaags de populairste is (Hopkin, 2018).

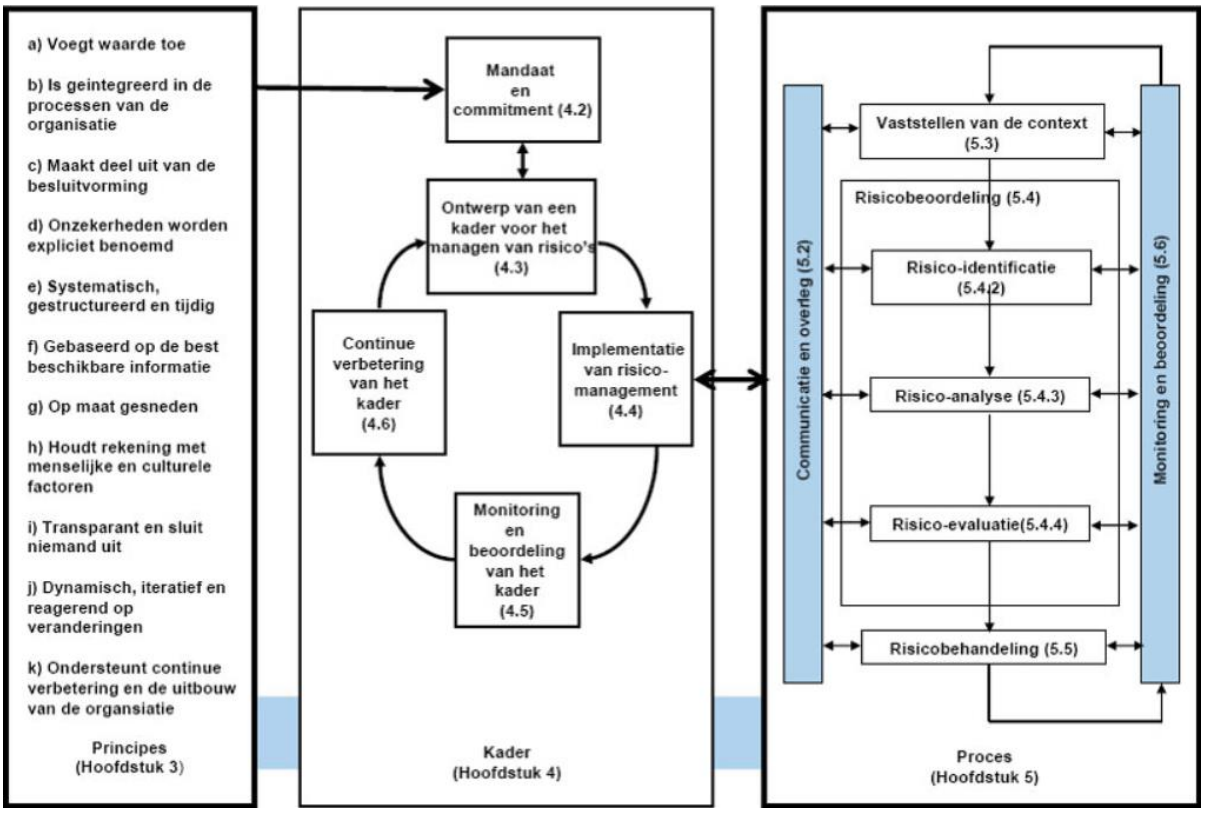
Figuur 1: COSO (Hopkin, 2018).

COSO identificeert de relaties tussen ondernemingsrisico's en het interne beheersingssysteem. Op de bovenzijde staan verschillende doelstellingen die een onderneming kan hebben.

De acht beheers componenten aan de voorzijde weergeven wat er nodig is om de geformuleerde doelstellingen te behalen. Mocht een component niet tot de geformuleerde doelstellingen toewerken dan is er afdoende controle, ofwel een risico. Nu het duidelijk is wat het risico is, kan er geïnventariseerd worden waar het zich precies bevindt. De rechterzijde van de kubus toont de verschillende eenheden van een onderneming. Door alle eenheden te bestuderen in relatie tot het risico kan er inzichtelijk gemaakt worden op welk niveau en plek er geen volledige controle op een risico is. Nu alles inzichtelijk gemaakt is kan het management keuzes maken of er beheersmaatregelen toegepast moeten worden om de geformuleerde doelstellingen toch te kunnen behalen.

2.2.5.2. ISO 31000.

International Organization for Standardization, ofwel ISO is ontstaan ten behoeve van kwaliteitsmanagementsystemen vanuit de militaire wapenindustrie. In 1959 stelde de NAVO hoge eisen aan al hun toeleveranciers waaraan ze aantoonbaar diende te voldoen. Dit was dan ook de basis van de ISO-kwaliteitseisen. ISO 31000 (2021) is het raamwerk voor risicomanagement. ISO 31000 biedt een algemeen kader voor ondernemingen die risicomanagement in de praktijk willen brengen.



Figuur 2: ISO (ISO, 2021).

Principes

Om effectief risicomanagement te kunnen toepassen dient er volgens de ISO 31000 te worden voldaan aan elf principes van risicomanagement. Desbetreffende principes benoemen een aantal kenmerken die al aan bod zijn gekomen tijdens het definiëren van het begrip risicomanagement.

- Het voegt waarde toe en draagt bij aan de verbetering van de onderneming;
- Het is integraal onderdeel van de (besluitvorming)processen;
- Het is maatwerk, past bij de context van de onderneming en speelt in op veranderingen;
- Het is systematisch ingericht;
- Het is open en transparant en heeft oog voor culturele en menselijke factoren.

Kader

Naast genoemde principes, heeft de ISO 31000 ook een raamwerk (kader) dat er zorg voor moet dragen dat risicomanagement ingebed wordt en blijft binnen een onderneming. Het raamwerk is cyclisch van aard ondersteunt het management met het continueren van risicomanagement in relatie tot visie, beoogde doelstellingen en het daadwerkelijke uit te voeren beleid.

Proces

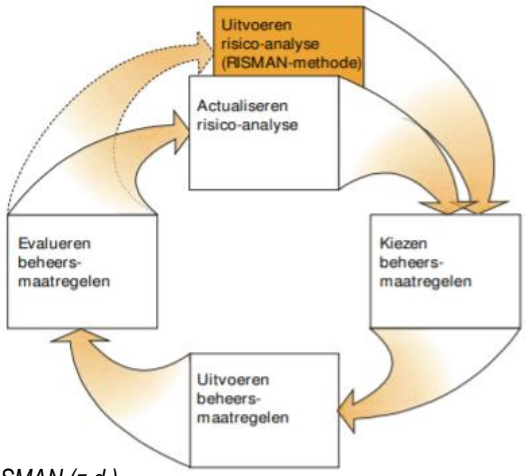
Het risicomanagementproces dat de ISO 31000 beschrijft, bestaat uit zes stappen die gezamenlijk inzicht geven in risico's en een onderneming in staat stellen om gevonden risico's te beheersen. De eerste stap is het vaststellen van de situatie en omgeving waarin een onderneming zich bevindt. In het hart van het proces zitten stappen zoals identificeren, analyseren en evalueren van risico's. Genoemde stappen maken gezamenlijk de risicobeoordeling. Tijdens het gehele proces vindt interne en externe communicatie, monitoring en beoordeling plaats.

Wanneer de context duidelijk is en de risicobeoordeling geanalyseerd is middels het doorlopen van alle stappen kan er overgegaan worden tot risicobehandeling. De stap risicobehandeling stelt de onderneming in staat om op basis van alle verkregen informatie een risicobeheersmaatregel te kiezen. Er kan bijvoorbeeld gekozen worden om een risico te vermijden, te reduceren, te accepteren of te overdragen. Ten einde vindt er rapportage, consolidatie en een nieuwe start van het proces plaats. Het ISO 31000 (2021) risicomanagementproces is dan ook cyclisch van aard.

2.2.5.3. RISMAN

De RISMAN-methode (Kenniscentrum RISMAN, z.d.) is een methode voor risicoanalyse en het toepassen van risicomanagement in projecten, ondernemingen en organisaties. De methode is tussen 1992 en 1999 ontwikkeld door een samenwerkingsverband van diverse ondernemingen en organisaties gezien er een behoefte was om risico's beter te kunnen beheersen. De RISMAN-methode wordt veelal toegepast bij bouw- en infrastructuurprojecten.

Doel van de RISMAN-methode is het continue expliciet maken risico's en deze te beheersen. In plaats van reactief omgaan met risico's, helpt de methode risico's proactief te benaderen. De RISMAN-methode stelt dan ook de gebruiker in staat om bewust om te gaan met risico's en bijhorende beheersmaatregelen op basis van een risicoanalyse te selecteren. De RISMAN-methode is cyclisch van aard en doorloopt vijf stappen om tot risicomanagement te komen.



Figuur 3: RISMAN (Kenniscentrum RISMAN (z.d.).

Stap één: Het uitvoeren van een integrale risicoanalyse

De eerste stap van de RISMAN-methode is het inzichtelijk maken van de IST, de huidige stand van zaken op een bepaald moment. Dit zal gebeuren door het uitvoeren van een integrale risicoanalyse. Om een integraal beeld te verkrijgen richt de RISMAN-methode zich tot de onderstaande invalshoeken.

- Politiek / bestuurlijk;
- Financieel / economisch;
- Juridisch / wettelijk;
- Technisch;
- Organisatorisch;
- Geografisch / ruimtelijk;
- Maatschappelijk.

Wanneer uitgevoerd zal, stap één inzicht geven in de risico's die relevant zijn voor de beoogde doelstellingen.

Onderkende risico's worden gesorteerd op volgorde gezien de grootte van de dreiging met daarbij mogelijke beheersmaatregelen die de kans van optreden verkleinen dan wel de gevolgen verkleinen.

Stap twee: Het vaststellen van beheersmaatregelen

De voorgaande risicoanalyse (stap één) heeft aangetoond wat de belangrijkste risico's zijn en welke mogelijke beheersmaatregelen van toepassing kunnen zijn. In deze stap zal er een besluit gemaakt worden welke beheersmaatregelen er daadwerkelijk genomen worden. Dit besluit zal gemaakt worden op basis van het verwachte effect van de beheersmaatregelen en welke inspanning (en of kosten) desbetreffende beheersmaatregel vergt. Daarnaast zal er bepaald worden wie verantwoordelijk is en wie de implementatie zal gaan doen.

Stap drie: Het implementeren van de gekozen beheersmaatregelen

Zoals bepaald in stap twee zullen de aangewezen functionarissen, afdelingen et cetera, de geselecteerde beheersmaatregelen (laten) implementeren.

Stap vier: Het evalueren van de geïmplementeerde beheersmaatregelen

De geïmplementeerde beheersmaatregelen dienen op regelmatige basis gecontroleerd te worden op werking, effectiviteit en noodzakelijkheid (risicomonitoring).

Stap vijf: Actualiseren risicoanalyse

Na de evaluatie van stap vier dient er een update gemaakt te worden van de lijst met risico's, zoals die oorspronkelijk is voortgekomen uit de risicoanalyse. Dit geeft de gelegenheid om risico's die niet meer actueel zijn te verwijderen en om nieuwe risico's toe te voegen aan de lijst. Naast het updaten van de lijst zal men middels een gezamenlijk dialoog bepalen of er nieuwe risico's geïdentificeerd zijn. Er zullen nieuwe beheersmaatregelen geïnventariseerd worden wanneer er sprake is van nieuwe risico's.

2.2.5.4. Risicogestuurd werken

Zoals eerder benoemd vindt er een verschuiving plaats van conventioneel- naar vernieuwend management. De voorgaande beschreven methoden zijn prima en toepasbaar, maar sluiten steeds minder aan bij de dagelijkse realiteit. De wereld zoals we die vandaag kennen wordt in het risicomanagementlandschap steeds meer beschreven als een VUCA-wereld. De term VUCA staat voor volatility (snelheid van verandering), uncertainy (onzekerheid rondom gebeurtenissen), complexity (complexiteit van de omgeving) en ambiquity (onduidelijkheid over oorzaak en gevolg) (Horney, Pasmore & O'Shea, 2010). Door deze VUCA-kenmerken is het voor organisaties steeds belangrijker om vanuit risicomanagementperspectieven in te spelen op de veranderingen in zijn omgeving.

Gezien de VUCA-wereld is het ook verklaarbaar dat er verschillende gerenommeerde instituten verkenningen schrijven over hoe er gestructureerd omgegaan kan worden met risico's. TNO (2017) heeft bijvoorbeeld een verkenning geschreven aangaande het sturen risico's in het veiligheidsdomein, bekeken vanuit het grensproces op luchthavens. In deze verkenning komt expliciet naar voren dat de manier waarop we omgaan met risico's veranderd, en dat het invloed heeft op de wijze waarop organisaties aangestuurd worden.

Eén conclusie van dat rapport is dan ook dat risico's niet meer enkel meer op conventionele, ook wel strategische manier moeten worden beheerst, maar iedere risico op zijn eigen niveau. Er vindt dan ook de afgelopen jaren een verschuiving plaats in het hedendaagse risicomanagement landschap. In plaats van conventioneel risicomanagement implementeren organisaties steeds meer het vernieuwende risicogestuurd risicomanagement, ofwel ze gaan risicogestuurd werken.

Risicogestuurd werken is gerelateerd aan het verminderen van de kans op een ongewenste gebeurtenis of het verminderen van het gevolg van deze ongewenste gebeurtenis. Risicogestuurd werken stelt een organisatie in staat om doelgericht te sturen op risico's die effect kunnen hebben op het behalen van zijn doelstellingen. Risico's die effect kunnen hebben op doelstellingen worden met risicogestuurd werken op ieder niveau inzichtelijk gemaakt. Niet alleen het management en het strategische niveau, maar iedereen binnen een organisatie wordt met risicogestuurd werken, risico-eigenaar. Risicogestuurd werken leent zich dan ook tot een meer flexibele wijze van risicomanagement. Het behalen van doelstellingen staat met risicogestuurd werken op ieder niveau centraal. Niet de methode, maar het maken van keuzes kijkend naar de risico's op doelstellingen staan meer centraal. Beschreven kenmerken van risicogestuurd werken laten dan ook zien dat deze manier van werken vraagt om een andere vorm van implementatie dan de conventionele risicomanagementmethoden. Van Staveren (2015) beschrijft dat er pas sprake is van risicogestuurd werken wanneer een implementatie volledig voldoet aan de '4 G's. Omgaan met risico's is dan (van Staveren, 2015, p. 102) gestructureerd, geformaliseerd, geïntegreerd en geaccepteerd. In de volgende vier sub-paragrafen zullen de '4 G's, afzonderlijk inhoudelijk toegelicht worden.

G-1: Gestructureerd: via de zes risicoprocesstappen

Zoals voorgaande drie risicomethoden laten zien bestaan er verschillende, maar toch enigszins vergelijkbare interpretaties van (conventioneel) risicomanagement. Net zoals de begrippen risico en risicomanagement, brengt Van Staveren (2015) in het boek Risicogestuurd werken in de praktijk ook de beschreven risicomanagementmodellen tot elkaar. In zijn boek worden de risicomanagementmethoden COSO-ERM, ISO 31000 en RISMAN gefilterd en teruggebracht naar zes gestructureerde, generieke risicoprocesstappen.

Stap één: doelen bepalen

In deze stap worden relevante doelen bepaald. Desbetreffende doelen kunnen operationeel, tactisch en of strategisch van aard zijn.

Stap twee: risico's identificeren

In deze stap worden alle risico's geïdentificeerd die de voorgaande doelstellingen negatief of positief kunnen beïnvloeden. Desbetreffende risico's kunnen kwalitatief of kwantitatief inzichtelijk gemaakt worden.

Stap drie: risico's classificeren

De (relevant) geïdentificeerde risico's worden in deze stap gewogen. Dit gebeurt veelal door kans x effect = risico. In deze stap is het van belang dat er goed gecommuniceerd wordt over risicoperceptie. Risicoperceptie kan (vaak) een onbewuste rol spelen bij het (on)juist classificeren van risico's.

Stap vier: risico's beheersen

Een risico kan voorkomen, verzekerd of geaccepteerd worden. Daarnaast kan een risico ook overgedragen geworden aan een andere partij. In deze stap wordt er bewust een keuze gemaakt hoe een risico gemitigeerd of toch geaccepteerd moet worden.

Stap vijf: risicobeheersmaatregelen evalueren

Met deze stap wordt nagegaan of de gekozen beheersmaatregelen het beoogde effect hebben.

Tevens dienen gekozen maatregelen periodiek beoordeeld te worden voor noodzakelijkheid en effectiviteit (risicomonitoring). Indien gewenst of noodzakelijk, kunnen gekozen beheersmaatregelen verminderd of opgehoogd worden.

Stap zes: overdracht risicodossier

De laatste stap gaat over communicatie en rapportage. Het is van belang dat er periodiek, kritisch gekeken wordt naar het gecreëerde risicodossier. Hierdoor ontstaat een lineair, dan wel cyclisch proces. Herhaling is van belang, risico's kunnen immers positief en of negatief veranderen. Genoemde stappen maken risicomanagement duidelijk en gestructureerd. Volgens Staveren (2015) zijn het in totaliteit zes generieke risicoprocestappen in werkprocessen. De zes stappen ondersteunen een organisatie in het risicogestuurd omgaan met risico's.

G-2: Geformaliseerd: officieel voorbij de vrijblijvendheid

Het uitvoeren van risicomanagement is het toepassen van de zes generieke risicomanagementprocesstappen. Echter zal er middels implementatie geborgd moeten worden dat het daadwerkelijk ook routinematig plaats vindt. Het is dus niet vrijblijvend, lineair en voor management. Risicogestuurd werken is voor iedereen en zal ter bevordering van de effectiviteit bij iedereen terug moeten keren zoals een doorlopend cyclisch risicoproces. Rollen, taken en verantwoordelijkheden zijn formeel afgesproken. Het omgaan met risico's wordt gedelegeerd naar personen die dit als onderdeel van hun dagelijkse werkzaamheden doen. Rapportages worden opgesteld met inachtneming van de geformuleerde doelstellingen en worden besproken met de juiste stakeholders. Op basis van formele afspraken wordt de externe omgeving betrokken en kunnen nieuwe inzichten effect hebben op de wijze waarop risico-gestuurd gewerkt toegepast wordt.

G-3: Geïntegreerd: onderdeel van de relevante werkprocessen

Risico's hebben effect op de gestelde doelen. Doelen zijn niet alleen strategisch en daarmee enkel voor het management, maar worden ook voor tactisch en operationeel niveau opgemaakt. Iedereen is risico-eigenaar en draagt bij aan het totale risicomanagement om zodoende de geformuleerde doelstelling op ieder niveau en werkproces te behalen. Om succesvol te zijn is de methode beschikbaar, toegankelijk, gebruiksvriendelijk en levert relatief voordeel voor de gebruikers op. Daarnaast sluit het naadloos aan op de werkprocessen en zijn de kosten acceptabel.

G-4: Geaccepteerd: iedereen ziet het nut ervan in en profiteert ervan

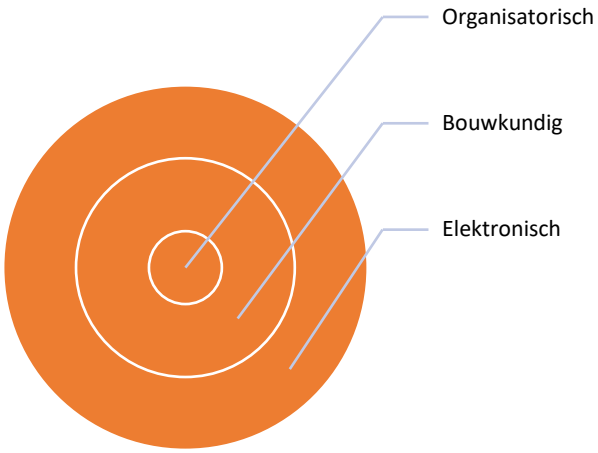
Naast structuurvoorwaarden die voornamelijk al besproken zijn is een bevorderlijke cultuur voor risicogestuurd werken zeer van belang. Om een effectief en bevorderlijke organisatiecultuur te creëren moet eenieder dezelfde taal spreken. Er moet sprake zijn van eenduidige werkdefinities voor risicogestuurd werken. Binnen een organisatie begrijpt iedereen dat risico-inschattingen subjectief zijn en verschillen in risicoperceptie en risicohouding uitgesproken en besproken worden. Omdat risico's discipline overstijgend kunnen zijn werken en communiceren interne, externe en multidisciplinaire teams met elkaar.

2.3 Theoretische verdieping ten behoeve van deelvraag twee

Deze paragraaf en bijhorende sub-paragrafen zullen zich richten op een verdieping van literatuur wat ten einde gebruikt zal worden voor het kunnen beantwoorden van deelvraag twee. De sub-paragrafen zullen zich dan ook richten of er met de ABDO, risicomanagement toegepast wordt bij een defensieorderbedrijf.

2.3.1. Integrale Beveiliging

De ABDO uit vier hoofdstukken met ieder zijn eigen aandachtgebied. Iedere norm afzonderlijk bied te weinig weerstand tegen een mogelijk risico. Het is dan ook van vitaal belang dat de vereiste beveiligingsnormen geïmplementeerd worden. De integraliteit van de beveiligingsnormen ten samen bereiken immers het beoogt, gewenste effect.



Figuur 4: OBE-beveiligingsmaatregelen.

Integrale beveiliging is dan ook een begrip dat steeds meer gebruikt wordt in het beveiligingsdomein. Maar wat is integrale beveiliging nou eigenlijk? Volgens Appelman (2010) is integrale beveiliging een 'allesomvattende' aanpak aangaande beveiliging. Dit betekent dat er een samenwerking en samenhang moet zijn tussen de verschillende soorten van beveiligingsmaatregelen om zodoende een bepaalde gelaagdheid in de beveiliging te creëren (zie bovenstaand figuur). Een enkele geïmplementeerde beveiligingsmaatregel is onvoldoende om een ongewenste risico te voorkomen, maar door het toepassen van integrale beveiliging (samenwerking, samenhang en gelaagdheid van diverse beveiligingsmaatregelen) wordt een risico beheersbaar. Integraliteit draagt dan ook bij aan een mate van gelaagdheid, wat resulteert dat bepaalde risico's niet meer mogelijk zijn of dat er voldoende tijd gegenereerd wordt om tijdig te kunnen interveniëren.

Maar wat moet er dan samenwerken? Binnen het beveiligingsdomein wordt er vaak onderscheid gemaakt tussen Organisatorische, Bouwkundige en Elektronische (OBE) beveiligingsmaatregelen. Ook wel de klassieke beveiligingsmaatregelgroepen genoemd. Deze drie maatregelgroepen komen dan ook terug in bijna alle beschikbare beveiligingsmethodieken. Volgens Appelman (2010) zijn de genoemde samenwerking en gelaagdheid van de drie maatregelgroepen gezamenlijk onvoldoende om te kunnen spreken van integrale beveiliging. Appelman (2010) vult de OBE-maatregelen aan met nog twee maatregelgroepen, namelijk Meldingen & stuurinformatie en Communicatie & bewustwording. Gezamenlijk noemt Appelman (2010) deze vijf maatregelgroepen MOBEC. De maatregelgroep Meldingen & stuurinformatie geeft informatie waar en hoe het beste beveiligd kan worden. Met Communicatie & bewustwording wil Appelman (2010) medewerkers van een organisatie bewuster maken van hun taken en verantwoordelijkheden het gebied van beveiliging.

2.3.1.1. Integrale beveiliging en risicomanagement

Wanneer de methodiek van Appelman (2010) wordt vergeleken met de klassieke benadering van integrale beveiliging (OBE) kan geconcludeerd worden dat de methode van Appelman in meer 'allesomvattende' aanpak voorziet.

Appelman (2010) richt zich niet alleen tot te nemen OBE-beveiligingsmaatregelen, maar inventariseert ook in de noodzaak daarvan. Daarnaast voorziet Appelman (2010) in tegenstelling van de klassieke benadering ook in het bewuster maken van de medewerker aangaande beveiliging. Dit laatste heeft een positief effect op de uitwerking van alle genomen beveiligingsmaatregelen. Gezien de operationaliserende werking van integrale beveiliging op het gebied van OBE-beveiligingsmaatregelen kan er tevens geconcludeerd worden dat integrale beveiliging onlosmakelijk bijdraagt aan de implementatie van risicomanagement.

2.3.2. Algemene Beveiligingseisen voor Defensieopdrachten 2019

Gezien de doelstelling van dit onderzoek zal deze paragraaf zich richten tot de meest recente versie van de ABDO. De ABDO 2019 bevat eisen voor de beveiliging van een kroonjuweel, ook wel een Te Beschermen Belang (TBB) genoemd, waaraan een defensieorderbedrijf aan moet voldoen om een bijzondere opdracht te mogen uitvoeren. Aan de productie, behandeling, verwerking, opslag en vernietiging van een TBB worden dus specifieke beveiligingseisen gesteld. Mocht het noodzakelijk zijn voor de uitvoering van de opdracht kan defensie (de opdrachtgever) het TBB overdragen aan het defensieorderbedrijf (de opdrachtnemer). Ook is het mogelijk dat de opdrachtnemer zelf een TBB bezit en of genereert. In beide gevallen wordt er gesproken over een bijzondere opdracht (BO).

NL rubricering	TBB categorie	Betekenis
Stg. ZEER GEHEIM.	TBB 1.	Kennisname door niet-gerechtigden kan zeer ernstige schade toebrengen aan het belang van de Staat of zijn bondgenoten.
Stg. GEHEIM.	TBB 2.	Kennisname door niet-gerechtigden kan ernstige schade toebrengen aan het belang van de Staat of zijn bondgenoten.
Stg. CONFIDENTEEL.	TBB 3.	Kennisname door niet-gerechtigden kan schade toebrengen aan het belang van de Staat of zijn bondgenoten.
DEPARTEMENTAAL VERTROUWELIJK.	TBB 4.	Kennisname door niet-gerechtigden kan nadeel toebrengen aan het belang van één of meer ministeries.

Tabel 10: Rubriceringen.

In bovenstaand tabel is zichtbaar dat in de ABDO vier mogelijke rubriceringen kent die overeenkomstig zijn met een TBB-categorie. Informatie die van één van de Rubriceringen is voorzien, wordt Bijzondere Informatie (BI) genoemd. Opgemerkt wordt dat in tegenstelling tot BI, een TBB niet gerubriceerd hoeft te zijn. Een gerubriceerd document is altijd een TBB, maar een TBB is niet altijd een gerubriceerd! Een voorbeeld hiervan is een wapensysteem, waar defensie er maar weinig van heeft. Desbetreffend wapensysteem is een zogenaamd commercial-off-the-shelf (COTS-) product, dus niet uniek. Maar omdat defensie er zo weinig heeft en het belangrijk is voor zijn operationele doeleinden kan het aangemerkt worden als een TBB. Het onderscheid in categorie is van belang omdat de ABDO een normkader is dat zijn eisen bepaald aan de hand van het vastgestelde TBB-categorie die door de opdrachtgever is bepaald.

2.3.2.1. Uiteenzetting van de ABDO 2019

De ABDO 2019 bestaat uit een viertal hoofdstukken die elk zijn eigen aandachtsgebied heeft. Daarnaast kent het normkader eenenveertig bijlages waar specifieke normen weer naar verwijzen. De bijlages geven veelal een begeleidend schrijven en zijn soms ook voorzien van een invulformulier.

In de opvolgende sub-paragrafen zullen de verschillende hoofdstukken doormiddel van een samenvatting beschreven worden.

Personeel en organisatie

Het eerste hoofdstuk staat in het teken van bestuur en organisatie. In dit hoofdstuk wordt beschreven dat het van belang is dat een defensieorderbedrijf een breed gedragen en structureel beveiligingsbeleid bezit dat bekrachtigd is door het hoogste bestuursorgaan (ministerie van Defensie, (2021b, mei 19, p. 10). Dit hoofdstuk richt zich dan ook voornamelijk op het maken van een beveiligingsplan, met inachtneming dat de gehele organisatie, van hoog tot laag is doordrongen van de waarde van een TBB. Daarbij zal gericht worden op de eigen bedrijfsprocessen, maar ook op dat van de resterende logistieke keten zoals eventuele (toe)leveranciers en of subcontractors. In dit hoofdstuk wordt ook meermalen verwezen naar bijlage vier van de ABDO. Hierin staat beschreven dat er een (dreigings-)analyse gemaakt dient te worden van de bestaande situatie en een inventarisatie van de reeds bestaande beveiligingsmaatregelen. Op basis van de gemaakte (dreigings-) analyse dient het bedrijf zo nodig naast de vereiste TBB-maatregelen, aanvullende maatregelen te implementeren om zodoende risico's te kunnen beheersen. Afsluitend beschrijft de bijlage dat er periodiek een evaluatie plaats dient te vinden of het beveiligingsplan nog voldoet of dat het bijgesteld moet worden.

Andere onderwerpen die aan bod komen zijn:

- Het aanstellen van een beveiligingsfunctionaris;
- Het opstellen van een beveiligingsplan;
- Het bevorderen van beveiligingsbewustzijn;
- Hoe om te gaan met media en relatie tot de bijzondere opdracht;
- Hoe om te gaan met beveiligingsincidenten.

Personeel

Hoofdstuk twee richt zich tot personele beveiliging. Het betreft maatregelen die gericht zijn op het verkrijgen van een bepaalde mate van zekerheid dat een persoon de belangen van het ministerie van Defensie niet schaadt. Ofwel, er worden betrouwbaarheidseisen gesteld aan personeel van defensie, alsmede aan het personeel in dienst van defensieorderbedrijven die uitvoering geven aan een bijzondere opdracht (ministerie van Defensie, 2021b, mei 19, p. 14). Personele beveiliging in relatie tot het kennisnemen van, werken met, produceren van of in aanraking komen met een TBB richt zich met name tot het veiligheidsonderzoek dat wordt uitgevoerd ter verkrijgen van een Verklaring Geen Bezwaar. Een Verklaring Geen Bezwaar is benodigd om aangesteld te worden als vertrouwensfunctionaris. Enkel vertrouwensfunctionarissen mogen werken aan een TBB dat aangemerkt is als een staatsgeheim. In een aantal andere gevallen kan veelal worden volstaat met een Verklaring Omtrent Gedrag (VOG), dat afgegeven wordt door het ministerie van Justitie en Veiligheid (Ministerie van Justitie en Veiligheid, Z.D.).

Andere onderwerpen die in dit hoofdstuk aan bod komen zijn:

- Geheimhoudingsverklaring;
- Ontheffing uit vertrouwensfunctie;
- Reizen naar het buitenland.

Fysiek

Het derde hoofdstuk beschrijft welke Organisatorische-, Bouwkundige-, Elektronische- en Reactieve- (OBER) maatregelen getroffen dienen te worden corresponderend aan het niveau van de TBB. Dit hoofdstuk is dan ook van toepassing wanneer er sprake is dat een TBB bij een defensieorderbedrijf op locatie belegd wordt.

Een afgewogen selectie van OBER maatregelen moet onrechtmatige toegang tot een TBB onmogelijk maken, of pogingen daartoe in elk gevalt tijdig signaleren (ministerie van Defensie, 2021b, mei 19, p. 17). Om dit te bewerkstelligen zal er bijvoorbeeld een schillenstructuur gerealiseerd moeten worden om zodoende de uitsteltijd te vergroten zodat er een tijdige interventie kan plaatsvinden. In bijlage 21 van de ABDO wordt beschreven dat geïdentificeerde risico's voor het TBB worden geclassificeerd kijkend naar het vastgestelde, geaccepteerde bewakingsrendement bijhorend bij de hoogte van het TBB. Doormiddel van een tijdspadanalyse kan inzichtelijk gemaakt worden voor welke geïdentificeerde risico's beheersmaatregelen gerealiseerd moeten worden. Voor een TBB 1 en TBB 2 is de norm dat er een positief bewakingsrendement moet zijn. Bij een TBB 3 en TBB 4 is een positief bewakingsrendement niet vereist, echter interventie dient binnen twee uur voor een TBB 3 plaats te vinden. Afsluitend beschrijft bijlage 21.1. een proces voor alarmopvolging waaraan een defensieorderbedrijf zich moet houden indien zich er een risico in relatie tot de bijzondere opdracht zich manifesteert.

Andere onderwerpen die in dit hoofdstuk aan bod komen zijn:

- Transport en verzenden (binnenland/buitenland;
- Fysieke opslag, verwerking en ontwikkeling.

Cyber

Met het onderwerp informatiebeveiliging worden de vier ABDO-hoofdstukken afgesloten. Net zoals voorgaand hoofdstuk is deze ook van toepassing wanneer een TBB bij een defensieorderbedrijf belegd wordt. Dit hoofdstuk draagt de naam cyber omdat het naast de IT-infrastructuur ook richt op het stelsel van activiteiten (o.a. bedrijfsvoering) wat met de infrastructuur mogelijk wordt gemaakt. Naast het aanstellen van een beveiligingsfunctionaris zoals genoemd in hoofdstuk één, dient er ook een cyber-beveiligingsfunctionaris aangesteld te worden. De cyber-functionaris heeft de verantwoordelijkheid om overzicht te houden op de cyberactiviteiten die uitgevoerd worden ten behoeve van het ministerie van Defensie en de maatregelen om deze te beschermen (ministerie van Defensie, 2021b, mei 19, p. 23).

Onderwerpen die aan bod komen zijn:

- Informatiebeveiligingsbeleid;
- Organiseren van Informatiebeveiliging;
- Veilig personeel;
- Beheer van bedrijfsmiddelen;
- Toegangsbeveiliging;
- Beveiliging bedrijfsvoering;
- Communicatiebeveiliging;
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen;
- Leveranciersrelaties.

3. Methode van onderzoek

In de voorgaande hoofdstukken vond de voorbereiding van dit onderzoek plaats. Er is een onderzoeksvraag met deelvragen geformuleerd en er vond een relevante verdieping plaats doormiddel van het theoretisch kader. In dit hoofdstuk worden de methoden, hulpmiddelen en technieken die voor dit onderzoek gebruikt worden nader omschreven en zodoende geborgd.

3.1 Kwalitatief onderzoek

Dit onderzoek is kwalitatief van aard. Kwalitatief onderzoek is niet gebonden aan het verzamelen van cijfermatig gegevens, er wordt geen causaal verband gezocht (Verhoeven, 2011). Kwalitatief onderzoek is voor dit onderzoek geschikt, omdat het verzamelen van gegevens open en flexibel is en er kan worden ingesprongen op onverwachte situaties (Maso & Smaling, 1998). Daarnaast geeft kwalitatief onderzoek een goed beeld van de uitvoering, ervaringen en meningen van de doelgroep, namelijk defensieorderbedrijven waarbij een bijzondere opdracht belegd is. Voor dit onderzoek betekende dit dat er op de wijze van onderzoeken zoveel mogelijk relevante informatie aangaande het toepassen van risicomanagement bij defensieorderbedrijven, vanuit de doelgroep meegenomen konden worden. De gegevens van dit onderzoek zijn niet numeriek opgemaakt, maar in alledaagse taal verwerkt (Maso & Smaling, 1998).

3.2 Onderzoeksmethoden

Er zullen verschillende kwalitatieve onderzoeksmethoden toegepast worden om de geformuleerde deelvragen en daarmee uiteindelijk de hoofdvraag te beantwoorden. Voor dit onderzoek is er gebruik gemaakt van literatuuronderzoek en interviews.

3.2.1 Literatuuronderzoek (deelvraag één)

De onderstaande deelvragenmatrix helpt om meer inzicht te verkrijgen in de onderzoeksmethodes en analyses die toegepast zijn om de deelvragen en zo uiteindelijk de hoofdvraag van dit onderzoek te beantwoorden. De deelvragenmatrix is ingevuld met de uitkomsten van iedere opvolgende paragraaf.

Deelvraag één.		
Welke risicomanagementmethode kan gebruikt worden ter ondersteuning van de ABDO?		
Onderzoeksmethoden:	Informatieverzameling:	Informatieanalyse:
- Literatuuronderzoek (secundaire literatuur) in verband met beperkte, relevante wetenschappelijke zoekresultaten.		

Tabel 11: Onderzoeksmethode deelvraag één.

Door het verrichten van literatuuronderzoek is er inzichtelijk gemaakt wat risicomanagement precies is, welke risicomanagementmethodes er zijn en uit welke bestandsdelen het precies bestaat (deelvraag één). Gezien de beperkte wetenschappelijke zoekresultaten aangaande het onderwerp van dit onderzoek (zie Bijlage twee) heeft er voornamelijk secundaire naslag plaatsgevonden. Ten einde is er op basis van een discussie gekozen welke risicomanagementmethode gebruikt kan worden ter ondersteuning van de ABDO. Volgens Verhoeven (2011) zijn er verschillende gradaties in literatuur.

Er is onderscheid te maken in drie verschillende gradaties:

- Primaire literatuur;
- Secundaire literatuur;
- Grijze literatuur.

Voor het beantwoorden van deelvraag één is er gebruik gemaakt van secundaire literatuur. Bij secundaire literatuur betreft het geen nieuw onderwerp. Het is literatuur waarin andere auteurs al over het te behandelen onderwerp gerapporteerd hebben, bijvoorbeeld op basis van nieuwe inzichten of onderzoek.

3.2.2 Literatuuronderzoek (deelvraag twee)

Met de uitkomsten van deelvraag één kon er worden overgegaan tot het beantwoorden van de tweede deelvraag. Om dit te kunnen doen moest er aanvullend literatuuronderzoek gepleegd worden middels het bestuderen van grijze literatuur. Grijze literatuur zijn boeken, rapporten, verslagen die niet in gangbare boekcollecties zijn opgenomen, bijvoorbeeld dissertaties die binnen een onderzoeksinstituut zijn uitgebracht, beleidsstukken bij ministeries, enzovoort (Verhoeven, 2011).

Deelvraag twee.		
Wordt er met de ABDO risicomanagement toegepast bij een defensieorderbedrijf?		
Onderzoeksmethoden:	Informatieverzameling:	Informatieanalyse:
- Literatuuronderzoek (grijze literatuur).		

Tabel 12: Onderzoeksmethode deelvraag twee.

3.2.3 Interviews (deelvraag drie)

De uitkomsten van deelvraag één en twee geven gezamenlijk input voor de voorbereiding van deelvraag drie. Deelvraag drie is beantwoord door het toepassen van interviews. Volgens Verhoeven (2011) is een interview een vraaggesprek waarin de beleving van de geïnterviewde voorop staat. Met als doel om informatie te verzamelen over een bepaald onderwerp. De interviews in dit onderzoek zijn gesprekken tussen twee personen.

Deelvraag drie.		
Hoe passen defensieorderbedrijven risicomanagement toe in de dagelijkse praktijk?		
Onderzoeksmethoden:	Informatieverzameling:	Informatieanalyse:
- Interviews (half-gestructureerde interviews).		

Tabel 13: Onderzoeksmethode deelvraag drie.

Er zijn verschillende methodes van interviewen. Voor dit onderzoek is er gebruik gemaakt van half-gestructureerde interviews. Half gestructureerde interviews geeft een onderzoeker de mogelijkheid om door te vragen waardoor er mogelijk meer en gedetailleerdere informatie naar voren kan komen. Het is gebruikelijk en daarom ook van toepassing voor dit onderzoek dat er voor dit type interview een vragen/topiclijst gebruikt wordt. Desondanks het gebruik van een lijst is er ook ruimte voor eigen inbreng van de respondent. De onderzoeker stelt zicht dan ook flexibel op en speelt in op de situatie (Verhoeven, 2011). De interviewvragen voor het beantwoorden van deelvraag drie zijn opgesteld met de resultaten van deelvraag één en twee.

Onderzoeksvraag:
Wat voor effect heeft de ABDO op het toepassen van risicomanagement bij defensieorderbedrijven waarbij een bijzondere opdracht belegd is?

Tabel 14: Onderzoeksvraag.

De resultaten van de geformuleerde deelvragen zullen gezamenlijk antwoord geven op de onderzoeksvraag van dit onderzoek.

3.3 Informatieverzameling

In de vorige paragraaf zijn de toegepaste kwalitatieve onderzoeksmethoden voor dit onderzoek behandeld. De volgende stap voor het onderzoek was om deze onderzoeksmethoden te operationaliseren.

3.3.1 Literatuuronderzoek (deelvraag één)

Deelvraag één		
Welke risicomanagementmethode kan gebruikt worden ter ondersteuning van de ABDO?		
Onderzoeksmethoden:	Informatieverzameling:	Informatieanalyse:
- Literatuuronderzoek (secundaire literatuur) in verband met beperkte, relevante wetenschappelijke zoekresultaten.	- Zie bijlage twee.	- Analyse aan de hand van zoektermen; - Analyse aan de hand van definitie risicomanagement.

Tabel 15: Informatieverzameling deelvraag één.

Zoals benoemd in paragraaf (zie 3.2.1 Literatuuronderzoek deelvraag één) is er voor de eerste deelvraag gebruik gemaakt van secundaire literatuur, dit gezien de beperkte wetenschappelijke zoekresultaten aangaande het onderwerp van dit onderzoek (zie Bijlage twee). Door het toepassen van informatieverzameling en het analyseren hiervan kan er antwoordt gegeven worden welke risicomanagementmethode gebruikt kan worden ter ondersteuning van de ABDO. Alle literatuur aangaande dit onderwerp is opgezocht via het internet, de openbare bibliotheek en in de eigen literatuurcollectie van de steller van dit onderzoek. Om de relevantie van literatuur te onderscheiden in relatie tot dit onderzoek zijn onderstaande zoektermen gebruikt.

- Risico;
- Risicomanagement;
- Risk;
- Security;
- Securitymanagement;
- Risk- securitymanagement;
- Integraal;
- Beveiliging;
- Integrale beveiliging.

De volgende stap was om alle gevonden literatuur te beoordelen op relevantie in relatie tot dit onderzoek. Dit is gedaan door gebruik te maken van de definitie van risicomanagement voor dit onderzoek. In totaliteit voldeden een tweeëntwintig aantal bronnen voor dit onderzoek. Geselecteerde bronnen zijn genummerd opgenomen in bijlage twee. Tevens zijn de geselecteerde bronnen voorzien van een onderwerp en een korte motivatie waarom ze opgenomen zijn voor dit onderzoek.

3.3.2 Literatuuronderzoek (deelvraag twee)

Deelvraag twee:		
Wordt er met de ABDO risicomanagement toegepast bij een defensieorderbedrijf?		
Onderzoeksmethoden:	Informatieverzameling:	Informatieanalyse:
- Literatuuronderzoek (grijze literatuur).	- Zie bijlage twee; - Resultaten deelvraag één; - ABDO.	- Analyse middels coderen.

Tabel 16: Informatieverzameling deelvraag twee.

Om de tweede deelvraag te kunnen beantwoorden zullen de resultaten van deelvraag één inhoudelijk vergeleken worden met de ABDO. Hierdoor kan bepaald worden of er met de ABDO daadwerkelijk risicomanagement toegepast wordt bij defensieorderbedrijven. De ABDO valt onder de categorie 'grijze literatuur'. De ABDO is een normkader dat te vinden is op de website van het ministerie van Defensie. Gezien het onderwerp van dit onderzoek is het niet noodzakelijk om de relevantie van de ABDO verder te duiden.

3.3.3. Interviews (deelvraag drie)

Deelvraag twee		
Hoe passen defensieorderbedrijven risicomanagement toe?		
Onderzoeksmethoden:	Informatieverzameling:	Informatieanalyse:
- Interviews (half-gestructureerde interviews).	- Er zijn vijf beveiligingsfunctionarissen van defensieorderbedrijven geïnterviewd. Vanwege de vertrouwelijkheid van de werkzaamheden zijn de namen van desbetreffende personen en bijhorende defensieorderbedrijven geanonimiseerd.	- Analyse interviews aan de hand van uitkomsten deelvraag één en deelvraag twee.

Tabel 17: Informatieverzameling deelvraag drie.

Om deelvraag drie te kunnen beantwoorden zijn er vijf half-gestructureerde interviews afgenomen. De vragen/topiclijst die gebruikt is bij de afname van de interviews (zie: Bijlage vier) is ingericht met de resultaten van deelvraag één en deelvraag twee. Alle interviews zijn door middel van geluidsopname opgenomen en hierna woordelijk overgenomen.

Voor dit onderzoek is er gekozen om beveiligingsfunctionarissen van midden- en groot-defensieorderbedrijven te interviewen. Volgens Rijksdienst voor Ondernemend Nederland (*Mkb-toets*, 2021) heeft een middenbedrijf maximaal 250 en een grootbedrijf 250 of meer werknemers in dienst. Verhoeven (2011) beschrijft dat er dan gesproken kan worden over een selecte steekproef. Bij een selecte steekproef worden respondenten bewust geselecteerd op basis van bepaalde eigenschappen. Defensieorderbedrijven die een bijzondere opdracht uitvoeren moeten contractueel voldoen aan de ABDO en daarmee zal er dus gedurende de gehele uitvoering van de opdracht een beveiligingsfunctionaris aanwezig zijn. Alle interviews worden gezien de vertrouwelijke aard van de bijzondere opdrachten, geanonimiseerd om herleidbaarheid naar de individu en het defensieorderbedrijf te voorkomen.

TBB-categorie:	Omvang:	Motivatie:
TBB 1.	- Groot.	Beperkt aanbod van defensieorderbedrijven die in deze TBB-categorie een opdracht uitvoeren.
TBB 2.	- Groot; - Middel.	Voldoende aanbod van defensieorderbedrijven die in deze TBB-categorie een opdracht uitvoeren.
TBB 3.	- Groot; - Middel.	Voldoende aanbod van defensieorderbedrijven die in deze TBB-categorie een opdracht uitvoeren.

Tabel 18: TBB-categorieën.

Gezien de vertrouwelijkheid en de aard van werkzaamheden (werken aan een bijzondere opdracht) kan er geen cijfermatige weergave in dit onderzoek worden opgenomen over hoeveel bedrijven voldoen aan de genoemde criteria. Defensieorderbedrijven die een bijzondere opdracht uitvoeren met opdracht aangemerkt als TBB 4 zullen buiten beschouwing gelaten worden. Dit omdat er in deze TBB-categorie geen sprake is van werken met een Staatsgeheim (Stg). Ook worden voor dit onderzoek kleine-defensieorderbedrijven buiten beschouwing gelaten omdat ze hoofdzakelijk opdrachten uitvoeren waarbij het Te Beschermen Belang de defensielocaties niet verlaten en hierbij dus niet hoeven te voldoen aan alle normen die de ABDO stelt (enkel hoofdstuk één en twee van de ABDO zijn dan van toepassing).

3.4 Betrouwbaarheid en validiteit

Voor ieder wetenschappelijk onderzoek is het van belang dat de betrouwbaarheid en kwaliteit geborgd is. De kwaliteit van dit onderzoek is dan ook te beoordelen aan de hand van betrouwbaarheid en validiteit. Met validiteit en betrouwbaarheid is er gekeken naar de (mogelijke) fouten die voor dit onderzoek voorkomen konden worden.

Verhoeven (2011) schrijft dat er systematische fouten gemaakt kunnen worden in een onderzoek. De betrouwbaarheid van onderzoeksresultaten geeft aan in hoeverre dit onderzoek vrij is van deze fouten. Van belang is dat de betrouwbaarheid te testen is middels herhaalbaarheid van dit onderzoek. Wanneer een herhaald onderzoek tot dezelfde resultaten leidt, kan er gesproken worden over een betrouwbaar onderzoek. Met validiteit wordt er volgens Verhoeven (2011) bepaald in welke mate het onderzoek vrij is van systematische fouten. De twee belangrijkste vormen van validiteit, zijn de onderzoeksgroep en de geldigheid van de toegepaste meetinstrumenten.

3.4.1 Betrouwbaarheid

Om deelvragen één en twee te beantwoorden is er gebruik gemaakt van literatuuronderzoek. Er is gebruik gemaakt van secundaire en grijze literatuur. De secundaire bronnen ten behoeve van het beantwoorden van deelvraag één, bestaan uit openbare, gepubliceerde boeken die relevant zijn voor dit onderzoek. Desbetreffende secundaire bronnen zijn geselecteerd door gebruik van geformuleerde zoektermen (zie 3.3.1). Om deelvraag twee te beantwoorden is er gebruik gemaakt van de ABDO, een normenkader dat ontwikkeld is door Bureau Industrieveiligheid wat ressorteert onder het ministerie van Defensie. De betrouwbaarheid is vastgesteld gezien er gebruik gemaakt wordt van een normkader dat ontwikkeld is door een overheidsorgaan.

Voor het beantwoorden van deelvraag drie zijn de interviews ingericht met de uitkomsten van deelvraag één en twee. De interviews zijn zoals beschreven (zie 3.3.3 Interviews) alleen gehouden met de beveiligingsfunctionarissen van defensieorderbedrijven waarbij een bijzondere opdracht belegd is. Er is gekozen om de interviews met de beveiligingsfunctionarissen (functie) te houden, omdat de bezetting (individu) kan wisselen.

Personalia zijn veiligheidswege geanonimiseerd. Tevens zal het anonimiseren herleidbaarheid van het defensieorderbedrijf voorkomen. Voor alle interviews is er een vragen/topiclijst gehanteerd. Een standaard vragen/topiclijst vergroot de betrouwbaarheid van het onderzoek (Swanborn, 2010).

Desondanks alle maatregelen is er gezien de aard van dit onderzoek altijd ruimte voor beïnvloeding van de respondenten. De beleving van de respondent stonden centraal in dit onderzoek. Het nadeel hiervan is dat de beleving van respondenten door mate van tijd kan veranderen of wanneer het onderzoek herhaald wordt er andere personen de functie van beveiligingsfunctionaris vervullen.

3.4.2 Validiteit

Zoals eerder benoemd is er voor dit onderzoek gebruik gemaakt van half gestructureerde interviews. Alle interviews zijn opgenomen en woordelijk overgenomen om de validiteit zodoende te borgen. Eventuele onduidelijkheden in het transcript zijn gearceerd en voorgelegd aan de geïnterviewde ter verduidelijking. Het interview is ter afsluiting, (bron)verificatie en voor een officieel akkoord voorgelegd aan de geïnterviewde.

Alle informatie die voor dit onderzoek gebruikt is, is zorgvuldig vastgelegd. Door het zorgvuldig vastleggen van gebruikte informatie is de validiteit gewaarborgd. Een andere reden voor het vastleggen van gebruikte informatie, is dat het mogelijk aan verandering onderhevig is.

Kijkend naar dit onderzoek kan sociaal wenselijkheid de gewenste mate van validiteit negatief beïnvloeden. Respondenten kunnen namelijk op interview vragen sociaal wenselijk antwoorden, dit met betrekking tot eigen of organisatiebelang.

3.5. Analyseren van data

3.5.1. Analyseren van data deelvraag één en twee

Voor dit onderzoek was een definitie van risicomanagement geformuleerd. Deze definitie is gebruikt om onderscheid te maken of literatuur relevant was voor dit onderzoek of niet. Daarnaast zijn er zoektermen gebruikt om de relevantie van de literatuur te kunnen bepalen (zie 3.3.1 Literatuuronderzoek). In bijlage twee is alle geselecteerde literatuur verwerkt in een tabel ter herleidbaarheid. In het tabel is ieder stuk genummerd, is de benaming opgenomen en is er gemotiveerd waarom het geselecteerd is voor dit onderzoek.

Om de tweede deelvraag te kunnen beantwoorden was een kwalitatieve analyse benodigd op reeds geselecteerde literatuur en de ABDO. Hiervoor is coderen toegepast. Coderen stelt een onderzoeker in staat om literatuur diepgaander te analyseren (Verhoeven, 2011). Met coderen worden codes toegewezen aan tekst. Verhoeven (2011) beschrijft dat er door het toepassen van coderen onderscheid gemaakt kan worden tussen verschillende categorieën. Door verschillende categorieën toe te passen kunnen resultaten overzichtelijker met elkaar vergeleken worden.

Codering: algemeen.	
Motivatie:	Door algemene vragen aangaande de ABDO en risicomanagement te coderen kan er onderscheidt gemaakt worden met de resterende coderingen die betrekking hebben tot de zes generieke risicoprocesstappen van risicogestuurd werken (Van Staveren, 2015).

Tabel 19: Codering algemeen.

Codering: doelen bepalen.	
Motivatie:	Door doelen bepalen te coderen kan er inzicht verkregen of de ABDO een defensieorderbedrijf voorziet in het bepalen van doelen met betrekking tot de uitvoering van de bijzondere opdracht.

Tabel 20: Codering doelen bepalen.

Codering: risico's identificeren.	
Motivatie:	Door het coderen van risico's identificeren wordt er inzichtelijk gemaakt of de ABDO voorziet in het identificeren van risico's.

Tabel 21: Codering risico's identificeren.

Codering: risico's classificeren.	
Motivatie:	Door risico's te classificeren te coderen wordt er inzicht verkregen of de ABDO voorziet in het classificeren van risico's.

Tabel 22: Codering risico's classificeren.

Codering: risico's beheersen.	
Motivatie:	Middels de codering risico's beheersen wordt er inzichtelijk gemaakt of de ABDO, defensieorderbedrijven in staat stelt om risico's te beheersen.

Tabel 23: Codering risico's beheersen.

Codering: risicobeheersmaatregelen evalueren.	
Motivatie:	De codering risicobeheersmaatregelen evalueren zal inzichtelijk maken of er sprake is van een controlewerking of gekozen beheersmaatregelen het beoogd effect hebben. Daarnaast zal gekeken worden naar noodzakelijkheid, aanpassingen en periodiek beoordeling (risicomonitoring).

Tabel 24: Codering risicobeheersmaatregelen evalueren.

Codering: overdracht risicodossier.	
Motivatie:	Met de codering overdracht risicodossier wordt er inzichtelijk gemaakt of een defensieorderbedrijf middels de ABDO periodiek en kritisch kijkt naar het gecreëerde risicodossier. Van belang is dat hierbij een lineair, dan wel cyclisch proces bestaat.

Tabel 25: Codering overdracht risicodossier.

Voor dit onderzoek zijn de zes bovenstaande coderingen (labels) opgesteld. Deze coderingen zijn gekozen omdat ze veelvuldig worden gebruikt in de geselecteerde literatuur aangaande de zes generieke risicoprocesstappen. De coderingen zijn gebruikt om de ABDO te vergelijken met de uitkomsten van deelvraag één (de zes generieke risicoprocesstappen). Gecodeerd literatuur is ter herleidbaarheid opgenomen in een coderingstabel (zie bijlage drie) en verwerkt in de presentatie (tabellen) van resultaten (4.2.1 Risicomanagement versus de ABDO 2019) ter beantwoording van deelvraag twee.

3.5.2. Analyseren van data deelvraag drie

Om de derde deelvraag te kunnen beantwoorden zijn er voor dit onderzoek half-gestructureerde interviews afgenomen met vijf beveiligingsfunctionarissen die werkzaam zijn bij verschillende defensieorderbedrijven die uitvoering geven aan een bijzondere opdracht. Alle interviews zijn door middel van geluidsopname opgenomen en woordelijk overgenomen. Om de afgenomen interviews te analyseren is er gebruikt gemaakt van coderen. Door het toepassen van verschillende categorieën kunnen resultaten (Verhoeven, 2011) overzichtelijker met elkaar vergeleken kunnen worden.

Voor deelvraag drie zijn dezelfde coderingen toegepast voor als deelvraag twee (zie 3.5.1. Analyseren data van deelvraag één en twee).

Coderingtabel.	
Codering:	Kleur:
Algemeen.	Roze.
Doelen bepalen.	Geel.
Risico's identificeren.	Groen.
Risico's classificeren.	Grijs.
Risico's beheersen.	Rood.
Risicobeheersmaatregelen evalueren.	Donker groen.
Overdracht risicodossier.	Paars.

Tabel 26: Coderingstabel.

De opmaak van coderen is wel anders toegepast dan bij deelvraag twee. De afgenomen interviews zijn gecodeerd door het toepassen van kleuren (zie bovenstaand coderingstabel).

Iedere codering heeft zijn eigen kleur. Afsluitend zijn er na het (kleur-)coderen samenvattingen opgemaakt per geïnterviewde gebaseerd op de gecodeerde teksten. Van ieder defensieorderbedrijf is er een samenvatting opgemaakt op basis van de gecodeerde tekst (zie 4.3 Resultaten deelvraag drie). De volledige, gecodeerde transcripties van de gevoerde gesprekken zijn opgenomen in bijlage vijf van dit onderzoek.

4. Resultaten

In dit hoofdstuk worden de onderzoeksresultaten per deelvraag gepresenteerd. De totstandkoming van de onderzoeksresultaten voor deelvraag één komen voort uit een grondige selectie van literatuur waarbij voor de beantwoording voor deelvraag twee ook coderen (labelen) is toegepast. Om de derde deelvraag te kunnen beantwoorden is er gebruik gemaakt van interviews met een selecte steekproef. De interviews zijn getranscribeerd, vervolgens gecodeerd en samengevat om tot een resultaat te komen.

4.1 Resultaten deelvraag één

In deze paragraaf wordt er een conclusie geformuleerd aan de hand van alle geselecteerde literatuur ter beantwoording van deelvraag één. De resultaten zijn geselecteerd uit tweeëntwintig bronnen die allen voldeden aan de selectiecriteria zoals beschreven in paragraaf 3.3.1 Literatuuronderzoek (deelvraag één).

Deelvraag één:
Welke risicomanagementmethode kan gebruikt worden ter ondersteuning van de ABDO?

Tabel 26: Deelvraag één.

Zoals de verdieping laat zien vindt er een verschuiving plaats in het risicomanagement landschap. Oude management kenmerken zoals één leidende methode, één doel en enkel een lineair proces volstaan niet meer en worden ingehaald door de dagelijkse realiteit. Vernieuwende kenmerken zijn dan ook steeds meer zichtbaar wanneer er gekeken wordt naar de Nederlandse defensie-industrie. Bureau Industrieveiligheid herkend dat risicomanagementmethoden het behalen van de beoogde doelen moet ondersteunen, daarbij maakt het niet uit welke of meerdere methoden er toegepast worden. Immers het behalen van de doelen is leidend, niet de achterliggende methode. De opdrachtgever van een bijzondere opdracht wilt gewoon het beoogde resultaat. Een andere verouderd kenmerk is dat waarde dominant is. Met conventioneel risicomanagement werd waarde veelal in geld uitgedrukt. Maar dit past bijvoorbeeld niet in de situatie wanneer er gesproken wordt over een Te Beschermen Belang. De waarde van een Te Beschermen Belang kan bijvoorbeeld ook gaan om exclusiviteit en hiermee een beoogd inzettingsvermogen. De geldelijke waarde doet er in zo'n situatie niet toe. Kortom, een kenmerk zoals de dominante waarde van geld is dan ook verouderd.

Risicomanagementmethoden bestaan al langere tijd en zijn daarom dan ook veelal conventioneel van aard. Ze zijn veelal gestoeld op oude kenmerken die conventionele managementmethoden typeren. COSO-ERM, ISO 31000 en RISMAN zijn 'oude' veel toegepaste en bekende conventionele risicomanagementmethoden. Alle drie de methoden leggen de nadruk op systemen, planning, controle en beheersbaarheid. COSO-ERM en ISO 31000 zijn hoofdzakelijk lineair van aard en de uitvoering vindt voornamelijk plaats op strategisch niveau. RISMAN onderscheidt zich met een cyclische uitvoering, de zogenaamde RISMAN-cyclus. Naast voorgenoemde, gebruiken de drie methodes afzonderlijk, verschillende vergelijkbare stappen om tot een risicomanagementproces te komen.

De laatste methode in de verdieping laat zien dat het ook anders kan. De methode risicogestuurd werken sluit wel aan bij de vernieuwende kenmerken die Bureau Industrieveiligheid herkend en ziet tijdens de uitvoering van een bijzondere opdracht in de dagelijkse praktijk. Een Te Beschermen Belang wordt beoordeelt op exclusiviteit en niet op basis van zijn geldelijke waarde. Ook worden bijvoorbeeld fouten vroegtijdig opgemerkt, omdat dit actief op basis van risico gestuurd werken dagelijks besproken wordt. Risicogestuurd werken brengt dan ook eenieder en alles tot elkaar.

Risicogestuurd werken kent verschillende voorwaarden (criteria) aan de methode om risicogestuurd te kunnen werken. De methode moet beschikbaar, toegankelijk en gebruiksvriendelijk zijn en voordeel opleveren voor de beoogde gebruikers. Daarnaast is het van belang dat de methode naadloos aansluit op de werkprocessen en de kosten van dit alles acceptabel zijn (van Staveren, 2015, p. 153). Kijkende naar het beschreven criterium, is risicogestuurd werken uitermate geschikt voor defensieorderbedrijven. Defensieorderbedrijven willen geld genereren door hun contractuele verplichtingen aangaande de bijzondere opdracht na te komen. Veranderen naar een vastgestelde risicomanagementmethode is hierbij niet van belang. Dit is geen probleem om risicogestuurd te kunnen werken. Risicogestuurd werken wordt niet gedefinieerd door de methode, maar door zich te richten op de juiste accenten ervan.

Risicogestuurd werken filtert de verschillende risicomanagementstappen van de drie genoemde methodes en komt tot zes generieke processtappen die voor eenieder te gebruiken zijn. De filtering laat ook zien dat de stappen van de verschillende methodes niet veel van elkaar verschillen.

De gefilterde stappen van risicogestuurd werken leggen de nadruk op mensen die dagelijks in aanraking komen met risico's die de doelstellingen van de organisatie kunnen raken. Door risicogestuurd te werken blijft risicomanagement niet enkel een gedocumenteerd en een strategisch gegeven, maar worden risico's daadwerkelijk bewust, gestructureerd aangepakt door risico-eigenaren op hun eigen niveau. Risicogestuurd werken is dan ook gebaseerd op variatie, het durven maken van keuzes en het uitnodigen in plaats van afdwingen van dialoog.

Bij defensieorderbedrijven worden bijzondere opdrachten ook uitgevoerd binnen ieder niveau. Niet alleen strategisch, maar ook tactisch en operationeel personeel zal in meer of mindere mate betrokken worden bij de uitvoering van de bijzondere opdracht. Dit betekent ook dat ze in meer of in mindere mate toegang of inzicht krijgen tot een Te Beschermen Belang. Het is dan ook begrijpelijk dat iedere medewerker geconfronteerd zal worden met zijn eigen risico's in relatie tot de uitvoering van zijn werkzaamheden aan de bijzondere opdracht.

Zoals voorgaande tekst laat zien, sluiten de kenmerken van vernieuwend management meer aan bij de uitvoering van een bijzondere opdracht door defensieorderbedrijven, met daarbij de ondersteuning van Bureau Industrieveiligheid en de ABDO. Daarnaast zijn de beschreven zes generieke risicomanagementstappen hanteerbaar voor iedereen. Gezamenlijk maakt dit dan ook de reden dat voor dit onderzoek de voorkeur niet uitgaat naar conventioneel risicomanagement ter ondersteuning van de ABDO, maar naar het 'nieuwe' risicogestuurd werken en daarmee de zes generieke risicomanagementprocesstappen. Gezien de geformuleerde hoofdvraag van dit onderzoek zullen alleen de zes generieke risicomanagementprocesstappen van risicogestuurd werken, ondersteunend gebruikt worden ter beantwoording van deelvraag twee. De overige elementen van risicogestuurd werken die in dit onderzoek beschreven zijn zullen buiten beschouwing gelaten worden.

4.2 Resultaten deelvraag twee

Deelvraag twee:
Wordt er met de ABDO risicomanagement toegepast bij een defensieorderbedrijf?

Tabel 27: Deelvraag twee.

In het theoretisch kader van dit onderzoek vonden er verdiepingen plaats betreffende de onderwerpen risicomanagement, integrale beveiliging en de ABDO. Voor dit onderzoek is het begrip risicomanagement beschreven, een definitie gekozen en is er gekeken naar de ontwikkeling hiervan. Daarnaast zijn er verschillende risicomanagementmethoden geanalyseerd. Dit alles geeft inzicht dat de ABDO kenmerken bezit van risicomanagement zoals beschreven in de verdiepingen (2.2. Theoretische verdieping ten behoeve van deelvraag één) die gebruikt zijn ter beantwoording van deelvraag één.

De verdiepingen (2.3 Theoretische verdiepingen ten behoeve van deelvraag twee) ter beantwoording voor deelvraag twee laten zien dat de ABDO ook elementen kent die operationaliserend van aard zijn. Voorbeeld hiervan zijn de verschillende type Organisatorische, Bouwkundige en Elektronische (OBE) beveiligingsmaatregelen die de ABDO ook hanteert. Er is dan ook sprake van een gelaagdheid middels integrale beveiliging. Om antwoord te kunnen geven op deelvraag twee van dit onderzoek moest er een analyse plaatsvinden tussen het resultaat van deelvraag één en de verdiepingen ten behoeve van deelvraag twee.

4.2.1. Risicomanagement versus de ABDO 2019

In de opvolgende tabellen worden de gedefinieerde zes generieke risicoprocesstappen van risicogestuurd werken naast de ABDO gehouden worden om zodoende inzicht te krijgen of er met de ABDO risicomanagement toegepast wordt bij een defensieorderbedrijf. In een tabel wordt de generieke stap in kwestie benoemd (uitkomst deelvraag één) en is er geïnventariseerd (middels coderen) welke specifieke ABDO normen hieraan corresponderen. De essentie van de geselecteerde normen is gezamenlijk vastgelegd middels een verkorte analyse.

Risicomanagement en de ABDO (stap één: doelen bepalen).	
In deze stap worden relevante doelen bepaald. Desbetreffende doelen kunnen operationeel, tactisch en of strategisch van aard zijn.	
Analyse ABDO:	Bijpassende ABDO normen:
De doelen kijkende naar ABDO zijn voornamelijk operationeel van aard. Gedurende de uitvoering van een defensieopdracht dient een TBB conform vastgestelde norm (1 tot en met 4) beschermd te worden.	- 1.1.1. - 1.2.1. - 1.2.2. - 1.2.3. - 1.3.1. - 1.2.1. - 1.5.1. - 1.5.2. - 1.7.1.

Tabel 28: Doelen bepalen.

Risicomanagement en de ABDO (stap twee: risico's identificeren).	
In deze stap worden alle risico's geïdentificeerd die de voorgaande doelstellingen negatief of positief kunnen beïnvloeden. Desbetreffende risico's kunnen kwalitatief of kwantitatief inzichtelijk gemaakt worden.	
Analyse ABDO:	Bijpassende ABDO normen:
Mogelijke risico's worden geïdentificeerd door middel van een (dreigings-)analyse dat een defensieorderbedrijf zelf moet aanleveren. Hierbij wordt gekeken naar bestaande en nog te nemen beveiligingsmaatregelen om zodoende te voldoen aan normen die de ABDO stelt, uiteraard is dit met inachtneming van de hoogte en bijhorende voorgeschreven bewakingsrendement van het Te Beschermen Belang.	- 1.3.1. - 1.3.2. - 1.3.3.

Tabel 29: Risico's identificeren.

Risicomanagement en de ABDO (stap drie: risico's classificeren).	
De geïdentificeerde risico's worden in deze stap gewogen. Dit gebeurt veelal door kans x effect = risico. In deze stap is het van belang dat er goed gecommuniceerd wordt over risicoperceptie. Risicoperceptie kan (vaak) een onbewuste rol spelen bij het (on)juist classificeren van risico's.	
ABDO:	Bijpassende ABDO normen:

Een risico wordt gedefinieerd als het product van de kans dat een dreiging zich daadwerkelijk manifesteert en het effect daarvan op het voorzettingsvermogen van Defensie. Kortweg: risico = kans x effect. Voor vaststelling heeft Defensie alle informatie, materieel, goederen en objecten op basis van een risicoanalyse ingedeeld in een Te Beschermen Belang (ABDO 2010, pag. 6). Aanvullende geïdentificeerde risico's die (ongewenste) invloed kunnen hebben op het Te Beschermen Belang worden geclassificeerd kijkende naar het vastgestelde vereiste bewakingsrendement, bijhorende de hoogte van het Te Beschermen Belang (ministerie van Defensie, 2021b, mei 19, p. 17).	- 1.1.1. - 1.2.2. - 1.3.1.

Tabel 30: Risico's classificeren.

Risicomanagement en de ABDO (stap vier: risico's beheersen).	
Een risico kan voorkomen, verzekerd of geaccepteerd worden. Daarnaast kan een risico ook overgedragen worden aan een andere partij. In deze stap wordt er bewust een keuze gemaakt hoe een risico gemitigeerd of toch geaccepteerd moet worden.	
ABDO:	Bijpassende ABDO normen:
Hoofdstuk twee voorziet in de screening van personeel dat betrokken is bij de uitvoering van de bijzondere opdracht. Door personeel te screenen worden er bepaalde risico's gemitigeerd. Hoofdstuk drie van de ABDO beschrijft dat er risico beheersmaatregelen aangebracht dienen te worden kijkende naar de resultaten van een tijdspadanalyse en het vereiste bewakingsrendement van het Te Beschermen Belang. De ABDO spreekt over (het mogelijk nemen van) Organisatorische-, Bouwkundige-, Elektronische- en Reactieve- (OBER) maatregelen (ministerie van Defensie, 2021b, mei 19, p. 17). Hoofdstuk drie richt zich op de OBER maatregelen. In hoofdstuk vier worden de vereiste informatiebeveiligingsmaatregelen beschreven (ministerie van Defensie, 2021b, mei 19, p. 23).	- 2.1. tot en met 2.2.4. - 3.1 tot en met 3.8.16. - 4.1. tot en met 4.11.2.

Tabel 31: Risico's beheersen.

Risicomanagement en de ABDO (stap vijf: risicobeheersmaatregelen evalueren).	
Met deze stap wordt nagegaan of de gekozen beheersmaatregelen het beoogde effect hebben. Tevens dienen gekozen maatregelen periodiek beoordeeld te worden voor noodzakelijkheid en effectiviteit. Indien gewenst of noodzakelijk, kunnen gekozen beheersmaatregelen verminderd of opgehoogd worden.	
ABDO:	Bijpassende ABDO normen:
In hoofdstuk één van de ABDO staat beschreven dat een defensieorderbedrijf dat uitvoering geeft aan een bijzondere opdracht de genomen beheersmaatregelen periodiek moet evalueren. Hierbij wordt gekeken naar effectiviteit en noodzakelijkheid.	- 1.3.1. - 1.3.2. - 1.3.3. - 1.3.4.

Tabel 32: Risicobeheersmaatregelen evalueren.

Risicomanagement en de ABDO (stap zes: overdracht risicodossier).	
De laatste stap gaat over communicatie en rapportage. Het is van belang dat er periodiek, kritisch gekeken wordt naar het gecreëerde risicodossier. Hierdoor ontstaat een lineair, dan wel cyclisch proces. Herhaling is van belang, risico's kunnen immers positief en of negatief veranderen.	
ABDO:	Bijpassende ABDO normen:
Omstandigheden en dreigingen zijn voortdurend aan wijzigingen onderhevig, de ABDO kent risicomanagement dan ook als een cyclisch proces (ministerie van Defensie, 2021b, mei 19, p. 6). Om deze reden dient een opgesteld beveiligingsplan periodiek geëvalueerd te worden (minimaal één keer per jaar). Daarnaast dient er een evaluatiemechanisme aanwezig te zijn waarmee specifieke lessen geïdentificeerd en verwerkt worden in het beveiligingsbeleid. Wanneer een bedrijf geautoriseerd is krijgt het toestemming om een Te Beschermen Belang te verwerken en of op te slaan. Het Te Beschermen Belang kan niet overgedragen worden aan een ander bedrijf. Wanneer dit wel gebeurt dient desbetreffend bedrijf eerst een ABDO autorisatie te verkrijgen en word het behandeld als een losstaande bijzondere opdracht.	- 1.2.2. - 1.3.1. - 1.3.2. - 1.3.3. - 1.3.4. - 1.3.5. - 1.3.6. - 1.9.6.

Tabel 33: Overdracht risicodossier.

De tot zover bestudeerde literatuur voor dit onderzoek heeft inzichtelijk gemaakt dat de ABDO elementen bezit van integrale beveiliging zowel als dat van risicomanagement. Het normkader is voornamelijk operationaliserend van aard. Door de resultaten van deelvraag één, de verdieping van deelvraag twee en de normen van de ABDO met elkaar te vergelijken is er inzicht verkregen in hoeverre de ABDO de zes generieke stappen van risicomanagement doorloopt. Op basis hiervan kan er geconcludeerd worden dat er risicomanagement toegepast wordt bij een defensieorderbedrijf doormiddel van de ABDO. Daarnaast is er inzichtelijk gemaakt dat de ABDO voldoet aan alle elementen waarmee van Staveren (2015) risicomanagement in zijn boek definieert.

Risicomanagement is:	
Doelgericht:	Het ABDO heeft als doel om een TBB te beschermen.
Expliciet:	Risico's worden door het toepassen van het ABDO omschreven en gewogen. Ten einde worden gevolgen voor het TBB inzichtelijk gemaakt.
Gestructureerd:	Het ABDO doorloopt middels eigen structuur alle zes de generieke stappen van risicomanagement.
Communicerend:	Door het doorlopen van het ABDO worden risico's inzichtelijk gemaakt en besproken.
Continu:	Voor iedere opdracht dient een nieuwe ABDO autorisatie afgegeven te worden. Hierdoor moeten alle stappen van het ABDO opnieuw doorlopen worden. Daarnaast moeten stappen opnieuw behandeld worden wanneer er zich een incident heeft gemanifesteerd of het dreigingsbeeld veranderd is.
Omgaan met risico's:	Door het toepassen van het ABDO moeten Bureau Industrieveiligheid en het defensieorderbedrijf in kwestie, communiceren over hoe om te gaan met alle risico's, kijkende naar het TBB. Beide partijen zijn erbij gebaat dat desbetreffende opdracht(-en) ten uitvoer worden gebracht.

Tabel 34: Risicomanagement en de ABDO.

4.3 Resultaten deelvraag drie

In deze paragraaf worden de onderzoeksresultaten van de vijf afgenomen interviews met betrekking tot deelvraag drie gepresenteerd. De resultaat-samenvattingen die gepresenteerd worden, zijn gebaseerd op de gecodeerde interviews die te vinden zijn in bijlage vijf. Om de resultaten verduidelijken is er onderscheidt gemaakt op basis van de zes generieke risicoprocesstappen van de methode risicogestuurd werken (zie 4.1 resultaten deelvraag één). De resultaten zullen per defensieorderbedrijf en codering gepresenteerd worden. Vervolgens zullen de resultaten gezamenlijk gepresenteerd worden om zodoende deelvraag drie te beantwoorden.

Deelvraag drie:
Hoe passen defensieorderbedrijven risicomanagement toe in de dagelijkse praktijk?

Tabel 35: Deelvraag drie.

4.3.1. Interview defensieorderbedrijf één

Codering: algemeen

Bedrijf één maakt deel uit van een holding, en is te beschrijven als een groot bedrijf. Het bedrijf is onder andere actief in de luchtvaart en maritieme sector. Voor de geïnterviewde is risicomanagement het in kaart brengen van risico's die er zijn, kijkende naar de grote van de kans dat een risico zich manifesteert, wat de waarde is en welke impact het uiteindelijk heeft. Het bedrijf maakt voornamelijk gebruik van risicomanagement op corporate niveau. Dit niveau voorziet in middelen zoals een risicomanagementsysteem. Daarbij maakt het bedrijf gebruik van verschillende risicomanagementmethodieken. Het is bij de geïnterviewde onbekend welke methodieken dit precies zijn. Risico's worden bewust en onbewust gemanaged. Bewust met het risicomanagementsysteem en onbewust in het dagelijks (automatische) functioneren van de medewerkers.

De geïnterviewde geeft ook aan dat de ABDO echt geschreven is vanuit een defensieorganisatie. Het was voor het bedrijf moeilijk om te inventariseren of iets beheersbaar was of niet en wat er dan eventueel aangepast moest worden. Het heeft de voorkeur dat de ABDO op een veel gebruikte standaard aangesloten wordt. Bedrijven zijn hier immers al bekend mee en hierdoor is veelal al het één en ander gerealiseerd.

Codering: doelen bepalen

Doelen worden door het bedrijf vanuit strategisch oogpunt bepaald. Daarna volgt er een vertaling naar tactisch en operationeel niveau. De doelen van bijzondere opdrachten (ABDO) worden wel geclusterd en komen niet direct voort uit de generieke strategische doelen. Strategische doelen veranderen zelden, maar tactische en operationele doelen gericht op de bijzondere opdracht doorgaans wel. Dit komt omdat de tactische en operationele doelen meer invloed en effect hebben op een bijzondere opdracht. De doelen voor de bijzondere opdrachten worden voor iedere processtap geïnventariseerd. Daarbij heeft de ABDO invloed gehad op het formuleren van de doelen. De implementatie van de ABDO kan veel impact hebben voor het gehele bedrijf. Om de opdracht rendabel te houden is er voor gekozen om de ABDO maatregelen zoveel mogelijk te beperken tot de groep die uitvoering geeft aan de bijzondere opdracht.

Codering: risico's identificeren

Binnen het bedrijf worden voorafgaand aan een opdracht, risico's geïdentificeerd door input vanuit verschillende expertise en de bijhorende afdelingen, zoals security, engineering en kwaliteit. Dit wordt gezamenlijk gebracht tot een risico-inventarisatie in het managementsysteem. Tijdens de uitvoering van een bijzondere opdracht is er altijd terugkoppeling vanuit de werkvloer.

Als er nieuwe risico's onderkend worden, wordt dit direct toegevoegd op de risico-inventarisatielijst. Risico's die niet meer valide zijn worden ook verwerkt in desbetreffende lijst. Risico identificatie is een continue doorlopend proces.

Codering: risico's classificeren

Risico's worden geclassificeerd middels een matrix met daarin opgenomen een waardering voor de kans van optreden van het risico en de mate van impact.

Codering: risico's beheersen

In het managementsysteem worden keuzes gemaakt hoe risico's beheerst gaan worden. De keuzes worden gemaakt door met elkaar in gesprek te gaan over een risico. Er wordt gezamenlijk in een gesprek gewogen of een risico beheersbaar is of niet. Ten einde zal er een actieplan komen om een risico te beperken of te mitigeren. Een risico kan ook geaccepteerd worden wanneer deze acceptabel blijkt.

Codering: risicobeheersmaatregelen evalueren

Het evalueren van risicobeheersmaatregelen is nog een aandachtspunt. Binnen het bedrijf is het wel in het proces opgenomen maar men verliest de aandacht wanneer de vorige stap (risico's beheersen) genomen is. Er vindt dan ook geen constante risicomonitoring plaats. Het bedrijf probeert dit sinds kort te ondervangen door gebruik te gaan maken van interne auditors. De interne auditors gaan toetsen of er daadwerkelijk opvolging is gegeven aan wat afgesproken is. Daarnaast zullen ze ook kijken of de gekozen beheersmaatregelen het beoogde effect hebben behaald. Het aanpassen van risicobeheersmaatregelen op basis van een evaluatie tijdens de uitvoering van een bijzondere opdracht zit nog in de beginfase. Het bedrijf moet eerst nog beginnen met de dagelijkse uitvoering een bijzondere opdracht.

Codering: overdracht risicodossier

Het bedrijf maakt gebruik van een managementsysteem. In dit systeem vindt dossieropbouw plaats. Dit geeft het bedrijf de gelegenheid om overdacht te laten plaatsvinden en historisch vastgelegde keuzes te raadplegen. Risicomanagement is bij dit bedrijf volgens geïnterviewde een cyclisch proces.

4.3.2 Interview defensieorderbedrijf twee

Codering: algemeen

Bedrijf twee is te typeren als een groot bedrijf. Het is dan ook actief over de gehele wereld en richt zich onder andere op asset management, automotive, banken, business services, financial services, consumenten & retail, infrastructuur, overheid, verzekeraars, pensioenen enzovoort. Risicomanagement is voor geïnterviewde een breed begrip. Het is een holistische manier van kijken naar wat kan. Risicomanagement heeft te maken met je bedrijfsvoering en doelen en het kan positief, maar ook negatief van aard zijn. Het bedrijf maakt gebruik van risicomanagement en bied dit ook aan als product voor derden. Intern maken ze gebruik van de 'Three Lines of Defense' model. Daarnaast zijn ze ISO 31000 gecertificeerd en wordt COSO gebruikt als risicomanagementmethodiek. Dit alles komt samen onder de afdeling Enterprise Risk Management waar ze uitvoering geven aan genoemde methodieken en daarbij de dagelijkse gerelateerde bedrijfsvoering.

De geïnterviewde geeft aan dat men moet oppassen dat de ABDO geen afvinklijst wordt. Geïnterviewde ziet voornamelijk het contact met medewerkers van Bureau Industrieveiligheid als meerwaarde. In dit contact wordt de nut en noodzaak van de ABDO en de daar bijhorende verplichtingen meer toegelicht. Dit laatste resulteert tot meer draagvlak voor de ABDO binnen het bedrijf.

Codering: doelen bepalen

Allereerst probeert het bedrijf een product en of dienst te verkopen aan een potentiële klant. Daarbij worden de wederzijdse doelen (verwachtingen) vastgelegd zonder gebruik te maken van een methodiek. Pas wanneer de opdracht gegund is gaat men kijken hoe ze de besproken doelen kunnen bereiken en zal er eventueel risicomanagement toegepast worden. Het bedrijf heeft het voornemen om dit in de toekomst integraal mee te nemen in de voorkant van het verkoopproces.

Codering: risico's identificeren

Het bedrijf gebruikt de eerder genoemde methodieken om risico's te identificeren. Afdeling Enterprise Risk Management richt zich voornamelijk op strategische en tactische risico's. Om risico's te duiden maken ze gebruik van medewerkers die verschillende expertises hebben. Het identificeren van risico's alvorens een project begint is een verplichting binnen het bedrijf.

Men kijkt hierbij naar alle risico's die betrekking kunnen hebben tot het project, enkele voorbeelden zijn; compliance, ethics en independence, finance, safety en security. Risico identificatie is een continue proces. Wanneer een project een andere invulling krijgt, kijkt men wederom of de geïdentificeerde risico's nog van toepassing zijn en of als er sprake is van nieuwe risico's. Het bedrijf maakt indien mogelijk risico's kwantitatief inzichtelijk. Het uitdrukken in waarde geeft een duidelijk beeld van de omvang van een risico. Maar toch zijn risico's voor het bedrijf niet geheel te kwantificeren. De kans van optreden van een risico wordt veelal kwalitatief uitgedrukt. Geïnterviewde ervaart dit als; 'natte vingerwerk'.

Codering: risico's classificeren

Bij het bedrijf worden risico's gesegmenteerd (per expertise) inzichtelijk gemaakt. De afdeling Enterprise Risk Management maakt gebruik van een heat map om risico's te classificeren. Daarbij wordt onderscheidt gemaakt van een laag, midden, hoog risico, de waarschijnlijkheid en impact van optreden. Mogelijk gebruiken andere afdelingen (expertises) ook 'risk appetitte' als meetinstrument.

Codering: risico's beheersen

Risico's worden voornamelijk intern beheerst. Hierbij maakt men gebruik van het 'Three Lines of Defense' model. Dit model laat medewerkers hun eigen werkzaamheden auditen. Dit model stelt men in staat om hun eigen beleid, proces en product of dienst te evalueren. Hierbij wordt genoteerd wat niet goed gegaan is en hoe dit uiteindelijk gecorrigeerd en of beheerst is. Ten einde zal dit door andere interne auditor beoordeeld worden. Voordeel van dit model is dat eenieder binnen het bedrijf actief en routinematig bezig is met zijn eigen handelen en zodoende impact heeft op de risico's die ze zelf kunnen beheersen.

Indien mogelijk heeft het de voorkeur om de opdracht op defensielocatie uit te voeren. Dit is voor het bedrijf risico verminderend (overdragen) gezien alle bijzonder informatie niet op de eigen bedrijfslocaties aanwezig zal zijn.

Codering: risicobeheersmaatregelen evalueren

Geïmplementeerde risicobeheersmaatregelen worden ieder kwartaal geëvalueerd in een kwartaalrapportage. Waar enkel grotere geïdentificeerde risico's specifiek worden geëvalueerd. Niet alle risicobeheersmaatregelen worden geëvalueerd. Het bedrijf probeert voornamelijk te voldoen aan contractuele verplichtingen (zoals de ABDO), wet- en regelgeving. Daarmee meent het bedrijf de voorgeschreven en noodzakelijke risicobeheersmaatregelen genomen te hebben. Het bedrijf kijkt niet of de geïmplementeerde maatregelen de aanleiding ervan dekt of als ze proportioneel en doelmatig zijn of waren.

Wanneer tijdens de uitvoering blijkt dat een geïmplementeerde beheersmaatregel niet volstaat, dan zal het bedrijf desbetreffende maatregelen naar boven aanscherpen. Echter zal de ABDO te allen tijde de (onder-) grenswaarde blijven die met elkaar contractueel bedongen is.

Codering: overdracht risicodossier

Het bedrijf maakt gebruik van een register voor de bijzondere opdrachten. In dit register worden alle bijzondere opdrachten opgenomen. In het register staat beschreven wat de opdracht is, welke specifieke afspraken er gemaakt zijn en hoe er invulling is gegeven aan de bijzondere opdracht. Het register geeft de mogelijkheid tot dossieropbouw en wordt daarom ook gearchiveerd. Wanneer de bijzondere opdracht eindigt wordt het register gebruikt als middel voor de eindrapportage. De eindrapportage vindt plaats tussen de business en de klant. Geïnterviewde ziet hierin heel duidelijk het cyclische Plan, Do, Check en Act proces in terug.

4.3.3 Interview defensieorderbedrijf drie

Codering: algemeen

Bedrijf drie is te beschrijven als een middelgroot bedrijf. Het bedrijf richt zich op scheepsbouw, scheepsvaart, offshore-industrie en overheden. Risicomanagement is voor geïnterviewde een allesomvattend begrip. Door risicomanagement toe te passen worden bedreigingen voor het bedrijf geïdentificeerd en vervolgens ingeschaald. De volgende stap is om eventueel maatregelen te nemen om de geclassificeerde risico's te beheersen.

Het bedrijf maakt gebruik van risicomanagement. Ze gebruiken hiervoor verschillende methodieken (SWOT-analyse, ISO27001, Kinney methode of de risicograaf). In de dagelijkse praktijk zijn ze veelvuldig bezig om risicomanagement een plaats te geven. Dit jaar zijn ze kijkend naar vorig jaar sterk vooruit gegaan in een meting van hun risicomanagementvolwassenheidsniveau. De vooruitgang is voornamelijk gemaakt in het borgen en beschrijven van procedures. Naast methodieken en procedures maakt het bedrijf ook gebruik van duidelijke tekenafspraken aangaande risicoacceptatie.

De ABDO en ABDO klanten (defensie) hebben het bedrijf aan het denken gezet over risico's. Echter had het bedrijf wel enige moeite met het implementeren van de ABDO normen. Het bedrijf ervaart dat de ABDO normen veelal geformuleerd zijn voor grotere bedrijven en dat ze hier door zwaar zijn kijkende naar de risico's die het bedrijf heeft geïdentificeerd.

Codering: doelen bepalen

Het bedrijf en zijn medewerkers formuleren hedendaags strategische, tactische en operationele doelen. In het verleden was men voornamelijk bezig met operationele doelen. Er werd niet tot weinig gekeken naar tactische en strategische doelen. Sinds enkele jaren is het bedrijf steeds meer bezig met voldoen aan normkaders, wet- en regelgeving. Dit gebeurd voornamelijk op de werkvloer en vertaald zich terug naar hogere managementstructuren. Hierdoor is het bepalen van doelen met betrekking tot risicomanagement ook steeds relevanter geworden. Er kan dan ook gesproken worden over een bottom up situatie.

Voor het bedrijf heeft de ABDO voornamelijk invloed gehad op de processen die aanwezig zijn. Het bedrijf heeft besloten om units anders in te richten om zodoende bijzondere opdrachten separaat uit te kunnen voeren. Daarnaast zijn er tactische en operationele doelen gesteld ter verbetering van risicomanagement en de dagelijkse bedrijfsvoering. Hierbij zijn de geformuleerde doelen vastgelegd.

Codering: risico's identificeren

Verschillende normkaders die het bedrijf gebruikt en wet- en regelgeving waar het bedrijf in aanraking mee komt schrijven voor dat risico's op regelmatige basis geïdentificeerd dienen te worden. Om risico's te identificeren maakt het bedrijf gebruik van een SWOT analyse. Door het doen van deze analyse krijgt het bedrijf inzicht in zijn eigen sterktes, zwaktes, kansen en bedreigingen. Risico's worden ook geïdentificeerd tijdens de uitvoering van een bijzondere opdracht. Daarnaast hanteert het bedrijf risicoklassen die corresponderen met de contractuele eisen (en geldende rubriceringen) van een opdrachtgever. Voor iedere risicoklassen zijn er mitigerende maatregelen die bijpassend zijn bij het bijhorende, vastgestelde dreigingsprofiel. Voordat men akkoord gaat met een contract kijken intern verschillende disciplines met verschillende expertises naar de opdracht. Naast dit alles krijgt het bedrijf ook risico's inzichtelijk door te praten met ketenpartners. Ook wordt het bedrijf geïnformeerd door diverse overheidspartijen wanneer er mogelijke risico's voor het bedrijf van toepassing kunnen zijn. Risico's worden indien mogelijk gekwantificeerd.

Codering: risico's classificeren

Het bedrijf maakt gebruik van wegingsmethodieken om risico's te kunnen classificeren (Kinney en de risicograaf). Deze methodieken stellen het bedrijf in staat om geïdentificeerde risico's te ordenen op urgentie en relevantie. Het bedrijf kan ook risico's classificeren op basis van gemaakte contractuele afspraken. Wanneer een opdracht gerubriceerd is (dit is altijd bij een bijzondere opdracht) dan maakt men gebruik van de aangeven rubricering en daarmee vastgestelde dreigingsprofiel. Het bedrijf heeft rubriceringen die de Nederlandse staat hanteert opgenomen in zijn eigen risicoklassen.

Codering: risico's beheersen

Het bedrijf beheerst risico's door ze te accepteren, overdragen, verzekeren of te mitigeren. Voornamelijk zet het bedrijf in het nemen van organisatorische maatregelen om risico's beheersbaar te maken. Geïdentificeerde en tevens geclassificeerde risico's worden altijd besproken wanneer een project zijn 'kick off' heeft. Op deze wijze hoopt het bedrijf dat personeel adequaat omgaat met risico's waar ze invloed kunnen hebben. Risico's worden ook steeds meer beheerst middels compliance-regelgeving en opgelegde normenkaders. Risicobeheersing is een continue proces.

Codering: risicobeheersmaatregelen evalueren

Risico's waar beheersmaatregelen voor genomen zijn worden door het gebruiken van een PDCA methode periodiek opnieuw geclassificeerd. Daarbij wordt er geïnventariseerd of het risico acceptabel is en of de geïmplementeerde beheersingsmaatregelen nog benodigd zijn of volstaan. Het bedrijf maakt gebruik van de ISO 29001 ter ondersteuning van het evaluatieproces.

Codering: overdracht risicodossier

Het bedrijf maakt voor bijzondere opdrachten gebruik van risicodossiers. Het risicodossier is gebasseerd op eisen vanuit de ISO 27001. Het bedrijf maakt nog geen gebruik van risicodossiers voor commerciële opdrachten, maar hoopt dit wel snel te realiseren om zodoende te voldoen aan de ISO27001.

Op het gebied van risicomanagement heeft het bedrijf een ontwikkeling doorgebracht. In het verleden ging men veelal lineair te werk en was er geen duidelijke overdracht. Tegenwoordig is het risicomanagementproces ingericht volgend de PDCA. De PDCA helpt het bedrijf om risicomanagement cyclisch te maken en hierdoor bewuster om te gaan met risico's.

4.3.4 Interview defensieorderbedrijf vier

Codering: algemeen

Bedrijf vier is te typeren als een midden grootbedrijf. Het is voornamelijk actief in geavanceerd design, architectuur en platform integrator voor de offshore-industrie en maritieme sector. Voor de geïnterviewde is risicomanagement niet alleen theoretisch van aard. Het kan ook zo zijn dat er een onderbuikgevoel aanwezig is waarbij men voelt dat er iets niet goed zit. Hierbij is het dan van belang dat er risicomanagement toegepast wordt door risico's inzichtelijk te maken. Waarbij risico op een gecontroleerde manier beheerst gaan worden. Risico's zijn niet alleen negatief, maar geven ook kansen. Risicomanagement is dan ook integraal onderdeel binnen de bedrijfsvoering binnen dit bedrijf. Het bedrijf meent een risicomanagementmethode te gebruiken. Risicomanagement wordt dagelijks voor opdrachten toegepast, waarbij stakeholder betrokken worden.

Geïnterviewde geeft aan dat het de voorkeur heeft om de ABDO op veel gebruikte standaarden te laten aansluiten. Bedrijven zijn hier immers al bekend mee een en hierdoor is veelal al het één en ander gerealiseerd. Dit laatste scheelt tijd en een verminderd de inspanningsverplichting voor een bedrijf.

Codering: doelen bepalen

Het bedrijf formuleert strategische, tactische en operationele doelen. Doelen in relatie tot een (ABDO) project worden gefaseerd geformuleerd en de bijhorende verantwoordelijkheden worden zover mogelijk naar beneden gedelegeerd. Iedere fase en bijhorende doelen worden dan ook vastgelegd. De ABDO heeft nog geen significante invloed gehad op het formuleren van doelen.

Codering: risico's identificeren

Het bedrijf identificeert risico's op routinematige basis met inachtneming van de geformuleerde doelen. Risico's worden op basis van gesprekken en op basis van vergaderingen geïdentificeerd. Deze vergaderingen vinden op wekelijkse basis plaats waarbij gekeken wordt naar alle soorten disciplines (bijvoorbeeld; security, financiën of algemene zaken). Omdat projecten (en dus ook bijzondere opdrachten) bewegen worden risico's ook tijdens de uitvoering terugkerend, opnieuw geïdentificeerd. Het bedrijf maakt risico's voornamelijk kwalitatief inzichtelijk.

Codering: risico's classificeren

Risico's worden zelfstandig door een medewerker geclassificeerd middels een matrix met daarin opgenomen een waardering voor de kans van optreden van het risico en de mate van impact. De uitkomsten hiervan worden intern besproken. Zwaarwegende risico's worden tijdens vergaderingen besproken.

Codering: risico's beheersen

Risico's worden beheerst door met elkaar in gesprek te gaan tijdens vergaderingen zoals project control. Men maakt hier een keuze wat ze met een risico gaan doen. Afsluitend worden de risico's en de genomen keuzes vastgelegd in een progress report.

Codering: risicobeheersmaatregelen evalueren

Er wordt routinematig besproken of de gekozen risicobeheersmaatregelen het beoogde effect hebben behaald. De gekozen risicobeheersmaatregelen worden niet kwantitatief inzichtelijk gemaakt.

Indien noodzakelijk worden tijdens de uitvoering van een bijzondere opdracht risicobeheersmaatregelen aangepast. Echter geniet het de voorkeur om alles goed te ingeregeld te hebben voordat er uitvoering gegeven wordt aan een opdracht.

Codering: overdracht risicodossier

Het bedrijf maakt gebruik van een quality assurance systeem. In dit systeem wordt alles gedocumenteerd. Voordat een opdracht begint zal afdeling sales alle voorwaarden en initiële risico's van de aanbieding bespreken met het projectmanagement team. Wanneer een project ten einde is kan dit systeem altijd geraadpleegd worden om zodoende opgedane ervaringen met elkaar te bespreken.

4.3.5 Interview defensieorderbedrijf vijf

Codering: algemeen

Dit bedrijf is te beschrijven als een middelgroot bedrijf. Het bedrijf is actief in industrieën zoals defensie, maritiem, industrieel en civiele architectuur. Risicomanagement is voor de geïnterviewde het beheersen van risico's of van de continuïteit van activiteiten van het bedrijf. Het bedrijf meent gebruik te maken van risicomanagement, echter gebruikt het hiervoor geen methodiek. In de dagelijkse praktijk is risicomanagement voor dit bedrijf een terugkerend iets wat op wekelijkse basis uitvoering aangegeven wordt.

De ABDO heeft een grote impact op het bedrijf gehad. Door de ABDO werd het bedrijf gedwongen om meer te kijken naar risico's en zijn eigen veiligheid. De ABDO heeft risico's en veiligheid helpen te verduidelijken en structureren. Voor het bedrijf is het nu duidelijk waarom ze iets doen op het gebied van risico's. De geïnterviewde geeft als advies dat de ABDO concreter opgesteld mag worden gezien het lezen en het leren begrijpen van het normenkader enorm veel werk is voor een MKB bedrijf.

Codering: doelen bepalen

Doelen worden binnen dit bedrijf voornamelijk bepaald op projectbasis. Deelproducten van het project kunnen een subdoel zijn. Voorafgaand aan een project inventariseert men of het de middelen heeft om de geformuleerde doelen te kunnen bereiken. Hiervoor wordt een zelf opgestelde actielijst gebruikt waarbij onderwerpen aan bod komen zoals budget, capaciteit en deskundigheid. De ABDO heeft geen invloed gehad op het bepalen van de doelen.

Codering: risico's identificeren

Het bedrijf kent geen vaste methode om risico's te identificeren. Wanneer men iets bedenkt of een risico ziet dan wordt dit ingebracht in een tweewekelijkse vergadering. Medewerkers zijn volgens de geïnterviewde gemotiveerd om dit te doen. Het bedrijf richt zich voornamelijk op risico identificatie met betrekking tot de bijzondere opdrachten die ze uitvoeren. Risico's worden kwalitatief inzichtelijk gemaakt.

Codering: risico's classificeren

Classificatie van risico's vindt normaliter plaats door het hebben van een gezamenlijk gesprek waarbij wordt bepaald welke risico's reëel zijn en welke niet.. Risico's voor de bijzondere opdrachten worden geclassificeerd doormiddel een matrix met daarin opgenomen een waardering voor de kans van optreden van het risico en de mate van impact.

Codering: risico's beheersen

Voor alle risico's die beheerst moeten worden, wordt een actieplan opgesteld. In dit actieplan worden acties opgenomen om een risico te beheersen.

Tevens worden er in dit actieplan momenten vastgelegd om te kijken of een risico daadwerkelijk beheerst wordt. Risico's aangaande de producten die het bedrijf levert zijn gemitigeerd met een bedrijfsaansprakelijkheid verzekering. Risico's kijkende naar de producten die het bedrijf vervaardigd, worden ondervangen door gebruikt te maken van de expertise van het personeel (bijvoorbeeld voldoende belastbaarheid) en door gebruik te maken van terugkerende kwaliteitscontroles.

Codering: risicobeheersmaatregelen evalueren

Beheersmaatregelen worden iedere twee maanden gecontroleerd of ze het beoogde effect behalen. Daarnaast worden de actielijsten (voor projecten), maandelijks gemonitord om te bepalen of beheersmaatregelen aangepast moeten worden. Het managementteam van het bedrijf acteert hier als eindverantwoordelijke en bepaald gezamenlijk of beheersmaatregelen gecontinueerd, aangepast of beëindigd moeten worden.

Codering: overdracht risicodossier

Het bedrijf hanteert een eigen variant van een risicodossier. De opgestelde risicoanalyse en actielijsten van ieder project worden periodiek geëvalueerd en opgeslagen als naslagwerk. Risicomanagement is bij dit bedrijf volgens geïnterviewde een cyclisch proces.

4.3.6 Gezamenlijke resultaten interviews defensieorderbedrijven

Defensieorderbedrijf:	Algemeen / processtap:	Resultaat (verkregen inzicht):
Eén.	Algemeen.	- Is een groot defensieorderbedrijf; - Maakt gebruik van een risicomanagementsysteem; - Maakt gebruik van risicomanagementmethodieken (onbekend welke); - Het bedrijf adviseert om de ABDO te laten aansluiten bij veel toegepaste standaarden / normenkaders.
	1.	- Formuleert doelen (strategisch, tactisch en operationeel) en kijkt daarbij naar iedere processtap / projectfasering.
	2.	- Identificeert doorlopend risico's op basis van expertise en maakt gebruik van een risico-inventarisatielijst. Risico's worden kwalitatief inzichtelijk gemaakt.
	3.	- Risico's worden geclassificeerd met een matrix (kans x effect).
	4.	- Risico's worden beheerst door met elkaar te praten om tot een actieplan te komen (accepteren, beperken of mitigeren).
	5.	- Risicobeheersmaatregelen is een actiepunt. Er vindt geen constante risicomonitoring plaats. Om dit te ondervangen gaat men gebruik maken van interne auditors.
	6.	- Er wordt een risicodossier opgemaakt in het risicomanagementsysteem. Dit systeem (en de uitvoering van risicomanagement) is ingericht als een cyclisch proces.
Twee.	Algemeen.	- Is een groot defensieorderbedrijf; - Maakt gebruik van een risicomanagementsysteem;

		- Maakt gebruik van risicomanagementmethodieken ('Three Lines of Defense' model, ISO 31000 en COSO); - Het bedrijf adviseert om de ABDO geen afvinklijstje te laten worden.
	1.	- Formuleert gezamenlijk met de klant doelen. Pas bij gunning wordt er gekeken hoe doelen van de opdracht bereikt kunnen worden. In de toekomst wilt het bedrijf dit toepassen aan de voorkant van het verkoopproces.
	2.	- Identificeert continue risico's met behulp van de expertise van medewerkers en gebruikt hiervoor de structuur van de risicomanagementmethodieken. Risico's worden kwalitatief inzichtelijk gemaakt en waar mogelijk gekwantificeerd.
	3.	- Risico's worden gesegmenteerd (per expertise) en met behulp van een heat-map geclassificeerd.
	4.	- Risico's worden beheerst het toepassen van interne controle (internal auditing) of door te kiezen voor risico overdracht (opdracht uitvoeren bij opdrachtgever).
	5.	- Vastgelegde risicobeheersmaatregelen worden periodiek geëvalueerd, daarbij word voornamelijk gekeken naar contractuele verplichtingen, wet- en regelgeving. Indien nodig worden beheersmaatregelen aangepast.
	6.	- Er wordt een register opgemaakt ter vastlegging van de opdracht, bijhorende afspraken en risico's etcetera. Het register word gebruikt voor de uiteindelijke eindrapportage. Alle stakeholders krijgen hierin inzicht. Er is dan ook sprake van een cyclisch proces.
Drie.	Algemeen:	- Is een middelgroot defensiebedrijf; - Maakt gebruik van een risicomanagementsysteem; - Maakt gebruik van risicomanagementmethodieken (ISO 27001); - ABDO normen kunnen te zwaar zijn kijkende naar de omvang van een bedrijf en de bijzondere opdracht die ze uitvoeren.
	1.	- Formuleert gezamenlijk met medewerkers strategische, tactische, operationele doelen op ieder niveau en voor elk proces.
	2.	- Risico's worden geïdentificeerd op basis van contract en bijhorende rubricering, SWOT analyses, expertise van medewerkers en informatie vanuit ketenpartners. Indien mogelijk worden risico's kwantitatief gemaakt.

	3.	- Risico's worden geclassificeerd met behulp van waarderingsmethodes (Kinney en de risicograaf). Risico's kunnen ook bepaald worden op basis van contractuele afspraken (rubricering met bijhorend dreigingsprofiel).
	4.	- Risico's worden beheerst door ze te accepteren, overdragen, verzekeren of te mitigeren. Daarnaast zijn er organisatorische maatregelen getroffen die bijdragen aan de mate van risico-eigenaarschap.
	5.	- Risico's worden periodiek geëvalueerd. Waarbij gekeken word gekeken of het risico acceptabel is en of de beheersmaatregelen (nog) benodigd zijn en of volstaan.
	6.	- Maakt gebruik van een risicodossier voor bijzondere opdrachten. Er worden nog geen risicodossiers opgemaakt voor commerciële opdrachten. Het risicodossier is ingericht conform ISO 27001 en is daarmee een cyclisch proces.
Vier.	Algemeen.	- Is een middelgroot defensieorderbedrijf; - Maakt gebruik van een quality assurance systeem; - Maakt gebruik van een risicomanagementmethode; - Het bedrijf adviseert om de ABDO te laten aansluiten bij veel toegepaste standaarden / normenkaders.
	1.	- Formuleert strategische, tactische, operationele doelen voor iedere projectfase, proces en bijhorend niveau. De ABDO heeft geen significante invloed gehad op het formuleren van de doelen.
	2.	- Risico's worden geïdentificeerd met inachtneming van de vastgestelde doelen. Dit gebeurd op basis expertise van medewerkers tijdens periodieke vergaderingen. Risico's voor bijzondere opdrachten (projecten) worden hierdoor doorlopend geïdentificeerd. Risico's worden veelal niet gekwantificeerd.
	3.	- Risico's worden geclassificeerd met een matrix (kans x effect). Zwaarwegende risico's worden tijdens vergaderingen besproken.
	4.	- Risico's worden beheerst door periodiek met elkaar in gesprek te gaan. Daarbij word er afgesproken hoe een risico beheerst moet worden. Dit wordt vastgelegd in een rapportage.
	5.	- Beheersmaatregelen worden periodiek geëvalueerd op het beoogde effect en indien noodzakelijk aangepast.
	6.	- Er word een risicodossier gedocumenteerd. Dit dossier kan altijd geraadpleegd worden en word tevens gebruikt om opgedane ervaringen met elkaar te bespreken.

Vijf.	Algemeen.	- Is een middelgroot defensieorderbedrijf; - Maakt geen gebruik van een bestaand risicomanagementmethodiek.
	1.	- Er worden project doelen en subdoelen opgesteld. De ABDO heeft geen invloed gehad op het formuleren van doelen.
	2.	- Risico identificatie vind plaats door met elkaar in gesprek te gaan tijdens periodieke vergaderingen. Het bedrijf richt zich hierbij op risico's die invloed kunnen hebben op een bijzondere opdracht. Risico's worden kwalitatief inzichtelijk gemaakt.
	3.	- Risico's worden geclassificeerd door met elkaar in gesprek te gaan en met een matrix (kans x effect).
	4.	- Risico's worden beheerst middels een actieplan. Beheersmaatregelen die genomen worden zijn; verzekeren, mitigeren en terugkerende kwaliteitscontroles.
	5.	- Beheersmaatregelen worden periodiek geëvalueerd op het beoogde effect en indien noodzakelijk aangepast.
	6.	- De risicoanalyse bij aanvang van een project en de actielijsten (per risico) vormen samen een risicodossier. De elementen in dit dossier worden ieder project periodiek geëvalueerd en opgeslagen als naslagwerk Dit ondersteunt het cyclische proces.

Tabel 36: Gezamenlijke resultaten interviews defensieorderbedrijven.

Om een overzichtelijk en duidelijk beeld te geven van alle resultaten van deelvraag drie, zijn de resultaten over hoe defensieorderbedrijven risicomanagement toe passen in de dagelijkse praktijk, verwerkt in de bovenstaande tabel.

5. Conclusie en discussie

5.1 Conclusie

Het doel van dit onderzoek was om te inventariseren wat voor effect de Algemene Beveiligingseisen voor Defensieopdrachten heeft op het toepassen van risicomanagement bij een defensieorderbedrijf in de dagelijkse praktijk. Dit gaf de mogelijkheid om aanbevelingen te formuleren om de effecten van de ABDO op risicomanagement bij defensieorderbedrijven en daarmee de bescherming van onze kroonjuwelen te bevorderen.

Om de hoofdvraag te kunnen beantwoorden zijn er drie deelvragen geformuleerd. De eerste deelvraag van het onderzoek luidde: welke risicomanagementmethode kan gebruikt worden ter ondersteuning van de ABDO?. De resultaten van deze deelvraag (zie 4.1 Resultaten deelvraag één) hebben inzichtelijk gemaakt dat er bij defensieorderbedrijven een verschuiving plaatsvindt van conventioneel- naar vernieuwend management. Kijkend naar de dagelijkse uitvoering van bijzondere opdrachten door defensieorderbedrijven is deze verschuiving ook voor medewerker van Bureau Industrieveiligheid duidelijk waarneembaar. Medewerkers van defensieorderbedrijven die uitvoering geven aan een bijzondere opdracht zijn veelal in meer- of mindere mate risico eigenaar en hebben daarmee direct en of indirect invloed op een Te Beschermen Belang. De dagelijkse praktijk laat zien dat risico's besproken worden en dat daarmee fouten vroegtijdig opgemerkt worden. Risico's worden bewust, gestructureerd aangepakt op ieder niveau. Deze werkwijze typeert zich dan ook als een vernieuwde manier van risicomanagement, namelijk risicogestuurd werken.

Risicogestuurd werken filtert de stappen van conventionele risicomanagementmethodes en brengt ze terug naar zes generieke risicomanagementprocesstappen die hanteerbaar zijn voor ieder defensieorderbedrijf en medewerkers op zijn eigen niveau. Gezien de generieke aard en waarneembare verschuiving naar conventioneel- naar vernieuwend management is er voor dit onderzoek dan ook gekozen om gebruik te maken van de zes generieke risicomanagementproces stappen van risico gestuurd werken ter beantwoording van deelvraag twee.

Zoals de resultaten laten zien passen de criteria (voorwaarden) van de methode risicogestuurd werken ook bij de wensen van defensieorderbedrijven. Defensieorderbedrijven willen namelijk geld genereren en daarom zo min mogelijk geld uitgeven aan elementen zoals risicomanagement. Risicogestuurd werken voorziet hierin. De methode is beschikbaar, toegankelijk, gebruiksvriendelijk en levert voordeel op voor de gebruiker. Om risicogestuurd te gaan werken hoeft het defensieorderbedrijf geen andere risicomanagement methode te gaan gebruiken, maar het hoeft zich enkel richten op het veranderen van de accenten daarvan. De kosten om risicogestuurd te kunnen gaan werken, zullen dan ook beperkt blijven.

De tweede deelvraag van het onderzoek luidde: wordt er met de ABDO risicomanagement toegepast bij een defensieorderbedrijf?. De voorafgaande theoretische verdiepingen ter beantwoording van deelvraag twee (zie 2.3 Theoretische verdieping ten behoeve van deelvraag twee) gaven inzicht dat de ABDO elementen bezit van integrale beveiliging zowel als dat van risicomanagement. Echter beantwoorde dit nog niet de geformuleerde deelvraag. Door de resultaten van deelvraag één, de verdieping van deelvraag twee en de normen van de ABDO met elkaar te vergelijken is er inzicht verkregen dat er met de ABDO de zes generieke risicomanagementprocesstappen van risicogestuurd werken aan bod komen. Op basis van deze vergelijking kan er geconcludeerd worden dat er risicomanagement toegepast wordt bij een defensieorderbedrijf doormiddel van de ABDO.

De derde deelvraag is beantwoordt door het afnemen van interviews. De derde deelvraag van het onderzoek luidde: hoe passen defensieorderbedrijven risicomanagement toe in de dagelijkse praktijk?. Door alle resultaten te transcriberen, te coderen en te gezamenlijk te vergelijken is er inzicht verkregen dat er geen tot weinig verschil is hoe defensieorderbedrijven van verschillend formaat risicomanagement toepassen. De geïnterviewde defensieorderbedrijven trachten allen compliance te zijn aan de normen die die ABDO hun voorschrijft. Om dit te doen maken ze gebruik van verschillende risicomanagementsystemen en risicomanagementmethodieken.

De grotere defensieorderbedrijven maken hierin ondersteunend gebruik van op de markt verkrijgbare Enterprise Risk Management systemen waarbij de middelgrote defensieorderbedrijven gebruik maken van eigen ingerichte systemen gebaseerd op bestaande risicomanagementmethodieken. In de dagelijkse praktijk formuleren alle vijf de bedrijven doelen die invloed hebben op het bereiken dan wel afronden van de bijzonder opdracht(en), ofwel het project. Daarbij benoemen merendeel van de respondenten dat de ABDO geen significante invloed heeft gehad op het stellen van deze doelen. De geformuleerde doelen zijn voornamelijk gericht op het behalen van de contractuele afspraken en compliance, maar niet op risicomanagement. Risico's worden op basis van expertise, contractuele- of wettelijke afspraken en compliance (in control) zijn geïdentificeerd. Geïdentificeerde risico's worden voornamelijk kwalitatief beschreven en niet gekwantificeerd. Vervolgens worden de risico's die invloed op een bijzondere opdracht kunnen hebben geclassificeerd middels de kans maal effect berekening gebruikmakende van de risicomatrix. Soms maakt men gebruik van een ander, maar vergelijkbaar risico- waarderingsinstrument. Wanneer de risico's geclassificeerd zijn gaat men met elkaar in gesprek om keuzes te maken hoe ze beheert of geaccepteerd dienen te worden. De gekozen beheersmaatregelen worden geïmplementeerd, periodiek geëvalueerd, waar nodig aangepast en gedocumenteerd. Afsluitend worden gedocumenteerde risicodossiers bij afsluiting van een bijzondere opdracht besproken, gebruikt voor naslagwerk of ter (her)initiatie van het te doorlopen risicomanagementproces.

De hoofdvraag van dit onderzoek luidde: wat voor effect heeft de ABDO op het toepassen van risicomanagement bij defensieorderbedrijven waarbij een bijzondere opdracht belegd is?.

Door de onderzoeksresultaten van alle drie de deelvragen samen te brengen kan er geconcludeerd worden, dat de ABDO een beperkt effect heeft op het toepassen van risicomanagement bij defensieorderbedrijven waarbij een bijzondere opdracht belegd is. De selectieve steekproef laat zien dat ieder bedrijf al bezig is met risicomanagement op zijn eigen manier, gebruikmakend van verschillende risicomanagementsystemen en methodieken. In de dagelijkse praktijk passen de defensieorderbedrijven voornamelijk risicomanagement toe om te kunnen voldoen aan wet- en regelgeving en contractuele verplichtingen om zodoende hun diensten- en of producten te kunnen leveren en daarmee een positieve geldstroom te kunnen genereren. Voor defensieorderbedrijven betekend dit dat ze compleet aan de ABDO moeten voldoen, alvorens ze uitvoering willen geven aan de bijzondere opdracht. Het is dan ook zo dat om deze situatie defensieorderbedrijven ervaren dat de ABDO weinig aansluit bij gangbare en reeds bestaande standaarden- en normkaders. Het implementeren van de ABDO wordt daarom ook als arbeidsintensief en soms kostbaar ervaren. Het is dan ook de gezamenlijke wens om de ABDO meer te laten aansluiten bij standaarden- en normkaders waar defensieorderbedrijven aan moeten voldoen.

5.2 Discussie

Het doel van dit onderzoek was om meer inzicht te krijgen wat voor effect de ABDO heeft op het toepassen van risicomanagement bij defensieorderbedrijven waar een bijzondere opdracht bij belegd is. Door het stellen van drie deelvragen kon er uiteindelijk antwoordt gegeven worden op de geformuleerde hoofdvraag.

De eerste deelvraag van het onderzoek was voornamelijk theoretisch van aard en richtte zich op welke risicomanagementmethode gebruikt kan worden ter ondersteuning van de ABDO. Om antwoordt te kunnen geven op deelvraag één is er eerst een verkenning gedaan wat een risico precies is, welke soorten risico's er zijn, wat risicomanagement is en hoe dit in de jaren door ontwikkelt heeft. Dit alles heeft laten zien dat er hedendaags een verschuiving plaatsvindt van conventioneel, naar vernieuwend risicomanagement.

De beschreven conventionele risicomanagementmethoden in dit onderzoek, COSO-ERM, ISO 31000 en RISMAN laten zien dat deze methodes sterk leunen op management en daarbij voornamelijk strategisch van aard zijn. Dit laatste sluit niet aan bij de dagelijkse praktijk die de medewerkers van Bureau Industrieveiligheid zien. Als laatste werd er gekeken naar een vernieuwende risicomanagementmethodiek, namelijk risicogestuurd werken (Van Staveren, 2015). Deze methode sluit wel aan bij de dagelijkse praktijk die te zien is bij de uitvoering van een bijzondere opdracht door een defensieorderbedrijf. Daarnaast maakt deze vernieuwende methode gebruik van zes generieke risicoprocesstappen en is daarmee voor ieder defensieorderbedrijf toepasbaar. Met de tweede deelvraag werd er gekeken of er met de ABDO risicomanagement toegepast werd bij defensieorderbedrijven. Door de ABDO middels codering te vergelijken met de resultaten van deelvraag één kon er antwoordt gegeven worden op deze vraag.

De volgende stap was om inzicht te krijgen hoe defensieorderbedrijven risicomanagement toepassen in de dagelijkse praktijk. Om de validiteit te borgen zijn er half-gestructureerde interviews afgenomen met vijf defensieorderbedrijven van vastgesteld formaat. Om alle interviews hetzelfde te laten verlopen is er gebruik gemaakt vaan een topiclijst. Door gebruik te maken van een topiclijst was het mogelijk om te controleren of alle interviewvragen besproken waren. Voor dit onderzoek was dit echt noodzakelijk omdat er inzichtelijk gemaakt moest worden of alle respondenten gebruik maakte van alle generieke risicoprocesstappen van risicogestuurd werken. Daarnaast kon er met behulp van de topiclijst eenvoudiger bepaald worden wanneer er sprake was van theoretische saturatie. Tijdens de gevoerde gesprekken kwam er geen nieuwe informatie meer naar boven die een ander effect konden hebben op de resultaten van dit onderzoek. Mede om deze reden en gezien de vertrouwelijke aard van dit onderzoek zijn er verder geen andere defensieorderbedrijven benaderd. Alle afgenomen interviews zijn getranscribeerd, vervolgens gecodeerd en daarna samengevat in één tabel. Dit gaf de onderzoeker de gelegenheid om alle onderzoeksresultaten met elkaar te vergelijken.

De resultaten van het onderzoek voldoen aan de verwachtingen van de onderzoeker en de opdrachtgever. Het onderzoek laat zien dat de huidige ABDO beperkt effect heeft op dagelijkse toepassing van risicomanagement bij defensieorderbedrijven. De ABDO is voornamelijk een initiator om compliant te zijn betreffende de gemaakte contractuele afspraken. Defensieorderbedrijven maken veelal al gebruik van risicomanagementmethodieken en proberen de ABDO hierin een plaats te laten vinden. Echter laten de onderzoeksresultaten zien dat er een duidelijke aansluiting met andere standaarden- en normkaders ontbreekt. Om dit inzichtelijk te kunnen maken is mogelijk verder onderzoek noodzakelijk (zie aanbevelingen). Het zou defensieorderbedrijven wellicht helpen om de 'gab' tussen verschillende de ABDO en andere standaarden- en normkaders inzichtelijk te maken.

6. Aanbevelingen

Gebasseerd op de resultaten van dit onderzoek zijn er voor Bureau Industrieveiligheid de onderstaande aanbevelingen geformuleerd.

Uit onderzoek is naar voren gekomen dat de defensieorderbedrijven al gebruik maken van verschillende risicomanagementmethodieken. Het advies is om de generieke risicoprocesstappen van risicogestuurd werken in het nieuwe ABDO te laten opnemen zodat eenieder hetzelfde aangaande risicomanagement kan naslaan en er geen ruimte is voor eigen interpretatie;

Om dit advies tot een succes te kunnen maken is het van belang dat Bureau Industrieveiligheid en zijn medewerkers kennis nemen van het onderwerp en daarna alle defensieorderbedrijven die een bijzondere opdracht uitvoeren actief informeren middels de reeds toegepaste communicatiemethoden (ABDO en de website van Bureau Industrieveiligheid). Het voordeel hiervan is dat de huidige communicatiemethoden bekend zijn bij de beoogd ontvangers (defensieorderbedrijven en hun beveiligingsfunctionarissen). Naast een informatieve weergave, kan risicogestuurd werken, de zes generieke risicoprocesstappen, de accenten en benodigde voorwaarden als gespreksonderwerp gebruikt worden tijdens de contactmomenten die Bureau Industrieveiligheid heeft met de aangewezen beveiligingsfunctionarissen. Naast het informeren is het van belang dat defensieorderbedrijven ook handvatten aangereikt krijgen om risicogestuurd werken daadwerkelijk te kunnen implementeren.

Stap:	Beschrijving:
1.	Definieer de doelstellingen voor de implementatie én die voor de uitvoering van risicogestuurd werken in de organisatie.
2.	Stel een eenvoudig risicodossier samen, op basis van de doelstellingen van de organisatie, afdeling, en dergelijke.
3.	Werk een eenvoudige en praktische procedure uit voor de uitvoering van risicogestuurd werken.
4.	Implementeer de procedure risicogestuurd werken, met expliciet aandacht voor gedrag, taken en verantwoordelijkheden.
5.	Evalueer het risicogestuurde werkproces en beoordeel het op effectiviteit en efficiëntie, pas het waar nodig.

Tabel 37: In vijf stappen naar een implementatieplan risicogestuurd werken (Van Staveren, 2015, p. 126).

Van Staveren (2015, p. 126) hanteert een vijfstappenplan om tot een tailormade, risicogestuurd werken implementatieplan te komen. Deze stappen kunnen ook via bestaande communicatiekanalen besproken en of gepresenteerd worden.

De onderzoeksresultaten hebben ook inzichtelijk gemaakt dat het onduidelijk is hoe de ABDO overeenkomt met andere bestaande standaarden- en normkaders. Advies is om een overzicht te creëren welke ABDO normen al toegepast worden wanneer het defensieorderbedrijf al voldoet aan andere standaarden- en normkaders. Het hebben van een compleet overzicht stelt een defensieorderbedrijf in staat om de focus te leggen naar de resterende, nog te implementeren normen.

Gebasseerd op de resultaten van dit onderzoek zijn de onderstaande aanbevelingen geformuleerd voor mogelijk toekomstig onderzoek.

1. De resultaten van dit onderzoeken wijzen uit dat defensieorderbedrijven duidelijkheid willen welke ABDO normen aansluiten bij andere standaarden- en normkaders. Om hier inzicht in te verkrijgen is verder onderzoek noodzakelijk;
2. Het onderzoek wijst uit dat de ABDO voornamelijk defensieorderbedrijven beweegt om compliant te zijn vanwege de contractuele afspraken waaraan ze moeten voldoen. Met dit onderzoek is er geen inzicht verkregen wat defensieorderbedrijven beweegt om risicomanagement toe te passen zonder dat er sprake is van contractuele afspraken. Hiervoor is verder onderzoek noodzakelijk.

Bibliografie

Appelman, A. (2010). *Intergrale beveiliging: een security management systeem in 7 stappen* (1ste editie). Vakmedianet.

Blunden, T. & Thirlwell, J. (2013). *Mastering Operational Risk: A practical guide to understanding operational risk and how to manage it*. Londen: Pearson.

Broder, J. F., & Tucker, G. (2012). *Risk Analysis and the Security Survey* (4th edition). Butterworth-Heinemann.

Chartered Institute of Internal Auditors. (2022, 1 februari). *Risk management*. Institute of Internal Auditors. Geraadpleegd op 25 maart 2022, van https://www.iia.org.uk/resources/risk-management?downloadPdf=true

COSO Enterprise Risk Management – Integrated Framework, Executive Summary Framework, The Committee of Sponsering Organizations of the Treadway Commission, September 2004.

DBB DV. (2022, 8 augustus). SWR Beveiligingsautoriteit (extern). https://bs-portal.mindef.nl/sites/00123/DBB DV/Forms/AllItems/D201.aspx

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review, 16*(2), 147-166.

Dornberger, K., Oberlehner, S, & Zadrazil, N. (2014). Challenges in Implementing Enterprise Risk Management. *ACRN Journal of Finance and Risk Perspectives, 3*(3), 1-14.

Geraets, R. (2016). *Veiligheid, Security Risk en Intelligence Management in de 21e eeuw* (1ste editie). Ministerie van Defensie.

Government Finance Function. (2021, 23 augustus). *Orange Book*. GOV.UK. Geraadpleegd op 30 januari 2022, van https://www.gov.uk/government/publications/orange-book

Headquarters, Department of the Army. (2021, 9 november). *Risk Management*. Army Resilience Directorate. Geraadpleegd op 22 april 2022, van https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34181-ATP_5-19-000-WEB-1.pdf

Hopkin, P. (2018). *Fundamentals of Risk Management* (5th Revised edition). Kogan Page Ltd.

Horney, N., Pasmore, B. & O'Shea, T. (2010). Leadership agility: A business imperative for a VUCA world. *Human Resource Planning, 33*(4), 32-38

Institute of Risk Management. (z.d.). *IRM's risk management standard*. Geraadpleegd op 30 januari 2022, van https://www.theirm.org/what-we-do/what-is-enterprise-risk-management/irms-risk-management-standard/

ISO. (2017, 8 november). *ISO Guide 73:2009*. Geraadpleegd op 30 januari 2022, van https://www.iso.org/standard/44651.html

ISO. (2021, 10 december). *ISO 31000 — Risk management*. Geraadpleegd op 30 januari 2022, van https://www.iso.org/iso-31000-risk-management.html

Kenniscentrum RISMAN. (z.d.). *Het Risman-proces : risicomanagement voor infrastructuurprojecten : naar een betere beheersing van tijd, geld en kwaliteit - Rijkswaterstaat Rapportendatabank*.

Rijkwaterstaat rapportendatabank. Geraadpleegd op 30 januari 2022, van https://puc.overheid.nl/rijkswaterstaat/doc/PUC_96120_31/

Maso, I., & Smaling, A. (1998). *Kwalitatief onderzoek* (1 editie). Boom Lemma.

Ministerie van Defensie. (2021a, april 30). *Jaarverslag MIVD 2020*. Jaarverslag | Defensie.nl. Geraadpleegd op 30 januari 2022, van https://www.defensie.nl/downloads/jaarverslagen/2021/04/30/jaarverslag-2020-mivd

Ministerie van Defensie. (2021b, mei 19). *ABDO 2019*. ABDO | Defensie.nl. Geraadpleegd op 30 januari 2022, van https://www.defensie.nl/downloads/beleidsnota-s/2020/02/04/abdo-2019

Ministerie van Justitie en Veiligheid. (z.d.). *Verklaring Omtrent het Gedrag (VOG) | Justis*. Geraadpleegd op 25 maart 2022, van https://www.justis.nl/producten/verklaring-omtrent-het-gedrag-vog

Mkb-toets. (2021, 26 april). Rijksdienst voor Ondernemend Nederland. Geraadpleegd op 25 maart 2022, van https://www.rvo.nl/subsidie-en-financieringswijzer/subsidiespelregels/ministeries/ministerie-van-economische-zaken-en-klimaat/aanvraag-indienen/mkb-toets

Rijksuniversiteit Groningen, Nyenrode School of Accountancy Breukelen, NBA en PwC. (2014, oktober). *Hoeveel zijn we opgeschoten na de crisis? Tweede Nationaal Onderzoek Risicomanagement in Nederland 2014*. Kloppenburg, M (red.). https://www.nba.nl/globalassets/themas/thema-corporate-governance/nba_rapport-risicomanagement-febr15_proef.pdf

Swanborn, P. G. (2010). *Basisboek sociaal onderzoek* (5de editie). Boom Lemma.

Talbot, J., & Jakeman, M. (2009). *Security Risk Management Body of Knowledge* (1ste editie). Wiley.

TNO. (2017). *Verkenning op risicosturing in het veiligheidsdomein*. Geraadpleegd op 25 maart 2022, van https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/met-technologie-betere-terrorismebestrijding/tno-verkenning-op-risicosturing-in-het-veiligheidsdomein/

Van Dale. (z.d.). *Risico*. Geraadpleegd op 30 januari 2022, van https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/risico#.YfbU1urMK3A

Van der Waal, D. (2019). *Inleiding risicomanagement* (1ste editie). Coutinho.

Van Staveren, M. (2015). *Risicogestuurd werken in de praktijk* (3de editie). Amsterdam University Press.

Verhoeven, N. (2011). *Wat is onderzoek? : praktijkboek methoden en technieken voor het hoger onderwijs* (4de editie). Boom Lemma.

wetten.nl - Regeling - Wet op de inlichtingen- en veiligheidsdiensten 2017 - BWBR0039896. (2022, 1 januari). overheid.nl. Geraadpleegd op 30 januari 2022, van https://wetten.overheid.nl/BWBR0039896/2022-01-01

Bijlage één

Verantwoording (interne) persoonlijke communicatie.

Op 8 augustus 2022 heeft de onderzoeker oriënterende gesprekken gevoerd met vijf accountmanagers die werkzaam zijn bij Bureau Industrieveiligheid. De gesproken accountmanagers houden zich dagelijks bezighouden met de ABDO in relatie tot defensieorderbedrijven en hun bijzondere opdrachten. Gezien de vertrouwelijke aard van de gevoerde gesprekken en aanwezigheid van persoonlijke context, mening en inzichten is het niet mogelijk om de gesprekken volledig te anonimiseren voor dit onderzoek.

Het ministerie van Defensie (en daarmee Bureau Industrieveiligheid, de opdrachtgever van dit onderzoek) staat het niet toe om persoons- en functiegegevens te delen van medewerkers. Deze gegevens gezamenlijk zijn aangemerkt als staatsgeheim (DBB DV, 2022). Om conform defensie richtlijnen herleidbaarheid op individueel niveau te voorkomen is er in samenspraak met de opdrachtgever besloten om de onderzoeksresultaten met betrekking tot de persoonlijke communicatie niet te publiceren in dit onderzoek.

Persoonlijke communicatie met medewerkers Bureau Industrieveiligheid.	
Functie bij Bureau Industrieveiligheid:	Respondent:
Senior Accountmanager.	Bekend bij onderzoeker en opdrachtgever.
Senior Accountmanager.	Bekend bij onderzoeker en opdrachtgever.
Accountmanager.	Bekend bij onderzoeker en opdrachtgever.
Accountmanager.	Bekend bij onderzoeker en opdrachtgever.
Accountmanager.	Bekend bij onderzoeker en opdrachtgever.

Bijlage twee

Geselecteerd literatuur op basis van definitie risicomanagement ten behoeve van beantwoording van deelvraag één.			
Leeswijzer tabel: Alle bronnen zijn genummerd middels een bronnummer. Er is beschreven waar de specifieke bron input heeft gegeven ter verdieping voor deelvraag één. Daarnaast is er een motivering waarom een bron is gebruikt voor dit onderzoek.			
Bron: alle bronnenverwijzingen zijn opgenomen in de bibliografie van dit onderzoek.			
Bronnummer:	Bronnaam:	Onderwerp:	Motivering:
1.	ISO Guide 73.	2.2.1. Risico.	Formulering begrip risico.
2.	Institute of Risk Management.	2.2.1. Risico.	Formulering begrip risico.
3.	Orange Book from HM Treasury.	2.2.1. Risico.	Formulering begrip risico.
4.	Institute of Internal Auditors.	2.2.1. Risico.	Formulering begrip risico.
5.	Dikke van Dale.	2.2.1. Risico.	Formulering begrip risico.
6.	Risicogestuurd werken in de praktijk.	2.2.1. Risico.	Formulering begrip risico.
7.	Risk analysis and the security survey.	2.2.1. Risico.	Formulering begrip risico.
8.	Veiligheid, Security en Intelligence Management in de 21e eeuw.	2.2.1. Risico.	Formulering begrip risico.
9.	Ministerie van Defensie, ABDO 2019.	2.2.1. Risico.	Formulering begrip risico.
10.	United States Army.	2.2.1. Risico.	Formulering begrip risico.
6.	Risicogestuurd werken in de praktijk.	2.2.2. Soorten risico's.	Verdieping soorten risico's.
11.	Mastering Operational Risk: A practical guide to understanding operational risk and how to manage it.	2.2.2. Soorten risico's.	Verdieping soorten risico's.
12.	Inleiding risicomanagement.	2.2.2. Soorten risico's.	Verdieping soorten risico's.
13.	Security Risk Management Body of Knowledge.	2.2.2. Soorten risico's.	Verdieping soorten risico's.
5.	Dikke van Dale.	2.2.3. Risicomanagement.	Formulering begrip risicomanagement.
14.	Fundamentals of Risk Management.	2.2.3. Risicomanagement.	Formulering begrip risicomanagement.

6.	Risicogestuurd werken in de praktijk.	2.2.3. Risicomanagement.	Formulering begrip risicomanagement.
15.	Risk management: History, definition and critique.	2.2.4 Risicomanagement in ontwikkeling.	Verdieping risicomanagement.
12.	Inleiding risicomanagement.	2.2.4 Risicomanagement in ontwikkeling.	Verdieping risicomanagement.
6.	Risicogestuurd werken in de praktijk.	2.2.4 Risicomanagement in ontwikkeling.	Verdieping risicomanagement.
16.	Challenges in Implementing Enterprise Risk Management.	2.2.4 Risicomanagement in ontwikkeling.	Verdieping risicomanagement.
17.	Tweede Nationaal Onderzoek Risicomanagement.	2.2.4 Risicomanagement in ontwikkeling.	Verdieping risicomanagement.
18.	Leadership agility: A business imperative for a VUCA world.	2.2.4 Risicomanagement in ontwikkeling.	Verdieping risicomanagement.
19.	TNO. Sturen op risico's.	2.2.4 Risicomanagement in ontwikkeling.	Verdieping risicomanagement.
20.	COSO-ERM.	2.2.5.1. Risicomanagementmethoden.	Verdieping methoden.
21.	ISO 31000.	2.2.5.2. Risicomanagementmethoden.	Verdieping methoden.
22.	RISMAN.	2.2.5.3. Risicomanagementmethoden.	Verdieping methoden.
6.	Risicogestuurd werken in de praktijk.	2.2.5.4. Risicogestuurd werken.	Verdieping methoden.

Bijlage drie

Coderingstabel ten behoeve van selecteren relevante ABDO 2019 normen ten aanzien van generieke risicoprocesstappen door middel van coderen.		
Leeswijzer tabel: Afzonderlijke normen zijn voluit beschreven. Wanneer alle normen van een paragraaf van toepassing zijn is enkel de naamgeving opgenomen.		
Bron: Ministerie van Defensie. (2021b, mei 19).		
Codering:	Norm:	Tekst / onderwerp van norm:
Doelen bepalen.	1.1.1.	Opdrachtnemer voldoet aan de eisen van de ABDO 2019 aangaande de gerelateerde gerubriceerde opdracht.
	1.2.1.	Opdrachtnemer beschikt over een integraal beveiligingsbeleid, waarin ook de organisatorische-, personele-, (waar nodig) fysieke- en informatiebeveiligingsaspecten in relatie tot het TBB zijn beschreven en is tevens bekrachtigd door het hoogste bestuursorgaan van de opdrachtnemer.
	1.2.2.	Opdrachtnemer beschikt over een beveiligingsplan, opgesteld door de BF, goedgekeurd door BIV en ondertekend door het hoogste bestuursorgaan van de opdrachtnemer, waarin een actuele beschrijving van de beveiligingssituatie (op basis van zelfinspectie) is opgenomen en de beveiligingseisen uit de ABDO zijn uitgewerkt in duidelijke, hanteerbare maatregelen en procedures.
	1.2.3.	Opdrachtnemer heeft de in het beveiligingsplan beschreven maatregelen en procedures eenduidig geïmplementeerd in de organisatie.
	1.3.1.	De beveiligingsfunctionaris is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert periodiek, doch minstens eenmaal per jaar een zelfinspectie uit. De resultaten zijn schriftelijk vastgelegd en gerapporteerd aan het bestuur van de opdrachtnemer.
	1.5.1.	Opdrachtnemer voert een programma uit ter bevordering van het beveiligingsbewustzijn waarbij deelname verplicht en meetbaar is.
	1.5.2.	De BF geeft voorlichting aan medewerkers die werken aan een bijzondere opdracht, aangaande ABDO 2019 procedures en de bijbehorende verantwoordelijkheden, bij aanstelling op een vertrouwensfunctie, bij de start van een nieuwe bijzondere opdracht en vervolgens periodiek, doch tenminste eenmaal per jaar.
	1.7.1.	Opdrachtnemer meldt voorgenomen uitbesteding van werkzaamheden in het kader van een bijzondere opdracht aan binnen- of buitenlandse subcontractor(s) vooraf aan BIV. BIV neemt hier een besluit over en verleent waar mogelijk toestemming.
Risico's identificeren.	1.3.1.	De beveiligingsfunctionaris is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert periodiek, doch minstens eenmaal per jaar een zelfinspectie uit. De resultaten zijn schriftelijk vastgelegd en gerapporteerd aan het bestuur van de opdrachtnemer.
	1.3.2.	De beveiligingsfunctionaris toetst periodiek, doch minimaal eenmaal per jaar, het beveiligingsplan aan de praktijk. De resultaten hiervan zijn schriftelijk vastgelegd en aan het bestuur, in afschrift aan BIV, gerapporteerd. Zo nodig wordt het beveiligingsplan geactualiseerd.
	1.3.3.	(Beleids)wijzigingen die impact hebben op het security beleid van het bedrijf zijn aan BIV ter beoordeling verstrekt en zijn verwerkt in het beveiligingsplan.

Risico's classificeren.	1.1.1.	Opdrachtnemer voldoet aan de eisen van de ABDO 2019 aangaande de gerelateerde gerubriceerde opdracht.
	1.2.2.	Opdrachtnemer beschikt over een beveiligingsplan, opgesteld door de BF, goedgekeurd door BIV en ondertekend door het hoogste bestuursorgaan van de opdrachtnemer, waarin een actuele beschrijving van de beveiligingssituatie (op basis van zelfinspectie) is opgenomen en de beveiligingseisen uit de ABDO zijn uitgewerkt in duidelijke, hanteerbare maatregelen en procedures.
	1.3.1.	De beveiligingsfunctionaris is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert periodiek, doch minstens eenmaal per jaar een zelfinspectie uit. De resultaten zijn schriftelijk vastgelegd en gerapporteerd aan het bestuur van de opdrachtnemer.
Risico's beheersen.	2.1. (geheel)	Het veiligheidsonderzoek, Verklaring Geen Bezwaar (VGB) en Verklaring Omtrent Gedrag (VOG).
	2.2. (geheel)	Geheimhoudingsverklaring.
	2.3. (geheel)	Ontheffing uit vertrouwensfunctie.
	2.4.1.	Een vertrouwensfunctionaris heeft een voorgenomen reis naar het buitenland in het kader van een bijzondere opdracht onverwijld gemeld aan de BF.
	2.4.2.	Een vertrouwensfunctionaris heeft een voorgenomen reis naar een risicoland onverwijld gemeld aan de BF.
	2.4.3.	Indien bij een zakelijke reis een request for visit (RfV) benodigd is, dient de vertrouwensfunctionaris, via de beveiligingsfunctionaris een RfV ter goedkeuring in bij BIV. Zonder goedgekeurd RfV kan de reis niet plaatsvinden.
	2.4.4.	De beveiligingsfunctionaris brieft en debrieft vertrouwensfunctionarissen die voorgenomen reizen naar risicolanden aan de beveiligingsfunctionaris hebben gemeld.
	3.1. (geheel)	Organisatorische maatregelen.
	3.2. (geheel)	Bouwkundige maatregelen.
	3.3. (geheel)	Elektronische maatregelen.
	3.4. (geheel)	Reactieve maatregelen.
	3.5. (geheel)	Transport en verzenden.
	3.6. (geheel)	Transport en verzenden binnenland.
	3.7. (geheel)	Transport en verzenden buitenland.
	3.8 (geheel)	Fysieke opslag, verwerking en ontwikkeling.
	4.1. (geheel)	Informatiebeveiligingsbeleid.
	4.2 (geheel)	Organiseren van informatiebeveiliging.
	4.3. (geheel)	Veilig personeel.

	4.4. (geheel)	Beheer van bedrijfsmiddelen.
	4.5. (geheel	Toegangsbeveiliging.
	4.6. (geheel)	Cryptografie.
	4.7. (geheel)	Fysieke beveiliging en beveiliging van de omgeving.
	4.8. (geheel)	Beveiliging bedrijfsvoering.
	4.9. (geheel)	Communicatiebeveiliging.
	4.10. (geheel)	Acquisitie, ontwikkeling en onderhoud van informatiesystemen.
	4.11. (geheel)	Leveranciersrelaties.
Risicobeheersmaatregelen evalueren.	1.3.1.	De beveiligingsfunctionaris is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert periodiek, doch minstens eenmaal per jaar een zelfinspectie uit. De resultaten zijn schriftelijk vastgelegd en gerapporteerd aan het bestuur van de opdrachtnemer.
	1.3.2.	De beveiligingsfunctionaris toetst periodiek, doch minimaal eenmaal per jaar, het beveiligingsplan aan de praktijk. De resultaten hiervan zijn schriftelijk vastgelegd en aan het bestuur, in afschrift aan BIV, gerapporteerd. Zo nodig wordt het beveiligingsplan geactualiseerd.
	1.3.3.	(Beleids-)wijzigingen die impact hebben op het security beleid van het bedrijf zijn aan BIV ter beoordeling verstrekt en zijn verwerkt in het beveiligingsplan.
	1.3.4.	Noodzakelijke wijzigingen n.a.v. een verhoogd dreigingsbeeld of een beveiligingsincident, zijn vastgelegd in het beveiligingsplan binnen de door BIV gestelde termijn.
Overdracht risicodossier.	1.2.2.	Opdrachtnemer beschikt over een beveiligingsplan, opgesteld door de BF, goedgekeurd door BIV en ondertekend door het hoogste bestuursorgaan van de opdrachtnemer, waar in een actuele beschrijving van de beveiligingssituatie (op basis van zelfinspectie) is opgenomen en de beveiligingseisen uit de ABDO zijn uitgewerkt in duidelijke, hanteerbare maatregelen en procedures.
	1.3.1.	De beveiligingsfunctionaris is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert periodiek, doch minstens eenmaal per jaar een zelfinspectie uit. De resultaten zijn schriftelijk vastgelegd en gerapporteerd aan het bestuur van de opdrachtnemer.
	1.3.2.	De beveiligingsfunctionaris toetst periodiek, doch minimaal eenmaal per jaar, het beveiligingsplan aan de praktijk. De resultaten hiervan zijn schriftelijk vastgelegd en aan het bestuur, in afschrift aan BIV, gerapporteerd. Zo nodig wordt het beveiligingsplan geactualiseerd.
	1.3.3.	(Beleids-)wijzigingen die impact hebben op het security beleid van het bedrijf zijn aan BIV ter beoordeling verstrekt en zijn verwerkt in het beveiligingsplan.
	1.3.4.	Noodzakelijke wijzigingen n.a.v. een verhoogd dreigingsbeeld of een beveiligingsincident, zijn vastgelegd in het beveiligingsplan binnen de door BIV gestelde termijn.
	1.3.5.	De BF draagt zorg voor volledige medewerking bij controles, audits en onderzoeken bij Opdrachtnemer door BIV/MIVD.

	1.3.6.	De BF stelt zich door middel van het onderhouden van contacten met de gemeente, omliggende bedrijven en de politie op de hoogte van zaken die de lokale beveiliging aangaan.
	1.9.6.	Er is een evaluatiemechanisme gedefinieerd waarmee men specifieke lessen (lessons learned) identificeert en deze verwerkt in het beveiligingsbeleid.

Bijlage vier

Interview-topiclijst risicomanagement	
Interviewer:	X
Functie:	Student.
Respondent:	X
Functie:	Beveiligingsfunctionaris.

Voorstellen en afspraken interview.

Voorstellen:
X, werkzaam bij ministerie van Defensie en tevens student Master Risicomanagement op de Universiteit Twente.

Doel van onderzoek:
Inzicht krijgen hoe een defensieorderbedrijf risicomanagement toepast in de dagelijkse praktijk.

Afspraken interview:
Het afgenomen interview zal enkel gebruikt worden bij akkoord respondent. Het interview zal middels een geluidopname worden opgenomen. Hierna zal een transcriptie gemaakt worden door interviewer. Om herleidbaarheid te voorkomen zullen alle interviewgegevens (geluidsopname en de transcriptie) geanonimiseerd worden.

Algemeen.

- Wat is volgens u risicomanagement?
- Maakt uw bedrijf gebruik van risicomanagement?
- Maakt u gebruik van een risicomanagementmethode?
- Op welke wijze gebruikt u risicomanagement in de dagelijkse praktijk?

Stap één: Doelen bepalen.

- Worden er strategische, tactische of operationele doelen bepaald kijkende naar de bijzondere opdracht?
- Worden er doelen gesteld voor iedere processtap?
- Heeft de ABDO invloed gehad het formuleren van de doelen?

Stap twee: Risico's identificeren.

- Hoe worden risico's geïdentificeerd?
- Welke risico's worden er allemaal inzichtelijk gemaakt?
- Worden risico's kwalitatief of kwantitatief inzichtelijk gemaakt?
- Worden er ook risico's geïdentificeerd tijdens de uitvoering van de bijzondere opdracht?

Stap drie: Risico's classificeren.

- Op welke wijze worden de risico's geclassificeerd?

Stap vier: Risico's beheersen.

- Op welke wijze worden risico's beheerst?

Stap vijf: Risicobeheersmaatregelen evalueren.

- Vindt er monitoring plaats of de gekozen beheersmaatregelen het gewenste effect hebben?
- Worden risicobeheersmaatregelen periodiek geëvalueerd?

- Worden risicobeheersmaatregelen tijdens de uitvoering van een bijzondere opdracht aangepast?

Stap zes: Overdracht risicodossier.

- Maakt u gebruik van een risicodossier? Zo ja, op welke manier vult u dit in? Zo nee, hoe verwerkt u de gegevens voor de risico's voor eventuele naslagwerk?
- Is risicomanagement bij uw bedrijf een lineair en cyclisch proces?

Afsluiting.

- In hoeverre heeft de bijzondere opdracht en daarmee de ABDO invloed gehad op risicomanagement bij uw bedrijf?
- Heeft feedback aangaande de ABDO in relatie tot risicomanagement?
- Hoe vond u het interview?

Bijlage vijf

Vanwege de vertrouwelijke aard van de transcripties zijn deze niet opgenomen in dit document. Bijlage vijf is eventueel verkrijgbaar via de onderzoeker.