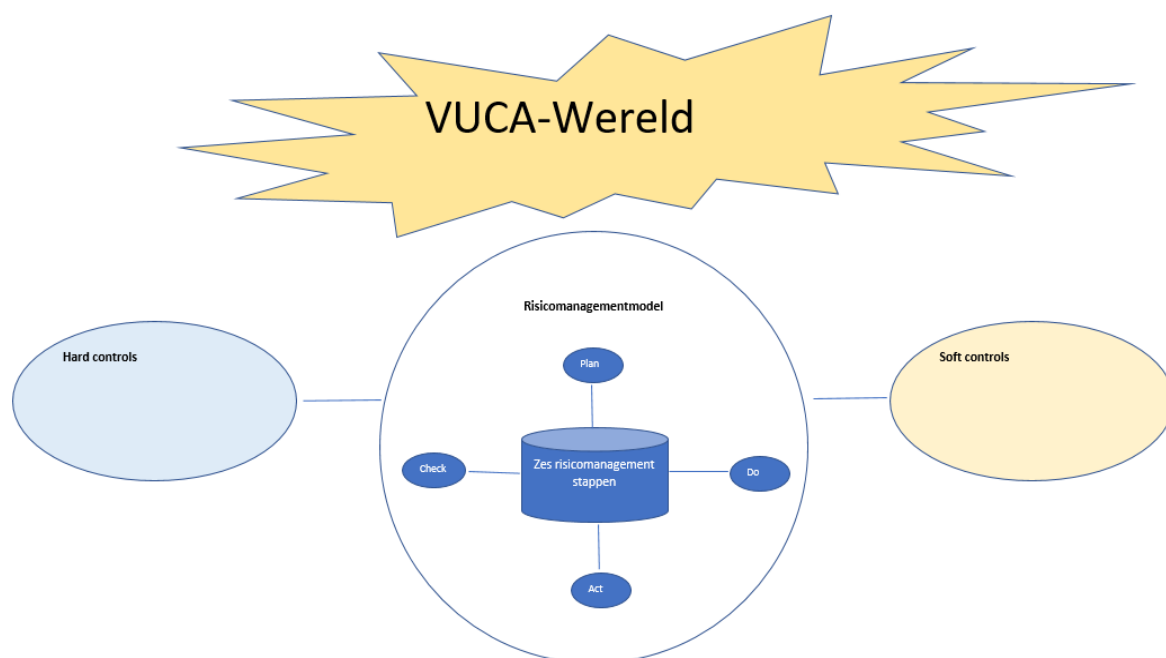




Een risicomanagement methodiek voor integrale beveiliging





Onderwijsinstelling	Uitgevoerd voor: Universiteit Twente Adres: Drienerlolaan 5 7522 NB Enschede 053 489 9111 info@utwente.nl 1e begeleider: prof. dr. Maria- Euginia. Lacob (hoogleraar Industrial Engineering en Business Information Systems) 2e begeleider: Prof. dr. ir. Petra C. de Weerd-Nederhof (hoogleraar Organisatiekunde)
Opdrachtgever	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het BVA-beraad
Gegevens afstudeerder	Titel: Een risicomanagement methodiek voor integrale beveiliging. Datum: 30 juni 2021 (versie 1.0) Masterthesis: uitgevoerd als afsluiting van de opleiding Master Risicomanagement Auteur: R.A Bhadjan Contact: rbhadjan@hotmail.com Studenten nr: S2080451



Lijst met afkortingen

ICBR	De Interdepartementale Commissie Bedrijfsvoering Rijk
BZK	het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
ADR	Audit Dienst Rijk
BVA	Beveiliging autoriteit
BVA-Beraad	Beveiligingsautoriteiten beraad
TBB	Te Beschermen Belangen
FEZ	Directie Financieel Economische Zaken



Voorwoord

Het afstudeeronderzoek dat voor u ligt is geschreven in het kader van de deeltijd master Risicomanagement aan de Universiteit Twente, faculteit Behavioural, Management and Social Sciences, afdeling Professional Learning & Development. In opdracht van het Beveiligingsautoriteiten beraad (BVA-beraad) is dit onderzoek uitgevoerd. Het BVA-beraad coördineert centraal en in gezamenlijk overleg de beveiliging van de Rijksdienst en geeft waar nodig advies aan interdepartementale besluitvormingsorganen. Het schrijven aan de afstudeeropdracht was een uitdagend proces, desalniettemin kijk ik terug op een zeer leerzame periode. De leuke en inspirerende gesprekken tijdens de opleiding als tijdens de uitvoering van dit onderzoek ga ik missen.

Er zijn een aantal personen die een bijdragen heeft geleverd tot het afronden van deze master. Vanuit de Master Risicomanagement organisatie van Universiteit Twente hebben Dick Wijnveen en Carla Knippers beiden zorggedragen dat ik aan de opleiding kon deelnemen. Dick Molenkamp, mijn voormalig leidinggevende. Marcel Hoogendonk, BVA Rijk en mijn huidige leidinggevende, Marc Modersheim (BVA van het ministerie Economische Zaken en Klimaat/ het ministerie van Landbouw, Natuur en Voedselkwaliteit), Terry Hasselo (BVA van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties & Justitie en Veiligheid) hebben mij de vrijheid gegeven om het onderzoek uit te voeren. Marleen Mensink mijn studiegenoot van Universiteit Twente dank voor het sparren en natuurlijk mijn begeleidend team Prof. dr. ir. Petra C. de Weerd-Nederhof hoogleraar Organisatiekunde en prof.dr. Maria- Euginia. Iacob, hoogleraar Industrial Engineering en Business Information Systems voor de waardevolle en constructieve feedback.

En zeker niet te vergeten mijn lieve dochter Parel. De rollen van moeder en dochter waren op een gegeven omgedraaid "Mam zou je niet naar bed gaan" of "Mam je zit al uren achter je beeldscherm is het niet verstandig dat je nu stopt en even gaat ontspannen". Echt mijn kostbare Parel!

Reshma Bhadjan



Samenvatting

Een snel veranderende wereld vraagt een andere aanpak van risicomanagement. Om hierop te kunnen anticiperen dienen doelen en strategieën frequent aangepast te worden. Het continu verbeteren is geen keuze maar een randvoorwaarden en noodzaak voor organisaties geworden. De Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) waaraan het BVA-beraad adviseert, heeft meermaals geconstateerd dat de integrale beveiliging van de Rijksdienst achterblijft. Zeker wanneer dit wordt vergeleken bij een aantal rijksbrede ontwikkelingen, zoals vergaande digitalisering van de samenleving, (cyber)spionage, terrorisme en andere ontwrichtende dreigingen en -activiteiten. Deze constatering heeft ertoe geleid dat de ICBR het BVA-beraad heeft gevraagd om een rijksbrede standaardmethodiek voor risicomanagement te ontwikkelen.

Dit onderzoek draagt bij aan de oplossingsrichting van het probleem '**Ontwikkel een rijksbrede standaardmethodiek voor het lijnmanagement voor eenduidig en uniform risicomanagement in het kader van integrale beveiliging**'. Het doel van de onderzoeker is om ontwerpen op te leveren die een bijdrage vormen voor de verdere professionalisering van risicomanagement binnen integrale beveiliging van de Rijksdienst.

Omdat dit onderzoek een wetenschappelijk karakter vereist is gekozen voor het Design Science Research Methodology¹ om dit onderzoek gestructureerd vorm te geven. Aan de hand van een probleemanalyse zijn vijf deelvragen geformuleerd. Bij deelvraag 1 is een literatuurstudie uitgevoerd. Voor deelvraag 2 heeft een documentenonderzoek plaats gevonden en bij deelvraag 3 is een praktijkonderzoek ingezet om de Ist-situatie (huidige situatie) te bepalen. Bij deelvraag 4 zijn de resultaten van de bovenstaande onderzoeksmethoden gebruikt om tot de ontwerpen te komen. Deelvraag 5 gaat over het valideren van de ontwerpen door een focusgroep. De deelvragen hebben verrassende inzichten opgeleverd.

¹ Design Science Research Methodology Peffers et al., 2007

Literatuurstudie

Uit de literatuurstudie blijkt dat het uiterst belangrijk is om in de organisatie standaard risicomanagement taal te bespreken. Zonder een gemeenschappelijk taal is een afdeling/team teveel tijd kwijt aan het oplossen van communicatiestoornissen. Daarnaast is bewezen dat de risicoperceptie van een niet deskundige anders is dan die van een deskundige of specialist. Uit de literatuurstudie blijkt ook dat de zes risicoprocesstappen van een aantal risicomanagement modellen zoals de NEN-ISO 31000-2018, COSO-Enterprise Risk Management (COSO-ERM) en Risman hetzelfde zijn. In al deze stappen is het PDCA-Cyclus verweven.

Zes generieke risico processtappen	Risicoprocesstappen in drie gangbare risicomanagementmethoden		
	2017	2018	
Nr. Omschrijving	COSO-ERM (Claassen, 2009)	NEN-ISO 31000 (NEN-2009)	RISMAN (Van Well-stam e.a. 2011)
1 Doelen bepalen	Objective setting	Vaststellen context	Vaststellen doel
2 Identificeren	Event identification	Risico-identificatie	Risico's in kaart
3 Classificeren	Risk assessment	Risicoanalyse	Belangrijkste risico's
4 Beheersen	Risk response Control activities	Risico-evaluatie Risicobehandeling	Beheersmaatregelen in kaart Beheersmaatregelen uitvoeren
5 Evalueren	Monitoring	Monitoring	Evalueren
6 Overdracht	Communication	Communicatie	Actualiseren risicoanalyse

Uit het praktijkonderzoek van Kaplan uit 2013 blijkt dat 80% van de onderzochte organisaties haar strategische doelen niet behaald. Een van de redenen is dat dat 85% van het management minder dan 1 uur per maand aandacht besteedt aan het bespreken en behalen van de strategische doelen.

Documentenonderzoek

Uit het documentenonderzoek blijkt dat er de afgelopen periode binnen de Rijksdienst veel nadruk is gelegd aan de ontwikkeling van systemen, procedures en protocollen (hard controls genoemd) ten behoeve van risicomanagement en Te Beschermen Belangen (TBB). De systemen, procedures en protocollen zijn geschreven door deskundigen en zijn niet altijd toegankelijk opgesteld voor alle beoogde gebruikers.

Praktijkonderzoek

Voor het praktijkonderzoek zijn drie ministeries geselecteerd om deel te nemen aan het onderzoek naar aanleiding van hun maatschappelijke taak. Twee van de ministeries ontwikkelen



beleid voor de burgers en het bedrijfsleven en het andere ministerie draagt zorg voor de nationale veiligheid. Uit het praktijkonderzoek blijkt dat het ministerie dat zorgdraagt voor de nationale veiligheid verder ontwikkeld is op het gebied van risicomanagement dan de andere twee ministeries. Uit het praktijkonderzoek blijkt ook dat ministeries, zonder er bewust van te zijn, risicogestuurd proberen te werken. Daarnaast blijkt uit het onderzoek dat er voldoende is ontwikkeld aan de hard controls kant, maar er weinig aandacht is geweest voor het gewenste menselijk gedrag, de soft controls. Hierdoor is momenteel te weinig en wisselend draagvlak voor risicomanagement bij het lijnmanagement.

Ontwerpen voor het onderzoek

De Auditdienst Rijk (ADR) heeft van 2018 tot september 2020 het rijksbrede programma 'Risicomanagement' getrokken. In het programma zijn de zes risicoprocesstappen om risicogestuurd te werken van Van Staveren als leerlijn ingezet om risicomanagement verder te implementeren binnen de Rijksdienst.

Gezien de bovenstaande inzichten uit de literatuurstudie, documenten-, praktijkonderzoek en de leerlijn die door de ADR is ingezet, is de keuze gemaakt om de leerlijn vast te houden en in de ontwerpen de nadruk te leggen op bewustwording en training. De onderzoeker heeft relevante wetenschappelijke kennis van systemen en methodes van risicomanagement vertaald naar concrete acties en veranderingen die in de praktijk toegepast kunnen worden voor en door het lijnmanagement. Het eerste ontwerp is gericht op de gedragsgerichte methode om bewustwording en draagvlak te creëren op het gebied van risicomanagement en TBB. Het tweede ontwerp is gericht om, via het menselijk gedrag, invloed uit te oefenen zodat een aantal handelingen wordt verricht. Door handelingen/activiteiten te koppelen aan de zes risicoprocesstappen die men volgordelijk moet uitvoeren ontstaat er een cyclus die als uniform model kan dienen voor het lijnmanagement. Dit model is toepasbaar in meerdere vakgebieden dan alleen integrale beveiliging.

De ontwerpen zijn ter toetsing voorgelegd aan de interdepartementale werkgroep 'implementatie van risicomanagement fiche 2' die als focusgroep functioneert in dit onderzoek. Een gedeelte van

de leden van de focusgroep zien meerwaarde in de ontwerpen en een andere deel heeft aangegeven meer tijd nodig te hebben om de ontwerpen te beoordelen. Deze groep zien de ontwerpen als een nieuw product. Afgesproken is bij het komend overleg in juli 2021 dat er gekeken wordt welke producten voor welk doelgroep is ontwikkeld. Daarnaast hebben de projectleiders gevraagd of de werkgroep suggesties heeft voor de ontwerpen.

Conclusie

Of het nu gaat om veiligheid of beveiliging van mensen, gebouwen, goederen of processen. Risicomanagement is een belangrijk instrument om de doelstelling op het gebied van integrale beveiliging te behalen. De hard- en soft controls zijn beide belangrijke elementen die het succes van risicomanagement bepalen.

Concluderend kan gezegd worden dat dit onderzoek een bijdrage kan leveren aan het beter toepassen van risicomanagement binnen integrale beveiliging en aan een ander werkveld. Het is een uitdaging voor de Rijksdienst om theorie met de praktijk te verbinden, te opereren als een open systeem en risico's te managen in de VUCA-wereld. VUCA-wereld staat voor een wereld die aan snelle verandering onderhevig is. Acteren in een VUCA-wereld vraagt een ander mindset, een andere vorm van leiderschapsstijl en 'leiderschaps' vaardigheden (B. Johansen, 2012), (van Staveren 2018). Naar aanleiding van de bovenstaande uitdagingen zijn een aantal aanbevelingen en voorstellen voor vervolgonderzoek gedaan in dit onderzoek. Er is dieper onderzoek nodig welke belemmerende factoren aan de cultuur en structuur kant de Gap veroorzaken tussen de academische- en praktijkwereld op het gebied van risicomanagement, er is dieper onderzoek nodig hoe de Rijksdienst functioneert binnen de keten van integrale beveiliging (functioneert het als een open systeem en wat is de invloed van het politieke krachtenveld). Daarnaast is wetenschappelijk onderzoek nodig hoe je een open systeem bestuurd met een koppeling naar de dynamiek van de VUCA-wereld en integrale beveiliging.



Inhoud

Lijst met afkortingen.....	4
Voorwoord	5
Samenvatting	6
Literatuurstudie	7
1 Inleiding	12
1.1 Aanleiding afstudeeronderzoek.....	12
1.2 Leeswijzer	13
1.3 De Rijksdienst als organisatie.....	13
1.4 Diagnose van het probleem.....	18
1.5 Doelstellingen	21
1.6 Keuze onderzoeksontwerp	22
1.7 Onderzoeksvragen	23
1.8 Scope onderzoek afbakening	25
1.9 Maatschappelijke relevantie	26
2. Onderzoeksopzet.....	27
3 Theoretisch kader	30
3. 1 Aanpak literatuurstudie	30
3.2 Dataverzameling deelvraag 1A	31
3.3 Uitwerking deelvraag 1A	32
3.4 Dataverzameling deelvraag 1B	37
3.5 Uitwerking deelvraag 1B	39
3.6 Documentenonderzoek.....	44
3.7 Kritische discussie na de literatuurstudie	45
4 Praktijkonderzoek	48
4.1 Analyse en resultaten van het onderzoek	50
4.2 Van Theorie en analyse naar ontwerpfase	53
4.3 Ontwerp	56
5 Validatie ontwerpen.....	63



5.1 Conclusies, vervolgonderzoek en aanbevelingen	67
Bijlagen	72
Bijlage 1 Global Risk Management Survey 2019 De top 15 risico's wereldwijd	72
Bijlage 2. Leervragen en praktijkvoorbeelden van verbeterpunten volgens de respondenten	73
Bijlage 3 Overzicht Wettelijk/Rijksbreed Kader.....	75
Bijlage 4 15 voorwaarden van Van Staveren	77
Bijlage 5 Interview vragen.....	78
Bijlage 6 Ontwerp 1 volgens de drie dimensies (methode, organisatie en mens).	80
Bijlage 7 Ontwerp 2 volgens de drie dimensies (methode, organisatie en mens).	81
Bijlage 8 Methodologische verantwoording stappenplan 'Van Asemma et al, 1992' focusgroep	82
Bijlage 9 Verslag focusgroep	83
Bijlage 10 Evaluatiegesprek deelnemers focusgroep	87
Bijlage 11 Het verandermodel van Kotter	88
Bronvermelding	89
Lijst met figuren	92
Lijst met tabellen	93

1 Inleiding

De Rijksdienst bevindt in een veranderende wereld 'VUCA-wereld'. VUCA is een acroniem dat staat voor veel Volatility (onvoorspelbaarheid), Uncertainty (onzekerheid), Complexity (talloze factoren wederzijdse beïnvloeding) en Ambiguity (dubbelzinnigheid).

Naast de VUCA-wereld heeft de Rijksdienst ook te maken met de hogere verwachtingen van de burgers en het bedrijfsleven. De dreigingen vinden tegenwoordig zowel online als offline plaats en brengen nieuwe uitdagingen mee. Opereren in de VUCA-wereld vraagt leren omgaan met de veelal nieuwe en onbekende combinaties van risico's: te beheersen waar het kan, te accepteren waar het moet en risico's te nemen waar het nodig is om waardevolle doelen te realiseren. Het gaat hier ook om hoe weerbaar een organisatie is wanneer er een crisis uitbreekt.

Een organisatie kan weerbaar zijn als de beheerskant, zoals sturing van processen en randvoorwaarden van risicomanagement goed zijn georganiseerd en zijn ingebed in de organisatie. Teveel focus op de beheerskant kan leiden tot bureaucratie en overregulering. Dit zorgt ervoor dat een organisatie minder wendbaar en veerkrachtig is. De gedachte dat risico's uitgedrukt kunnen worden in geld en inzichtelijk en beheersbaar gemaakt kunnen worden, gaat niet meer op. De wereldwijde top 15 risico's² in bijlage 1 vraagt van de toezichthouders om meer risicogestuurd te werken. Dit zodat ze adequaat kunnen inspelen op de complexe ontwikkelingen. We hebben niet meer te maken met een maakbare wereld en 100 procent veiligheid en beveiliging bestaat niet. De plaatsgevonden crises en onzekerheden bieden organisaties kansen om te innoveren en te excelleren.

1.1 Aanleiding afstudeeronderzoek

Risicomanagement is een belangrijk onderdeel van toezicht, veiligheid en beveiliging. Het veld waarvoor het lijnmanagement verantwoordelijk voor is en toezicht op moet houden wordt steeds complexer. De ICBR, heeft geconstateerd dat de integrale beveiliging van de Rijksdienst achterblijft bij een aantal rijksbrede ontwikkelingen.³ Deze constatering heeft ertoe geleid dat de ICBR het BVA-beraad heeft gevraagd om met een rijksbrede standaardmethodiek te komen die

² Global Risk Management Survey 2019_De top 15 risico's wereldwijd

³ Nota Uitwerking ICBR-opdracht jaarplan IBR 2018 uitwerking ICBR-opdracht (Departementaal vertrouwelijk)



tot eenduidig risicomanagement leidt. In de oriëntatiefase heeft een uitgebreide documenten onderzoek plaatsgevonden en de onderzoeksrapporten van de (ADR)⁴ zijn geanalyseerd om helder te krijgen wat daadwerkelijk het probleem is. Dit onderzoek speelt zich af binnen de ministeries van de Rijksdienst.

1.2 Leeswijzer

In hoofdstuk één wordt de diagnose van het probleem, de hoofdvraag, de keuze voor het onderzoeksmethode en de deelvragen vastgesteld. Hoofdstuk twee geeft het onderzoeksontwerp weer. Hoofdstuk drie vormt het wetenschappelijk kader voor dit onderzoek. In hoofdstuk vier wordt het opzet van het praktijkonderzoek besproken daarnaast volgt een analyse van de beschikbare praktijkresultaten. Aan de hand van de literatuurstudie, documentenonderzoek, praktijkresultaten worden een aantal ontwerpen gemaakt. In hoofdstuk vijf wordt de validatie van de ontwerpen beschreven. Het hoofdstuk wordt afgesloten met een aantal conclusies en aanbevelingen.

1.3 De Rijksdienst als organisatie

De Rijksdienst kent twaalf ministeries deze zijn het ministerie van Algemene Zaken, het ministerie van Defensie, het ministerie van Economische Zaken en Klimaat/ het ministerie van Landbouw, Natuur en Voedselkwaliteit, het ministerie van Financiën, het ministerie van Infrastructuur en Waterstaat, het ministerie van Buitenlandse Zaken, het ministerie van Onderwijs Cultuur en Wetenschap, het ministerie van Sociale Zaken en Werkgelegenheid, het ministerie van Volksgezondheid, Welzijn en Sport het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Justitie & Veiligheid (figuur 1). Elk departement heeft een Beveiligings Autoriteit (BVA) toegewezen.

⁴ Inventarisatie risicomanagementpraktijken bij het Rijk 2012 ,2018 en
Risicomanagementproces integrale beveiliging,2018

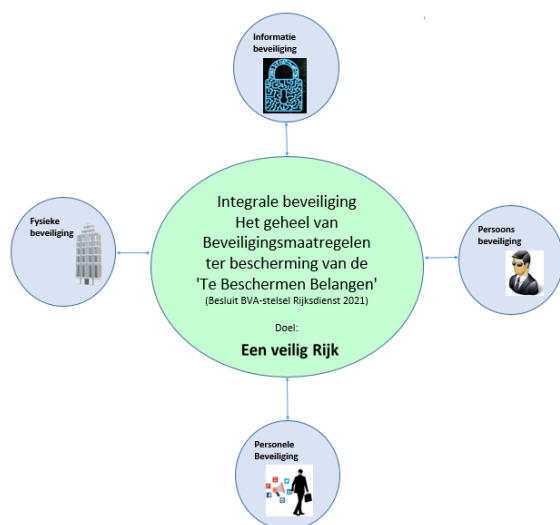


Figuur 1: De 12 ministeries binnen de Rijksdienst

Volgens Daft zijn organisaties: “(1) sociale entiteiten die (2) gericht zijn op een doel, (3) ontworpen zijn als systemen van bewust gestructureerde en gecoördineerde activiteiten, en (4) verbonden zijn met de externe omgeving.” (Daft, 2016, p. 12). De Rijksdienst is een organisatie met een open systeem. Een organisatie die een open systeem is, moet constant in wisselwerking staan met haar omgeving en ze moet constant aanpassen aan de omgeving. Een gesloten systeem is niet afhankelijk van zijn omgeving; het is autonoom, begrensd en hermetisch afgesloten van de buitenwereld Daft (2016, p.14).

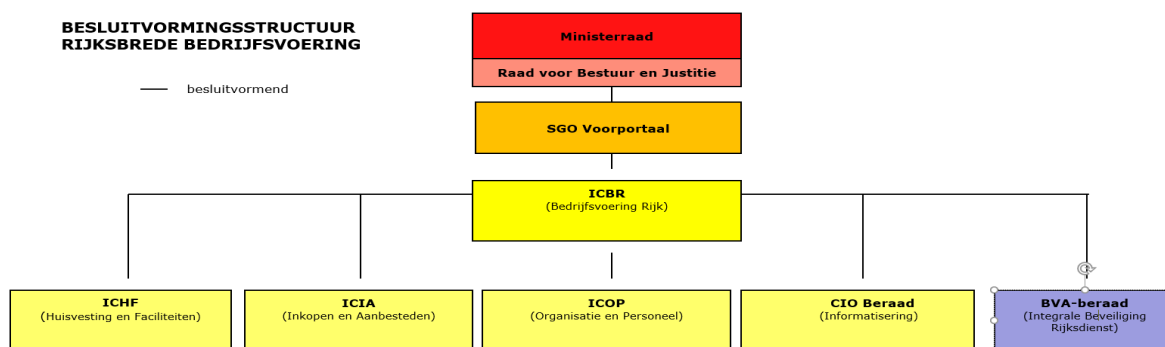
De BVA is verantwoordelijke voor de integrale beveiliging van zijn departement. De rollen en verantwoordelijkheden van de BVA's zijn vastgelegd in het Besluit BVA-stelsel Rijksdienst 2021. De Minister van (BZK) is systeemverantwoordelijk voor de integrale beveiliging van de Rijksdienst. Onder integrale beveiliging wordt verstaan 'het geheel van beveiligingsmaatregelen ter bescherming van de TBB (figuur 2). De TBB zijn personen, informatie, informatiesystemen, materieel, goederen, imago en objecten waarbij in geval van compromittering, of de mogelijkheid van compromittering, nadelige gevolgen, of een risico daarop, kan ontstaan voor de vertrouwelijkheid, beschikbaarheid en integriteit van de primaire processen van de rijksoverheid, delen daarvan of voor andere belangen van de Staat, van zijn bondgenoten of van één of meer ministeries⁵.

⁵ Besluit BVA-stelsel Rijksdienst 2021



Figuur 2: Overzicht TBB

De Beveiligingsautoriteit Rijk (BVA Rijk) heeft een onafhankelijke positie bewaakt en houdt toezicht op de werking van de integrale beveiliging van de Rijksdienst. Voor de integrale karakter en de consistentie wordt de BVA Rijk bijgestaan door de Beveiligingsautoriteiten (BVA's) van de ministeries die ook de deelnemers zijn van het BVA-beraad. Het BVA-beraad is op strategisch niveau gepositioneerd en adviseert aan het Secretarissen-Generaal Overleg (SGO) en de ICBR over de werking van de integrale beveiliging van de Rijksdienst (figuur 3).

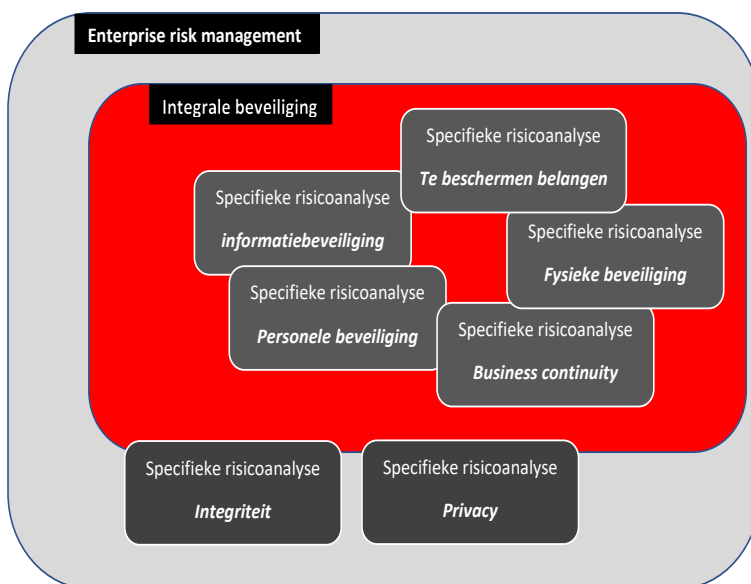


Figuur 3: Besluitvormingsstructuur van Rijksbrede Bedrijfsvoering

Risicomanagement binnen de Rijksdienst en toezicht

Er is in februari 2020 een rijksbreed kaderdocument opgesteld⁶. Het kaderdocument beschrijft wat, ten aanzien van risicomanagement, (minimaal) wordt verwacht en gedefinieerd bij de ministeries. Het doel van dit rijksbrede kader is het creëren van een uniforme werkwijze bij alle ministeries in het denken in termen van risico's, dezelfde risicotaal spreken, het voeren van het juiste gesprek hierover en het nemen van adequate beheersmaatregelen.

In het rijksbrede kaderdocument staat vermeld dat de richtlijnen en principes, dus ook het ISO framework uit de NEN-ISO 31000:2018 als uitgangspunt wordt gebruikt bij risicomanagement. Omdat een aantal ministeries aan het experimenteren zijn met het COSO-Enterprise Risk Management wordt het framework COSO/ERM (figuur 4) ook toegestaan dat het model wordt ingezet als systeem bij integraal risicomanagement. Het kader geeft ook aan dat integrale beveiliging geen eenmalige activiteit is, maar een continu verbeterproces is. Tevens wordt in het document ook aangegeven dat bij het implementeren, uitvoeren en onderhouden van de integrale beveiliging de Plan-Do-Check-Act-cyclus (PDCA-cyclus) kwaliteitscyclus, dient te volgen.

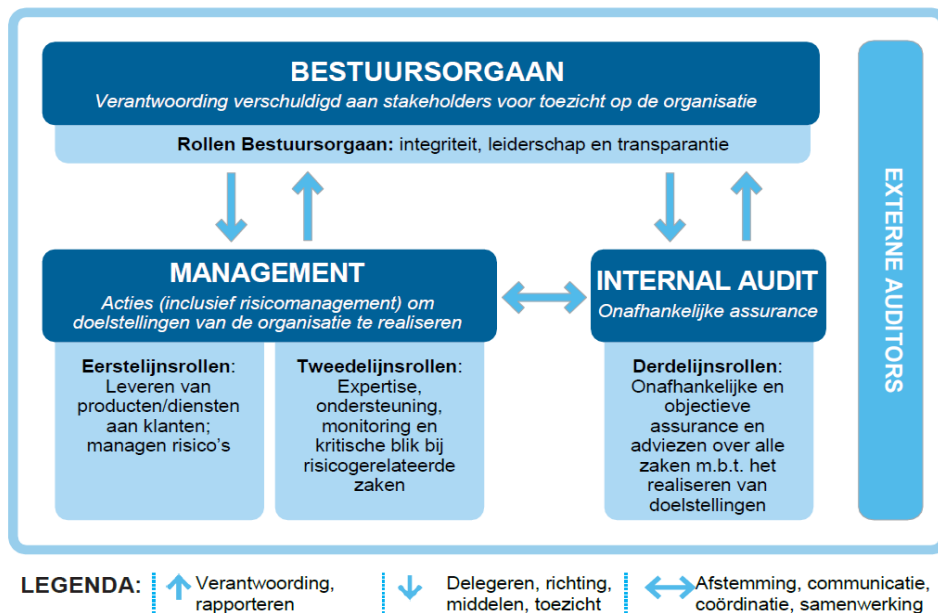


Figuur 4: COSO-ERM versus integrale beveiliging (Bron ministerie van EZK/LNV)

⁶ Rijksbreed kaderdocument 'Risicomanagement Integrale Beveiliging, goed risicomanagement geeft vertrouwen', 2020

Binnen de Rijksdienst wordt er toezicht op integrale beveiliging gehouden middels 'Het Three Lines Model van het Institute of Internal Auditors' (figuur 5). The Three Lines of Model van IIA vermeldt dat 'de verantwoordelijkheid van het management om doelstellingen van de organisatie te realiseren omvat zowel eerste- als tweedelijnsrollen'. In de praktijk houdt dit in dat de eerste- en tweedelijnsverantwoordelijken de samenwerking intensiveren om de doelstellingen te behalen. Echter, de verantwoordelijkheid voor het managen van risico's blijft een onderdeel van de eerstelijnsrol⁷. De derdelijnsrollen beoordelen de werking en samenhang van de eerste- en tweede lijn en rapporteert hierover aan het eindverantwoordelijke lijnmanagement. Dit betekent dat de BVA intern toezicht houdt op het ministerie en de BVA Rijk en andere toezichthouders zoals de ADR, de Algemene Rekenkamer, inspecties, de Algemene Inlichtingen- en Veiligheid dienst (AIVD), de Militaire- en Veiligheidsdienst (MIVD), de Europese Unie (EU), de Noord Atlantische Verdragsorganisatie (de NAVO) toezicht houden op de ministeries.

Het Three Lines Model van het IIA



Figuur 5: The Three Lines Model van het IIA, die binnen de Rijksdienst wordt toegepast

⁷ Het Three Lines Model IIA, 2020

1.4 Diagnose van het probleem

De wens van het ICBR is dat er een rijksbrede standaardmethodiek komt voor het lijnmanagement voor eenduidig en uniform risicomanagement in het kader van integrale beveiliging. Dit zodat ze doordachte en gefundeerde afwegingen kunnen maken om het doel van adequate beveiliging van de aangewezen TBB te behalen. In de praktijk betekent dit dat het lijnmanagement op een uniforme wijze risicomanagement voor integrale beveiliging toepast in de dagelijkse werkzaamheden net zoals bij financiële risico's.

De ADR heeft twee onderzoeken verricht naar risicomanagement. Het eerste onderzoek gaat over 'Inventarisatie risicomanagementpraktijken bij het Rijk'. Het tweede onderzoek heeft de ADR verricht in opdracht van BVA Rijk. Het tweede onderzoek gaat over 'de wijze waarop integrale beveiliging binnen de ministeries is vormgegeven gericht op de TBB'. Deze onderzoeken zijn verricht in 2012 en 2018. De onderzoeker heeft de rapporten van de ADR als uitgangspunt genomen om te analyseren wat daadwerkelijk het probleem is. In tabel 1 staan de belangrijke conclusies uit het eerste onderzoek. In tabel 2 staan de conclusies uit het tweede onderzoek. De conclusies van het tweede onderzoek zijn departementaal vertrouwelijk gekenmerkt. Hierdoor worden alleen de algemene conclusies gedeeld.

Conclusies uit het onderzoek: 'Inventarisatie risicomanagementpraktijken bij het Rijk'

- Er is minimale verbetering te zien ten opzichte van het onderzoek van 2012.
- Er is geen uniform taal gebruik voor risicomanagement.
- In het dagelijks taalgebruik binnen de ministeries is het begrip risico over het algemeen eerder negatief geladen dan positief. Risico wordt als ongewenste gebeurtenis ingevuld; wat kan er misgaan? Dingen waarvan je niet wilt, dat de media bereikt. Risicomanagement wordt daardoor eerder geassocieerd met (nog meer) problemen in plaats van oplossingen. Positieve mogelijkheden (kansen) als gevolg van onzekerheden blijven daardoor buiten beeld.

- Uit de inventarisatie blijkt dat geen van de ministeries gebruik maakt van een expliciet model of framework voor risicomanagement. In een aantal interviews wordt aangegeven dat men impliciet wel 'de stappen van het risicomanagement framework COSO- ERM volgt. Met deze stappen worden de fasen van het risicomanagementproces bedoeld.
- Uit de interviews komt naar voren dat met name bij strategische risico's van de Ambtelijke top komt tot en met de stap van risicoanalyse, maar dat de stappen daarna (risicobeheersing en monitoring) soms lastig zijn te zetten. De oorzaak hiervan wordt gelegd bij het abstracte gehalte van de risicoformulering en de gedeelde verantwoordelijkheid voor de beheersing.
- De ministeries kiezen voor *make* als het gaat om risicomanagement: elk ministerie en elk organisatieonderdeel vindt zelf het wiel (opnieuw) uit, soms meerdere keren over de jaren heen.
- Opvallend is dat de meeste mensen die een opleiding hebben gevolgd zich daarna blijven afvragen hoe ze de geleerde modellen, methoden en technieken kunnen toepassen bij de Rijksdienst en het management en medewerkers overtuigend kunnen adviseren over het nut daarvan. Er is sprake van een transferproblematiek tussen risicomanagementopleidingen en praktijk.
- Het stimuleren van risicomanagement in de praktijk wordt niet altijd aangepakt als een veranderopgave, maar eerder als het inregelen van procedures.

Tabel 1: Conclusies van de ADR uit het onderzoek 'Inventarisatie risicomanagementpraktijken bij het Rijk'

Conclusies uit het onderzoek 'de wijze waarop integrale beveiliging binnen de ministeries is vormgegeven gericht op de TBB'

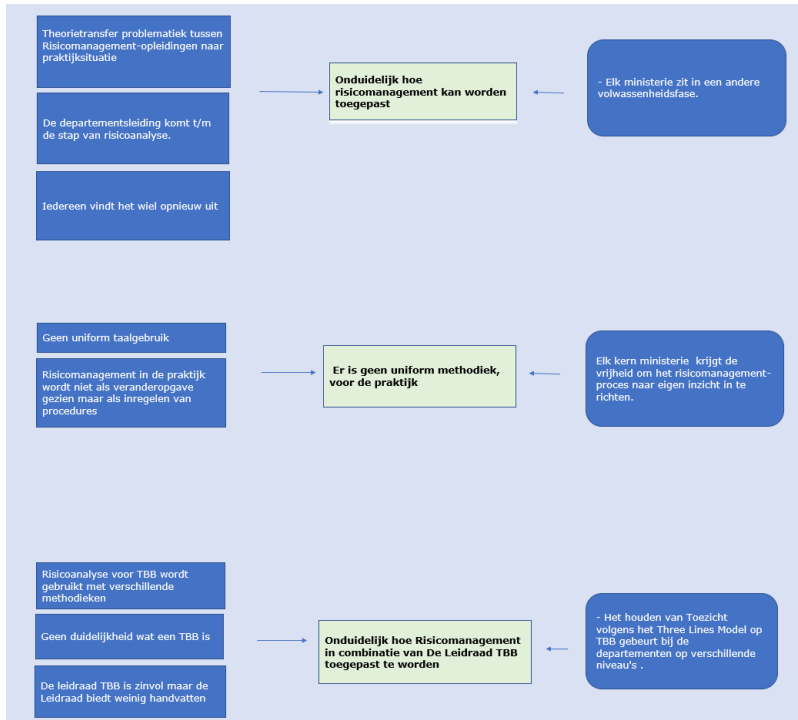
Er bestaan verschillende inzichten over wat een TBB is.

Er vinden risicoanalyses plaats vanuit andere initiatieven die niet specifiek gericht zijn op beveiliging. De risicoanalyses vinden plaats op basis van verschillende methodieken.

De geïnterviewden achten de Leidraad TBB zinvol, maar ze geven aan dat de leidraad weinig handvatten biedt hoe tot een juiste identificatie van de TBB, bij behorende inschaling van de TBB (impact schaling) en bepaling van het restrisico te komen.

Tabel 2: Conclusies van de ADR uit het onderzoek 'de wijze waarop integrale beveiliging binnen de ministeries is vormgegeven gericht op de TBB'

Op basis van de vooronderzoeken en de tabellen 1 en 2 kan het volgende oorzaak- en gevolg diagram worden opgemaakt figuur 6.



Figuur 6: Oorzaak- en gevolg diagram van het probleem

Aan de hand van oorzaak- en gevolg diagram is het daadwerkelijk probleem:

Er is geen uniform methodiek voor risicomanagement voor het lijnmanagement. Hierdoor worden de TBB niet naar urgentie beschermd en kan het lijnmanagement niet doelmatig toezicht houden.

Conclusie:

Er is binnen de Rijksdienst de afgelopen periode geïnvesteerd in hard controls en minder in soft controls. Waar de hard controls gaat over de tastbare, harde elementen in een organisatie zoals structuren, systemen, procedures en protocollen, gaat de soft control kant over de menselijk houding, gedrag, competenties en vaardigheden.

1.5 Doelstellingen

Volgens Van Verschuren en Doorewaard (2015, p. 17) bestaat een doelstelling van een onderzoek uit twee delen: het doel van het onderzoek (extern) en het doel in het onderzoek (intern). Het doel in het onderzoek levert een bijdrage aan de oplossing van het probleem en hierdoor ook aan het doel van het onderzoek.

Op basis van het vooronderzoek, de probleemstelling, de sub-conclusie en de doelstelling is de volgende centrale hoofdvraag van het onderzoek geformuleerd.

Ontwikkel een rijksbrede standaardmethodiek voor het lijnmanagement voor eenduidig en uniform risicomanagement in het kader van integrale beveiliging.

In de probleemstelling spelen meerdere aspecten mee. Uit de analyse uit de ADR-onderzoeken blijkt het volgende:

- Niet-specialisten vinden het lastig om risicomanagement toe te passen en weten niet wat TBB is.
- Het woord ‘risico’ heeft een negatieve lading want risico wordt geassocieerd/ ingevuld als een ongewenste gebeurtenis. Denk hierbij aan; ‘wat kan er misgaan’ of ‘dingen waarvan je niet wilt, dat het de media bereikt’. Risicomanagement wordt hierdoor eerder geassocieerd met (nog meer) problemen in plaats oplossingen.
- Dat een risico ook kansen en mogelijkheden biedt voor innovatie of herinrichting van processen om zodoende weerbaarder te kunnen zijn, wordt niet gezien.

De ADR heeft bij de herhaling van het eerste onderzoek in 2018 ‘Inventarisatie risicomanagementpraktijken bij het Rijk’ leervragen van de respondenten meegekregen op het gebied van cultuur, structuur en methoden. Daarnaast hebben de respondenten praktijkvoorbeelden van verbeterpunten aangedragen (zie bijlage 2). Onderstaand staan de belangrijkste bevindingen uit het overzicht:

- Het is een zoektocht voor de medewerkers om risicomanagement toe te passen;
- Er zijn vragen over ‘Hoe integreer je risicomanagement in de P&C-cyclus en hoe creëer je meer draagvlak in de organisatie;

- Er is nog geen gemeenschappelijke taal en begrippenkader over risico's en risicomanagement.

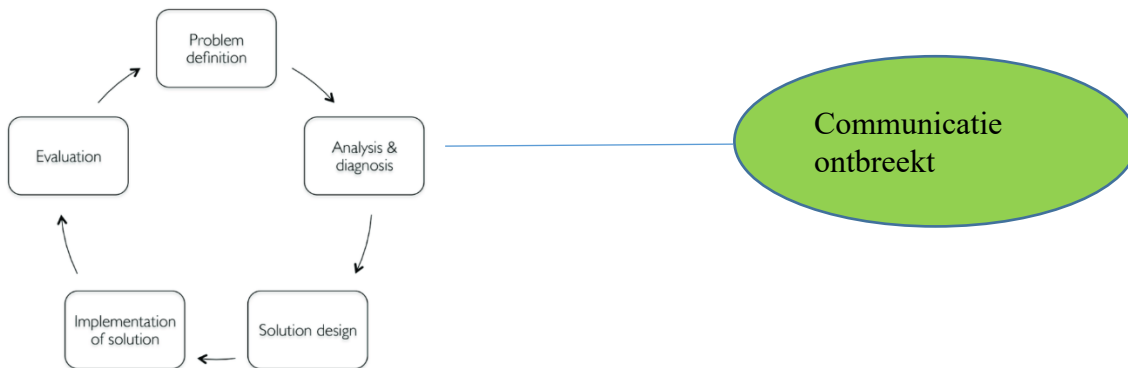
Naar aanleiding van de onderzoeken heeft de ADR van 2018 tot september 2020 het rijksbrede programma 'Risicomanagement' getrokken. In het programma zijn de zes risicoprocesstappen om risicogestuurd te werken van Van Staveren als leerlijn ingezet om risicomanagement te implementeren binnen de Rijksdienst. Daarnaast is in het rijksbreed kaderdocument afgesproken om bij integrale risicomanagement de PDCA-cyclus toe te passen. Gezien deze ontwikkelingen is gekozen om de zes risicoprocesstappen, waarin de PDCA-cyclus model is verweven, als innovatie-instrument in te zetten om risicogestuurd werken te professionaliseren.

Het doel in het onderzoek luidt:

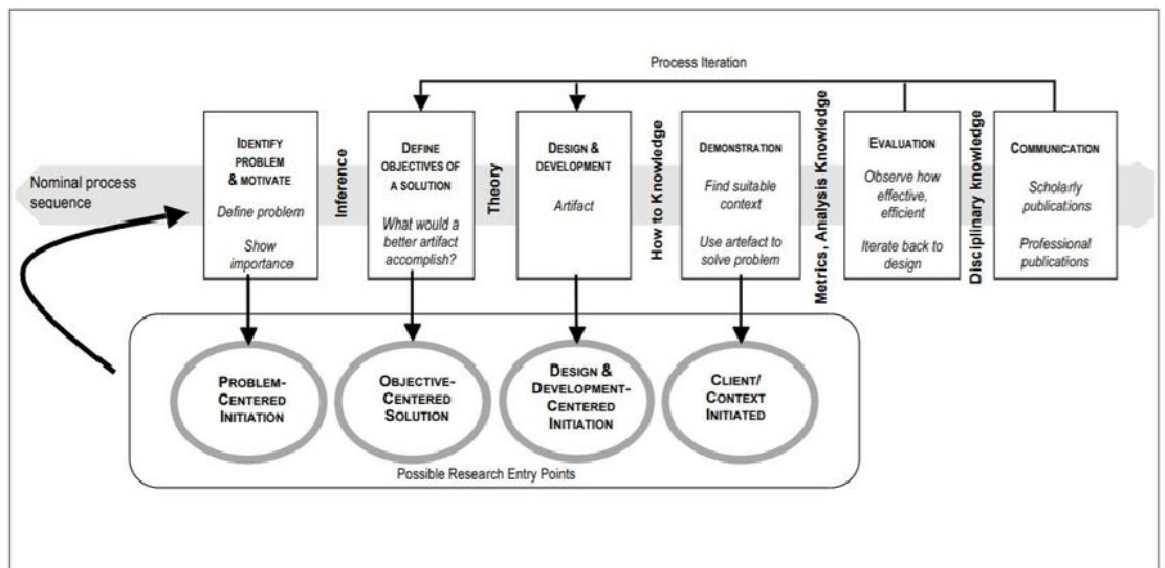
Welke aanpak binnen integrale beveiliging is nodig om het proces van risicomanagement te innoveren naar risicogestuurd werken aan de hand van de PDCA-cyclus model?

1.6 Keuze onderzoeksontwerp

Het doel van dit onderzoek is om een ontwerp te maken die aansluit om de problematiek in de praktijksituatie op te lossen. Om het onderzoek stapsgewijs en gestructureerd uit te voeren, zijn twee modellen vergeleken. Er is gekeken naar het model problem solving cycle van Aken, Berendsen, & Van der Bij, 2012 (figuur 7) en naar de Design Science Research Methodology (DSRM) (Peffer et al., 2007) (figuur 8). Er is gekozen om het DSRM-model toe te passen in het onderzoek omdat bij het problem solving cycle model 'communicatie' geen onderdeel uitmaakt van het proces. Als er een methodiek ontworpen is voor het lijnmanagement voor integrale beveiliging dan dient hierover rijksbreed gecommuniceerd te worden aangezien de relevante doelgroepen verspreid binnen de Rijksdienst werken.



Figuur 7: Model problem solving cycle (bron Aken, Berendsen, & Van der Bij, 2012)



Figuur 8: Het DSRM-model (Peffer et al., 2007)

1.7 Onderzoeksvragen

Het DSRM-model kent een aantal fases om tot een ontwerp te komen. Om antwoord te krijgen op het probleem en te komen tot één oplossing voor een ontwerp zijn vijf onderzoeksvragen geformuleerd. Vanwege de samenhang bestaat onderzoeksvraag 1 uit de delen 1A en 1B. Voor onderzoeksvraag 1 is een literatuurstudie uitgevoerd. Bij onderzoeksvraag 2 is gebruik gemaakt van een documentenonderzoek. De onderzoeksvragen 3 tot en met 5 zijn gericht op het ontwerp. Bij deze vragen is een praktijkonderzoek en focusgroep ingezet. In tabel 3 is een overzicht opgenomen welke inzichten de deelvragen moeten opleveren om tot een ontwerp te komen.



Deelvraag nr.	Formulering deelvraag	Welke inzichten moet de deelvraag opleveren
1 A	Wat is de relatie van risicomanagement met risicogestuurd werken en integrale beveiliging?	Uit het vooronderzoek blijkt dat in de praktijk: - Niet duidelijk is hoe risicomanagement moet worden toegepast; - Het begrip Te Beschermen Belangen is een onderdeel van Integrale beveiliging; De beantwoording van deze vraag geeft inzicht wat risicomanagement en integrale beveiliging inhouden.
1B	Wat is de relatie tussen risicomanagement en risicogestuurd werken en welke rol speelt het menselijk aspect/gedrag bij het inschatten van risico's in het risicomanagement proces.	Bij risicogestuurd werken spelen een aantal menselijke componenten een rol bij het nemen van een beslissing. De beantwoording van deze deelvraag moet inzichtelijk maken welke factoren dit zijn. Dit zodat de inzichten meegenomen kunnen worden bij deelvraag 4. In deelvraag 4 wordt getoetst of de organisaties aandacht besteed aan de menselijke componenten bij risicomanagement.
2	Welke raamwerk/kader/norm zijn er ontworpen door de Rijksdienst die handvatten geven voor risicomanagement en om integrale beveiliging vast te stellen binnen de ministeries .	Uit het oorzaak- en gevolgdiagram en onderzoek van ADR blijkt dat niet duidelijk is wat onder het begrip TBB wordt verstaan. Uit het onderzoek moet blijken of er raamwerk/kader en normen zijn ontwikkeld voor risicomanagement en op het gebied van integrale beveiliging en of deze toepasbaar zijn voor eenieder. De uitkomst van deze deelvraag wordt meegenomen in deelvraag 4. In deelvraag 4 wordt getoetst of de ontwikkelde raamwerk/kader en normen worden gebruikt.
3	In hoeverre wordt risicogestuurd gewerkt momenteel op het gebied van integrale beveiliging en is er een ministerie die als voorbeeld kan dienen?	In de praktijk wordt getoetst of de ministeries risicogestuurd werken op het gebied van integrale beveiliging. De geformuleerde vragen zijn ingedeeld in de thema's cultuur, structuur en methode. Tevens wordt onderzocht of een van de ministeries als voorbeeld kan dienen.
4	Wat is nodig om een stap verder te maken naar risicogestuurd werken in de praktijk en welke aanpassingen zijn nodig om volgens de PDCA-cyclus te werken?	Uit eerder onderzoek blijkt dat risicomanagement is geïmplementeerd maar dat de PDCA-cyclus te abstract is. Bij deelvraag 4 wordt getoetst welke aanpassingen nodig zijn

		om volgens de zes risicoprocesstappen te werken.
5	Biedt het ontwerp volgens experts voldoende basis om een stap te maken naar risicogestuurd werken?	Bij deelvraag 5 wordt het ontwerp gevalideerd. Er wordt getoetst op bruikbaarheid, gebruiksvriendelijkheid en toepasbaarheid.

Tabel 3: Deelvragen met inzichten

In tabel 4 wordt aangegeven welk onderzoeksmethoden per deelvraag worden ingezet.

Deelvragen	Literatuur-studie 	Documenten-onderzoek 	Interview 	Focusgroep 
Deelvraag 1A onderzoek kernwoorden risio.risicomanagement en integrale beveiliging.	X			
Deelvraag 1B risicomanagement versus risicogestuurd werken en het menselijk aspect.	X			
Tweede deelvraag onderzoek welke raamwerk/kader/norm zijn ontwikkeld		X		
Derde deelvraag benchmark hoe wordt er risicogestuurd gewerkt .			X	
Vierde deelvraag is ontwerp artefact naar aanleiding van literatuuronderzoek, documentenonderzoek en interview .	input voor ontwerp	input voor ontwerp	input voor ontwerp	
Vijfde deelvraag is het valideren van inzichten en artefact met de focusgroep.				X

Tabel 4: Onderzoeksmethoden die in het onderzoek worden ingezet

1.8 Scope onderzoek afbakening

Het onderzoek kan breed opgepakt worden. Het vraagstuk raakt diverse ‘hard’ en ‘soft’ controls van de organisatie zoals; proces inrichting, procedures, organisatiecultuur, leiderschap, organisatiestructuur en houding en gedrag van medewerkers. Om antwoord te geven op de onderzoeksvragen is het omwille van de tijd niet mogelijk al deze componenten te verwerken in het onderzoek. Voor het interview gedeelte worden deskundigen die werkzaam zijn in de tweedelijnsrollen van het model van het Three Lines Model geïnterviewd omdat in de praktijk de deskundigen het lijnmanagement ondersteunen en adviseren op het gebied van integrale beveiliging. In dit onderzoek wordt geen plan van aanpak of implementatieplan aangeboden, omdat er vervolgonderzoek nodig is.



1.9 Maatschappelijke relevantie

Dit onderzoek en de resultaten hiervan kunnen ook relevant zijn voor andere bedrijfsonderdelen van de ministeries zoals projecten en programma's die risicomanagement willen vormgeven. Daarnaast kan dit onderzoek als referentiemateriaal ingezet worden om risicogestuurd werken binnen de Rijksdienst te professionaliseren. Ook kan het ingezet worden als een nulmeting voor een vervolgonderzoek om te toetsen of er verbetering is te zien op het gebied van integrale beveiliging versus risicogestuurd werken. Bovendien maakt het onderzoek ook inzichtelijk dat er noodzaak is voor het anders/beter inrichten van risicomanagement.

2. Onderzoeksopzet

In dit hoofdstuk wordt de onderzoeksopzet toegelicht middels het DRSM-model.

Daarnaast wordt aangegeven in welke fase bepaalde onderzoeksmethoden worden gehanteerd.

2.1 Onderzoeksproces en onderzoeksmethoden

Om de probleemstelling helder te krijgen heeft in de orientatie fase vooraf een documentenonderzoek plaatsgevonden. Vervolgens is met de opdrachtgevers verkend wat het probleem is en wat de maatschappelijke relevantie is van het onderzoek. Aanvullend hierop is gekeken door de onderzoeker welke stappen doorlopen moeten worden volgens het DRSM-model om tot een ontwerp te komen.

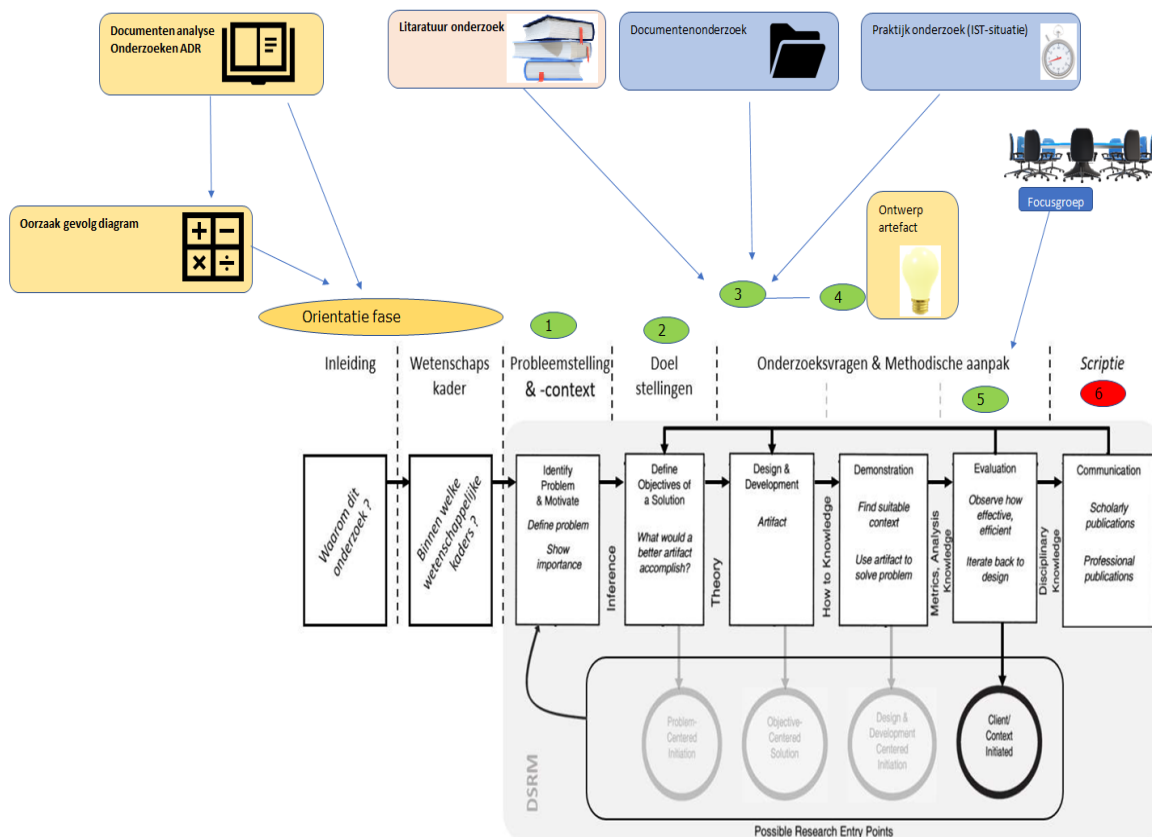
In fase 1 wordt onderzocht wat het probleem is dit is omschreven in paragraaf 1.4.

In fase 2 wordt, naar aanleiding van de probleemstelling, de doelstelling, de scope, de hoofdvraag, de deelvragen en de onderzoeksmethode besproken om het onderzoek vorm te geven. Dit is gebeurd in paragraaf 1.5 t/m 1.8. Door middel van de geformuleerde deelvragen in paragraaf 1.7 wordt invulling gegeven aan fases drie, vier en vijf van het model.

In fase 3 worden de methodische aanpak uitgevoerd. De deelvragen 1 tot en met 5 worden in deze fase uitgevoerd. Er vindt een literatuuronderzoek plaats voor de deelvragen 1A en 1B. Voor deelvraag 2 vindt er een documentenonderzoek plaats. Om antwoord te vinden voor deelvraag 3 wordt naast de literatuuronderzoek en documentenonderzoek ook gebenchmarkt in de praktijk middels een semigestructureerd interview. De deelvragen 1 tot en met 4 worden gebruikt om tot het ontwerp te komen.

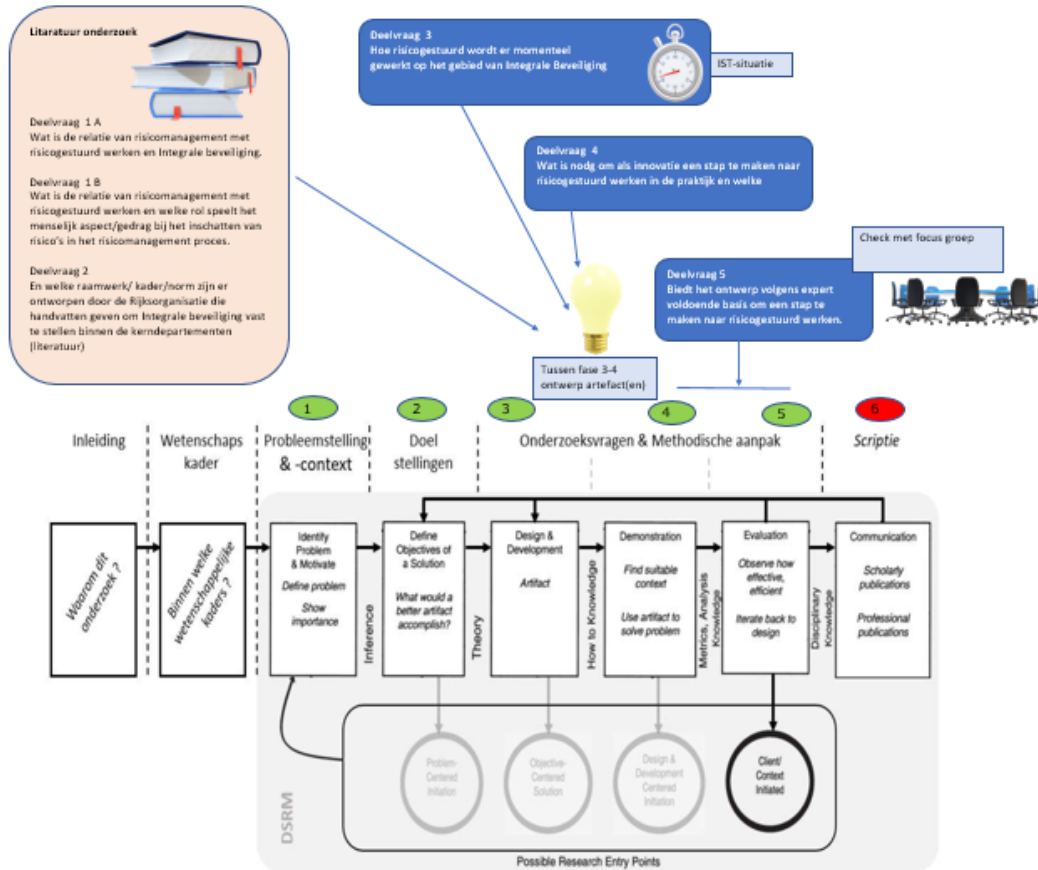
Gezien de termijn van de onderzoeksperiode is gekozen om in dit onderzoek de fases 4 en 5 te combineren. Er wordt geen demonstratie gegeven, maar naast het ontwerp wordt een procesbeschrijving van het ontwerp aangereikt voor validatie aan de focusgroep. Bij positief advies op het ontwerp/ontwerpen wordt in dit onderzoeksrapport als aanbeveling opgenomen om in het 'jaarplan BVA-beraad 2022' als activiteiten op te nemen om over het ontwerp/ontwerpen te communiceren en ermee te experimenteren.

In figuur 9 is een schematische weergave die inzichtelijk maakt bij welke fase de onderzoeksmethoden literatuurstudie, documentenonderzoek, praktijkonderzoek en focusgroep zijn ingezet.



Figuur 9: schematische weergaven fases DSRM versus onderzoeksmethoden

In figuur 10 is een weergave van de deelvragen per fase volgens het DRSM-model.



Figuur 10: Schematische weergave deelvragen versus fases van het DRSM-model

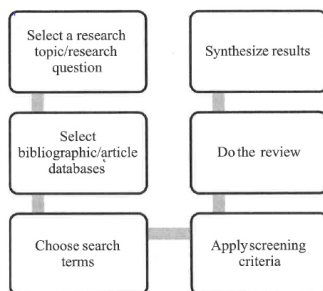
3 Theoretisch kader

Dit hoofdstuk vormt het wetenschappelijk kader voor dit onderzoek. Deelvragen 1 tot en met 2 worden hier behandeld en het hoofdstuk wordt afgesloten met een discussiestuk. Aan de hand van de opgedane wetenschappelijke kennis wordt het onderzoek verder ingericht.

3.1 Aanpak literatuurstudie

De literatuurstudie is het fundament van elk onderzoek. Verschuren en Doorewaard (2015, p. 45-59,) maakt onderscheid tussen theoretisch onderzoek (theorie-ontwikkeland of theorie-toetsend) en praktijkgericht onderzoek (probleemsignalerend, diagnostisch, ontwerpgericht, verandergericht of evaluatief onderzoek) en verder tussen kwantitatief- en kwalitatief onderzoek. Ter inspiratie is de methodiek van Frank & Hatak, 2013 (figuur 11) gebruikt om systematisch literatuuronderzoek uit te voeren en om de nodige data te verzamelen.

How to get published in the best entrepreneurship journals



Figuur 11: Model voor systematisch gericht literatuuronderzoek (bron Frank & Hatak,2013)

Voor de deelvragen 1A en 1B is een literatuuronderzoek uitgevoerd. Er is eerst gekeken naar de aangereikte literatuur uit de masterclasses door de Universiteit Twente. In tabel 5 staat de aangereikte en gebruikte literatuur vermeld.

Onderzoekstermen	Aangereikte literatuur uit de masterclasses door de Universiteit Twente
- Risico	van Staveren, 2015, Hopkin,2010
- Risicomanagement	Bernstein 1995, Hopkin 2010, Van Staveren,2015
- Risicogestuurd werken	Risk taxonomy, 2013, Van Staveren, 2015
	2018 -MRM- S1S1b RM Scope en Doelen- Martin van Staveren .
	2018 - MRM- S1S2 RM concepten & principes - Martin van Staveren - VSRM
	2018-MRM- S2dd7 Risicobeheersing - kansreductie & risico eliminatie 2
	2018 MRM - S2dd8 Risicobeheersing - gevolgreductie & risico -allocatie
	Masterclasses Risicomanagement Sjoerd blokpoel Amsterdam (sessieversie) - 2november 2018
	Organiseren van risicomanagement Presentatie Stuart van den Bos en Edwin Martherus
	Organiseren van Risicomanagement Presentatie Jos Groenendijk

Tabel 5: Aangereikte literatuur door de Universiteit van Twente

Tevens is er gebruikgemaakt van de literatuurdatabase Google Scholar voor het vinden van literatuur.

3.2 Dataverzameling deelvraag 1A

De onderzoeksbegrippen risico, risicomanagement en integrale beveiliging zijn belangrijke kernbegrippen die onderdeel uitmaken van deelvraag 1A.

Wat is de relatie van risicomanagement met risicogestuurd werken en integrale beveiliging?

Omdat er veel literatuur beschikbaar is voor deze onderzoekstermen is er allereerst een overzicht gemaakt met de belangrijke zoektermen in het Nederlands. Omdat onderzoeken vaak in het Engels worden gepubliceerd is er ook een overzicht gemaakt met gerelateerde Engels termen (tabel 6).

Nederlandse term	Gerelateerde term in engels
Risico	risk, ISO 31.000, describe risk, describe risk en Aven
Risicogestuurd werken	riskdriven, probability, riskmanagement
Integrale beveiliging	safety, security, relation safety and security

Tabel 6: Overzicht voor de onderzoekstermen voor deelvraag 1A

Aan de hand van de bovenstaande tabel is naar relevante literatuur gezocht voor de onderzoekstermen risico, risicogestuurd werken en gerelateerde termen. In de database is de selectie periode bijgesteld van 2007 t/m 2021. Dit omdat na de wereldwijde bankcrises 2007/2008 aandacht voor risicomanagement met een razend tempo is toegenomen. Voor de onderzoeksterm integrale beveiliging en de Engelse termen is de selectie periode niet bijgesteld. In de onderstaande tabel (tabel 7) staat in de kolom 'onderzoeksterm versus resultaten in database' weergegeven wat de zoekresultaten zijn geweest.

Nederlandse term	Selectie onderzoeksperiode	Onderzoeksterm versus resultaten in database	Gevonden relevante onderzoeken
Risico	zoek selectie 2007-2022	Risk (620.000)	ISO 31000 2009 – Setting an New Standard for Risk Management (geciteerd 566)
		Risk and ISO (809.000)	
		ISO 31000 and risk (17.000)	
		Describe risk (807.000)	On how to define and understand, and describe risk I. Aven, 2010 (geciteerd 392)
		Describe risk- Aven (17.300)	On How to conceptualise and describe risk I. Aven, 2011 (geciteerd 23)
Risicogestuurd werken	zoek selectie 2007-2022	Aven and ISO 31000 (1590)	The flaws of the ISO 31000 conceptualisation of Risk, 2017 (geciteerd 11)
		Riskdriven (4.810.000)	Risk Governance van Assel & Renn,2010 (geciteerd 444)
		Risk management (740.000)	
		risk management and probability (1.060.000)	
		Risk management and probability and effect (375.000)	
Integrale beveiliging	geen zoek selectie ingesteld	Safety and security	The conceptual and Scientific Denarcation of security in contrast to safety J.Jore 2019, (11 x geciteerd) (met link naar Boholm, et all 2015)
		Springerlink database security 865,065	
		Security and safety 218,225	
		Security in contrast safety 92,485	

Tabel 7: Overzicht van de gevonden onderzoeksrapporten

In tabel 8 staan de belangrijkste onderzoeken vermeld die zijn gebruikt in dit onderzoek.

Gevonden relevante onderzoeken	Reden gebruik in het onderzoek
ISO 31000 2009 – Setting an New Standard for Risk Management (geciteerd 566)	Omschrijving risico en risicomanagement
On how to define and understand, and describe risk I. Aven, 2010 (geciteerd 392)	Risico wordt op verschillende manieren geïnterpreteerd
The conceptual and Scientific Denarcation of security in contrast to safety J.Jore 2019, (geciteerd 11)	Definitie van safety and security door ontwikkelingen
J. Jore 2019 (met link naar Boholm, et all 2015)	De definities voor veiligheid en beveiliging zijn begrippen die door elkaar worden gebruikt.
Riskmanagemetn and Strategy excecution systems Kaplan 2009 (geciteerd 62)	Vier oorzaken dat een organisatie haar strategische doelen niet bereikt
Philosophical perspectives of risk S. Hansson. Aven, 2004 (geciteerd 118)	Verschillene definities van Risico

Tabel 8: Onderzoeksrapporten die gebruikt zijn in dit onderzoek

3.3 Uitwerking deelvraag 1A

Het ontstaan van het begrip risico

Bernstein, 1995 vermeld in zijn boek ‘Against the Gods’ dat in 1654 de doorbraak heeft plaats gevonden in het denken in kansen en risico. Het begon bij het toepassen van gokspellen, het doorontwikkelde instrument werd later ingezet bij verzekering van schepen. Na de financiële crisis van 2008, die omsloeg naar een economische wereldwijde crisis, hebben nationale- en internationale organisaties risicomanagement op een hoger plan gezet. Veel organisaties hebben de silobenadering losgelaten en zijn overgegaan op een organisatie brede benadering (Waal, 2019, p.13).

Volgens de Dikke Van Dale woordenboek betekent risico: gevaar van schade of verlies: risico lopen; op eigen risico waarbij je zelf het risico loopt. De definitie die NEN-ISO 31000:2018 hanteert voor risico is: "effect of uncertainty on objectives. De NEN-ISO 31000:2018 standaard beschrijft dat de effecten van risico's zowel positief als negatief of beiden kunnen zijn en dat het kansen en bedreigingen kan creëren. Van Staveren, (2015, p. 47) omschrijft risico als: een onzekere gebeurtenis met oorzaken, een kans van optreden en effecten op doelstellingen. Volgens van de Waal (2019, p. 16) gaat het bij risico's om gebeurtenissen waarvan het onzeker is of deze gaan plaatsvinden. Het uiteindelijke gevolg is eveneens onzeker. Wanneer het zeker is dat een gebeurtenis wel of niet gaat plaatsvinden is er geen sprake van een risico. P. Slovic (2002) geeft aan dat risico's elementen van subjectiviteit bevat die inzicht geven in de complexiteit van publieke waarneming. Daarnaast geeft P. Slovic aan dat in de communicatie de definitie van risico's niet eenduidig wordt gebruikt. Aven (2012) geeft aan dat de definitie risico beschreven in de NEN-ISO 31000:2018 standaard op verschillende manieren geïnterpreteerd kan worden. S. Hansson (2004) heeft een aantal verschillende definities van risico's opgesomd deze zijn te vinden in tabel 9. Hopkin (2010) vermeldt dat het heel belangrijk is om in de organisatie een standaard risicotaal te bespreken. Zonder een gemeenschappelijk taal zal een afdeling/team veel tijd kwijt zijn aan het oplossen van communicatiestoornissen.

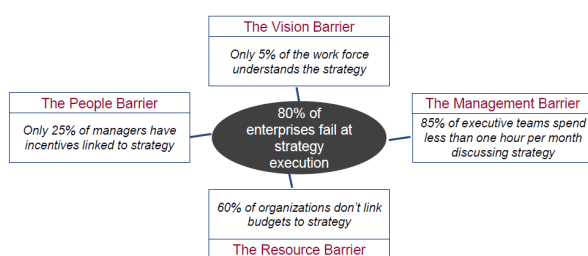
Nr	Definities van Risico
1	Risk = an unwanted event which may or may not occur.
2	Risk = the cause of an unwanted event which may or may not occur.
3	Risk = the probability of an unwanted event which may or may not occur.
4	Risk = the statistical expectation value of unwanted events which may or may not occur.
5	Risk = the fact that a decision is made under conditions of known probabilities ("decision under risk")

Tabel 9: Overzicht van verschillende definities van risico (bron S. Hansson ,2004)

Het begrip risicomanagement

De Risk Taxonomy (2013) geeft aan dat risicomanagement fundamenteel gaat over het nemen van beslissingen. De beslissingen gaan over welke risico prioriteit dienen te krijgen, welke risico's niet relevant zijn (risico acceptatie) en hoeveel kosten en aandacht er besteed moet worden aan

de risico die eraan toe doen. Het Besluit BVA-stelsel Rijksdienst 2021 houdt de volgende definitie van risicomanagement aan 'inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes'. De definitie die ISO 31000:2018 aanhoudt voor risicomanagement is 'Risk management coordinated activities to direct and control an organization with regard to risk'. Van de Waal (2019 p.15) meldt 'Risicomanagement is het proces waarmee wordt geprobeerd de onzekerheid rond het behalen van doelstellingen te managen. Dit proces heeft als doel om ervoor te zorgen dat deze doelstellingen worden bereikt'. Volgens Hopkins, 2010 is risicomanagement 'The set of activities within an organization undertaken to deliver the most favourable outcome and reduce the volatility or variability of that outcome. Volgens van Staveren (2015, p.60) is risicomanagement doelgericht, expliciet, gestructureerd, communicerend en continu omgaan met risico's. Kaplan en Mikes, 2012 geven aan dat je bij risicomanagement te maken hebt met een drie niveaus van risicomanagement. De te voorkomen risico's (interne risico's), strategische risico's en externe risico's. Kaplan, 2013 concludeert in zijn onderzoek dat 80% van de onderzochte organisaties haar strategische doelen niet realiseert. Er worden in zijn onderzoek vier oorzaken genoemd (figuur 12). De belangrijkste oorzaak die genoemd wordt is dat ongeveer 85% van het management minder dan 1 uur per maand besteedt aan het bespreken van strategische doelen.



Figuur 12: Overzicht van vier belangrijke oorzaken waarom een organisatie haar doelen niet realiseert (bron, Kaplan, 2013)

Het begrip Integrale beveiliging

Sinds 1 januari 2005 zijn de Nederlandse beursgenoteerde ondernemingen wettelijk verplicht om conform de Corporate Governance code (voorheen code Tabaksblat) te handelen. De code

schrijft voor dat er een betere verdeling van macht, controle en verantwoordelijkheden zijn binnen een organisatie. Doordat ondernemingen hun risicomanagement zeer gefragmenteerd hebben ingericht vraagt de code ondernemingen ook relaties te leggen tussen expliciete doelstellingen van de onderneming en alle soorten risico's op operationele- en compliance niveaus. Om de interne beheersing te waarborgen schrijft de code voor om met het COSO-ERM risicomanagementmodel te werken. De eerdere code Tabaksplat heeft gezorgd voor een impuls richting risicomanagement en interne beheersing. Dit is ook een van de redenen geweest dat ondernemingen hun traditionele manier van benaderen per vakgebied los hebben moeten laten en een integrale benadering moesten toepassen, voor het vak integrale beveiliging geldt dit ook.

Het Besluit BVA-stelsel Rijksdienst 2021 geeft aan dat integrale beveiliging: het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van beveiligingsmaatregelen voor de beveiliging van de TBB op basis van risicomanagement. Het platform voor Informatiebeveiliging (2010) vermeldt dat integrale beveiliging kan worden omschreven als 'beveiligen door een gecontroleerde samenwerking' waarbij gecontroleerd een aspect is van Enterprise Risk Management uitgevoerd door een 'integraal opererende' beveiligiger, de Enterprise Risk Officer. Appelman (2010, p.13) constateert dat 'De term integrale beveiliging (en veiligheid) te pas en te onpas wordt gebruikt in organisaties, literatuur, kranten en op televisie. Ook komt dit binnen de meeste organisaties voor en zijn er veel organisaties die een eigen of ingehuurde afdeling beveiliging hebben. Vaak worden de begrippen beveiliging en veiligheid (ofwel safety & security) door elkaar gebruikt en door elkaar gehaald'. Boholm et al. (2015) concludeert ook dat de termen safety en security door elkaar worden gebruikt en als synoniemen worden ingezet. Om te achterhalen wat de relatie is van beveiliging en veiligheid met integrale beveiliging is kort aandacht besteedt wat de literatuur vermeldt over de termen security/veiligheid en safety/beveiligen.

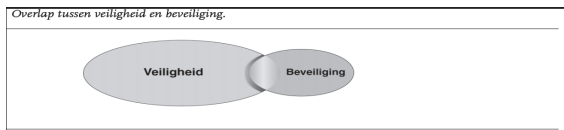
Het begrip veiligheid/security in relatie met integrale beveiliging

Veiligheid wordt gedefinieerd door de Van Dale als 'het veilig zijn en iets in veiligheid brengen'. Volgens W. Stol & Tielenburg (2016, p. 43) betekent veiligheid 'dat mensen effectief beschermd zijn tegen persoonlijk leed tegen de aantasting van hun lichamelijke en geestelijke integriteit'.

Veiligheid heeft ook te doen met goederen. Maar of de aantasting van goederen (het stukgaan of verloren gaan daarvan) een veiligheidskwestie is, hangt uiteindelijk af van de vraag of mensen daardoor leed ondervinden'. Appelman (2010, p.18) geeft aan dat onder veiligheid kan worden verstaan 'een totaalpakket van samenhangende maatregelen om personen binnen de organisatie te beschermen tegen gevaarlijke situaties. Personen kunnen medewerkers, bezoekers, studenten, cliënten, toeleveranciers, partners, gasten enzovoort zijn'. J Jore (2019) omschrijft 'Security can be defined as the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, malicious acts, such as terrorism, sabotage, organized crime, or hacking.'

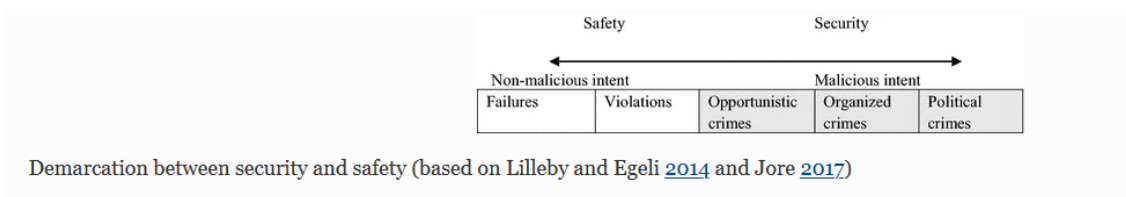
Het begrip beveiligen/ Safety in relatie tot integrale beveiliging

Het Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten, 2019, beschrijft 'Het doel van het stelsel bewaken en beveiligen is het voorkomen van (terroristische) aanslagen op personen, objecten en diensten. Bij de beveiliging van personen staat het voorkomen van ernstige schending van de fysieke integriteit centraal. In het stelsel werken het OM, inlichtingen- en veiligheidsdiensten, politie en bestuurlijke organisaties samen om zorg te dragen dat personen, objecten en diensten, ondanks dreiging en risico, zo veilig en zo ongestoord mogelijk kunnen functioneren'. A. Appelman, (2010, p.16) geeft aan dat onder beveiligen wordt verstaan 'Het totaalpakket van samenhangende maatregelen om de continuïteit van de organisatie te waarborgen tegen (ongewenste) incidenten die door kwaadwillende mensen worden veroorzaakt'. Hollnagel, (2014) omschrijft 'safety is the system of property or quality that is necessary and sufficient to ensure that number of events that could go be harmful to workers, the public, or the environment is acceptably low. J. Jore (2019) omschrijft 'safety risks are associated with an organization's production and profit'. Productions of goods and services are always connected with some kind of risk, and these are risks the organization is willing to take to produce its desired outcome and to gain profit'. Appelman (2010, p.18) concludeert dat er een overlap zit tussen beveiliging en veiligheid, figuur 13.



Figuur 13: Overzicht dat laat zien dat er een overlap zit tussen veiligheid en beveiliging (bron A. Appelman, 2010)

J. Jore (2019) beredeneerd dat safety en security niet hetzelfde zijn. Het grootste verschil zit dat bij security de dader met voorbedachten rade een misdaad wil plegen en bij safety gaat het om fouten en overtredingen die plaatsvinden in de processen, figuur 14. In sommige gevallen gaan safety en security hand in hand.



Figuur 14: Overzicht wat onder safety en security wordt verstaan

3.4 Dataverzameling deelvraag 1B

De onderzoeksbegrippen risicoperceptie, invloed van intentie, risk appetite en determinanten zijn belangrijke kernbegrippen die onderdeel zijn van deelvraag 1B

Wat is de relatie van risicomanagement met risicogestuurd werken en welke rol speelt het menselijk aspect/gedrag bij het inschatten van risico's in het risicomanagement proces.

Aan de hand van tabel 10 is naar relevante literatuur gezocht. Voor de onderzoekstermen risico, risicogestuurd en gerelateerde termen is de selectie periode niet bijgesteld in de database.

Nederlandse term	Gerelateerde term in engels
Risio perceptie	risk, risk perception, influence risk peception, cultural and risk perception
Invloed van intentie	behavior Intention, attitude, drivers for behavioural intention
Risk appetite	risk appetite, heuristos , uncoertaint and heuristos
Determinanten	geen vertaling gebruikt

Tabel 10: Onderzoekstermen voor literatuuronderzoek deelvraag 1B

In tabel 11 wordt in de kolom 'Term versus resultaten in database aangegeven' weergegeven wat de zoekresultaten zijn geweest om relevante onderzoeken/rapporten te vinden voor dit onderzoek.

Nederlandse term	Selectie onderzoeksperiode	Onderzoeksterm versus resultaten in database	Gevonden relevante onderzoeken
Risico perceptie	geen zoek selectie ingesteld	Risk perception (1.900.000)	Why study risk perception P. slovic, 1982 (geciteerd 955)
		Risk perception study (1.050.000)	
		Influence risk perception (1.060.000)	Cross-cultural Risk Perception state challenges O.Renn B. Rohrmann, 2000 (geciteerd 96)
		Different cultural risk perception (759.000) verwijzing naar gerelateerde zoekopdracht 'cross-cultural risk perception'	
Invloed van intentie	geen zoek selectie ingesteld	Behavior (5.170.000)	The theory of planned behavior I. Azjen, 1991 (geciteerd 87.341)
		Behavior and intention (2.790.000)	
		Intention and Attitude (2.960.000)	
		Drivers for behavioural intention (160.000) verwijzing naar gerelateerde zoekopdrachten 'theory of planned behavioral', Gezocht op the theory of planned behavior (2.080.000)	
Risk appetite	geen zoekselectie ingesteld	Risk appetite (739.000)	Judgement under uncertainty Tversky & Kahneman (1974) (geciteerd 40.493)
		Risk appetite and uncertainty (165.000)	
		Risk appetite and uncertainty heuristics (17.800)	
		Uncertainty heuristics (699.000)	
Determinanten	geen zoekselectie ingesteld	Determinanten (202.000)	Determinanten van risicoperceptie Gutteling, 2017 (geciteerd 2.794)
		Determinanten en risico (16.300)	
		Determinanten en risicoperceptie (716)	

Tabel 11: Overzicht van onderzoeksrapporten die gevonden zijn in de database

In tabel 12 staan de onderzoeken vermeld die gebruikt worden voor het rapport.

Gevonden relevante onderzoeken	Reden gebruik in het onderzoek
Why study risk perception P. slovic, 1982 (geciteerd 955)	Risicoperceptie van een leek verschilt met die van een deskundigen
Cross-cultural Risk Perception state challenges O.Renn B. Rohrmann, 2000 (geciteerd 96)	Er zijn 4 lagen die invloed hebben op de samenhang met risicoperceptie
The theory of planned behavior I. Azjen, 1991 (geciteerd 87.341)	Er zijn 3 componenten die invloed hebben of iemand een gewenst gedrag gaat vertonen
Determinanten van risicoperceptie Gutteling, 2017 (geciteerd 2.794)	Er zijn determinanten die een rol spelen bij risicoperceptie

Tabel 12: Onderzoeksrapporten die gebruikt zijn in dit rapport

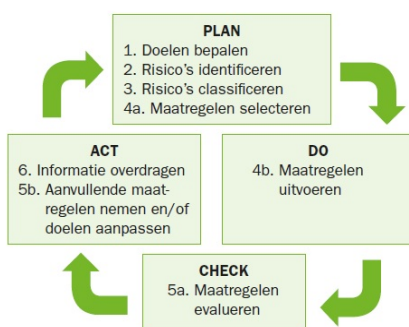
3.5 Uitwerking deelvraag 1B

Risicomanagement versus risicogestuurd werken

Het gangbare risicomanagement legt als kloon van het Tayloriaanse scientific management de nadruk op systemen, planning, controle, beheersbaarheid en daarmee de illusie van onbegrensde maakbaarheid van organisaties. Risicogestuurd werken legt meer nadruk op mens, cultuur, flexibiliteit, leren, aanpassingsvermogen en de realiteit van begrensde maakbaarheid van organisaties. Bij risicogestuurd werken is het doel en het toepassen van de zes generieke risicoprocesstappen in de werkprocessen leidend. De zes risicoprocesstappen zijn niet anders dan de risicostappen die in COSO-ERM NEN-ISO31000 en Risman voorschrijven (van Staveren, 2015 p. 70) (tabel 13). Daarnaast zijn de zes risicoprocessen ook geïntegreerd in het PDCA-cyclus (figuur 16).

Zes generieke risico processtappen		Risicoprocesstappen in drie gangbare risicomanagementmethoden		
		2017	2018	
Nr.	Omschrijving	COSO-ERM (Claassen, 2009)	NEN-ISO 31000 (NEN-2009)	RISMAN (Van Well-stam e.a. 2011)
1	Doelen bepalen	Objective setting	Vaststellen context	Vaststellen doel
2	Identificeren	Event identification	Risico-identificatie	Risico's in kaart
3	Classificeren	Risk assessment	Risicoanalyse	Belangrijkste risico's
4	Beheersen	Risk response Control activities	Risico-evaluatie Risicobehandeling	Beheersmaatregelen in kaart Beheersmaatregelen uitvoeren
5	Evalueren	Monitoring	Monitoring	Evalueren
6	Overdracht	Communication	Communicatie	Actualiseren risicoanalyse

Tabel 13: Overeenkomst risicoprocesstappen (bron van Staveren, 2015 p.70)



Figuur 1. De zes generieke risicoprocesstappen in de PDCA-cyclus

Figuur 15: de zes risicoprocesstappen in het PDCA-cyclus

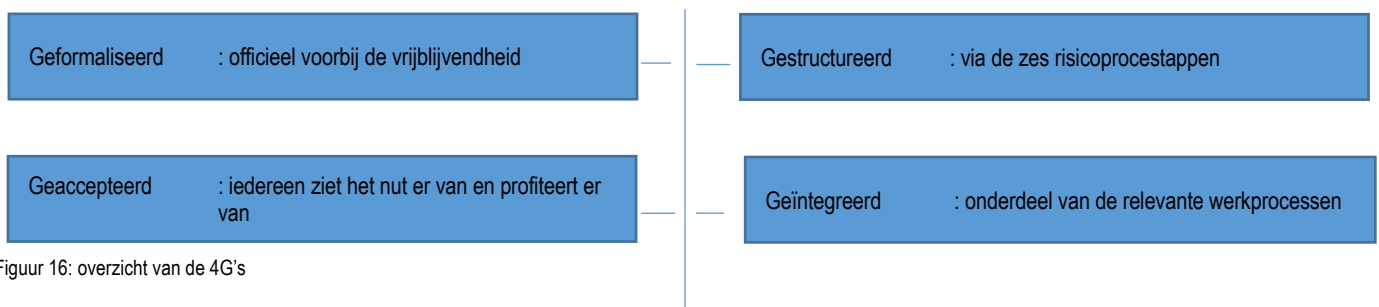
Risicomanagement dient gekoppeld te worden aan de doelen van een organisatie.

Van Staveren (2015, p. 33) heeft een overzicht ontwikkeld waarin een aantal kenmerken van conventioneel risicomanagement ten opzichte van risicogestuurd werken wordt benoemd in onderstaand tabel (tabel 14).

	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 14: Kenmerken conventioneel risicomanagement versus kenmerken van Risicogestuurd werken (bron van Staveren, 2015 p. 33)

Van Staveren, (2015 p.152 + 153 + 102) heeft 15 voorwaarden benoemd op het gebied van organisatiestructuur, organisatiecultuur en aan de methode om risicogestuurd te werken. Van Staveren geeft ook aan dat niet alle 15 voorwaarden aanwezig hoeven te zijn om een start te maken met risicogestuurd te werken. Risicogestuurd werken is pas geïmplementeerd als er cyclisch volgens de 4 G's wordt gewerkt (figuur 16).



Figuur 16: overzicht van de 4G's

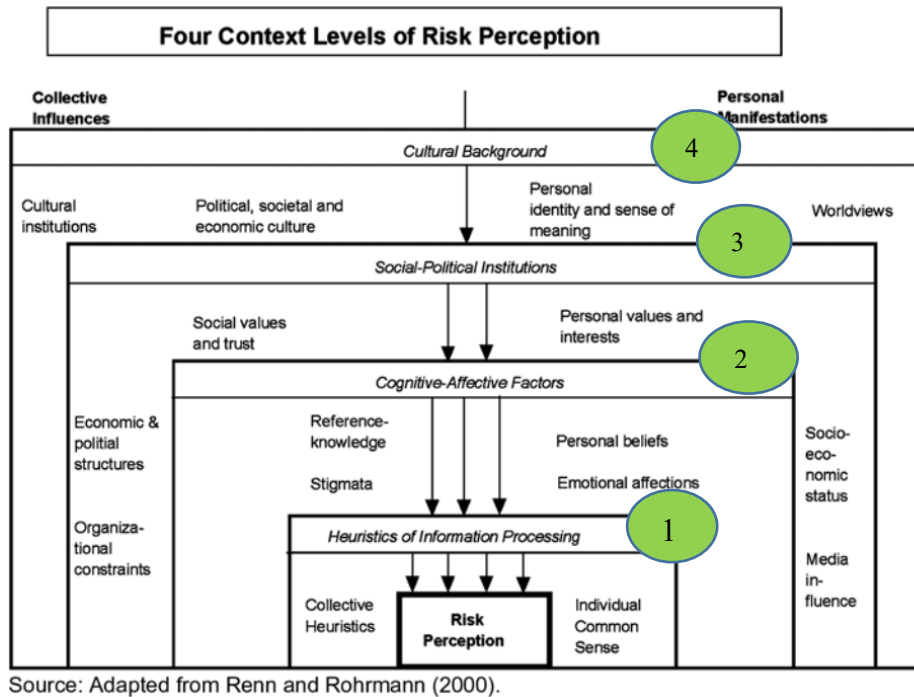
Inschatten van risico is subjectief

Om een inschatting te maken over de grootte van de risico's (risicobeoordeling) wordt bij risicoanalyses vaak gebruikt gemaakt van kans maal effect waarbij het risico het product is van kans maal effect. Bij het toepassen van deze formule worden er drie inschattingen gemaakt hoe vaak de situatie voorkomt, wat is de kans dat een ongewenst effect optreedt en wat is het mogelijke effect dat zal optreden. Aan de blootstelling, waarschijnlijkheid en het effect zijn getallen verbonden. Deze worden met elkaar vermenigvuldigd, hoe groter het getal is, hoe groter het risico is dat het ongewenste negatieve effect zal optreden. Deze methodiek wordt vaak ingezet in de verzekeringswereld. Tegenwoordig staat deze wegingsmethodiek ter discussie omdat het inschatten van risico's niet relatief maar subjectief is. Renn, Klinke en Van Asselt, (2011) beargumenteren wetenschappelijk waarom kans maal effect niet meer op gaat: 'not all risks are simple: they cannot all be calculated as a function of probability and effect. Many risks, which require societal choices and decisions, are adequately characterized as complex, uncertain and/or ambiguous'. Van Staveren (2015, p. 51 + 52) benadrukt ook dat 'risico als kans maal gevolg gebruikt kan worden zolang de onvermijdelijke subjectiviteit die ten grondslag ligt aan de inschattingen van de risico's niet wordt veronachtzaamd, want het inschatten van kansen en risico's is niet relatief maar subjectief is en dat de subjectiviteit het resultaat is van de perceptie van de werkelijkheid'.

Risicoperceptie

Risicoperceptie is een belangrijke factor bij beslissingen die mensen nemen over risico's (Slovic, 1987). Van Staveren (2015, p. 53) geeft aan dat risicoperceptie is de unieke wijze waarop een persoon een risico ziet. Renn & Benninghaus (2013) geven aan dat er vier lagen zijn met belangrijkste componenten die samenhang hebben met risicoperceptie, iedere laag is een onderdeel van de volgende laag (figuur 17). In het overzicht wordt onderscheidt gemaakt in persoonlijke en collectieve invloeden. Laag 1 gaat over het oordelen van een risico op basis van ervaring uit het verleden. Laag 2 gaat over cognitieve- en affectieve factoren (overtuiging en gevoelens) bij de beoordeling van risico's. Bij laag 3 spelen sociale- en politieke

organisatievormen een rol bij het beoordelen van risico en bij laag 4 spelen culturele achtergrond bij de beoordeling van risico een rol.



Figuur 17: Overzicht van vierlagen van risicoperceptie (bron Renn en Rohrmann, 2000)

P. Slovic, (1987) meldt dat de risicoperceptie van niet deskundigen verschilt van de risicoperceptie van experts. Gutteling (2017, p. 14) benoemd een aantal determinanten die bij risicoperceptie een rol spelen en meldt dat het inschatten van risico's subjectief is, zie tabel 15.

Heuristiek/vertekening	Verklaring
Ankerings	Beoordeelde kansen, frequenties, of getalsmatige waarden liggen te dicht bij de initiële waarden (wellicht op basis van irrelevante cues), ondanks nieuwe informatie.
Beschikbaarheid	Achtergrond informatie krijgt te weinig waarde in vergelijking met makkelijk in het geheugen gevonden informatie.
- Primacy/recency	De eerste of meest recente gebeurtenissen kunnen het makkelijkst worden teruggehaald uit het geheugen en krijgen om die reden teveel gewicht.
- Saliency	Saillante informatie krijgt teveel gewicht in vergelijking tot andere informatie.
- Status Quo	Ervaring uit het verleden is levendiger en van meer gewicht dan hypothetische alternatieven.
Overmoedigheid	Geschatte kansen zijn niet accuraat.
Lichtgelovigheid	Bewijs dat patronen en causale verklaringen ondersteunt wordt te snel geaccepteerd.
Framing	Presentatie van gegevens (bv. in oplopende of aflopende wijze) heeft invloed op kans schattingen of de inschatting van onzekere gebeurtenissen.
Wijsheid achteraf	Geloof dat een kans gebonden gebeurtenis onvermijdelijk of te voorspellen was.
Illusie van controle	Mensen denken dat hun vaardigheden de kans op optreden van kans gebonden gebeurtenissen kan beïnvloeden.
Wet van de kleine getallen	Het idee dat kleine steekproeven representatief zijn voor de populatie.

Tabel 15: Determinanten die een rol spelen bij risicoperceptie (bron Gutteling 2014)

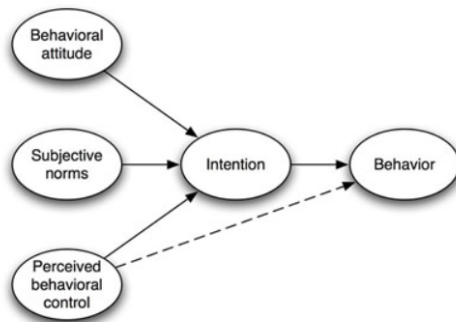
Bias

Naast risicoperceptie speelt bias ook een rol bij het nemen van beslissingen. Slovic (2010, p. 21) meldt dat er een relatie is tussen risico en gevoelens en concludeert 'if we like an activity, we tend to judge its benefit as high and its risks as low; if we dislike it, we judge it the opposite- low benefits and high risk. Van Staveren (2015, p. 55) benadrukt dat er drie belangrijke systematische afwijkingen voor omgaan met risico's zijn de beschikbaarheidsbias (risico inschatten op basis van ervaring uit het verleden), optimisme-bias (risico inschatten op basis zelfoverschatting) en de bevestigingsbias (risico inschatten op basis van opvatting en overtuigingen). Inzicht hebben in deze bias en erop inspelen kan door een multidisciplinair team in te zetten bij een risicoanalyse.

Componenten die een rol spelen bij het nemen van risicobeslissingen

The theory of planned behavior (I. Azjen (1985) (figuur 18) geeft aan dat het bewust gedrag voortkomt uit de intentie om het gedrag te vertonen. De drie componenten attitude 'toward the behavior' (houding van een persoon ten opzichte van het gedrag, subjective norm/ subjectieve normen (datgene wat een persoon denkt dat anderen in zijn directe omgeving vinden en hoe ze over oordelen) en Perceived behavioral control/waargenomen gedragscontrole (mate waarin gedrag eenvoudig is uit te voeren, het gaat hierom eigen vaardigheden en omgevingsfactoren die het gedrag bevorderen of belemmeren) bepalen de intentie of iemand wel of niet het gedrag gaat

uitvoeren. Hoe sterker de intentie is om het gedrag uit te voeren, des te groter de kans is dat een individu daadwerkelijk in actie komt.



Figuur 18: The theory of planned behavior (bron I. Azjen, 1991)

3.6 Documentenonderzoek

Voor het documentenonderzoek is een bureaustudie uitgevoerd, de volgende deelvraag is geformuleerd:

Welke raamwerk/kader/norm zijn er ontworpen door de Rijksdienst die handvatten geeft om integrale beveiliging vast te stellen binnen de ministeries?

Er is gekeken naar de ontwikkelde jaarplannen, handreikingen, kaders en besluiten die zijn ontwikkeld. Voor de documenten is gebruik gemaakt van het rijksportaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de website www.wetten.overheid.nl. Gebaseerd op de bureaustudie kan geconcludeerd worden dat er voldoende kaders, handreikingen en werkdocumenten zijn ontwikkeld voor de TBB en voor risicomanagement. Het overzicht met de belangrijke ontworpen kaders en handreikingen die zijn ontworpen voor TBB en risicomanagement staat in bijlage 3 vermeld.

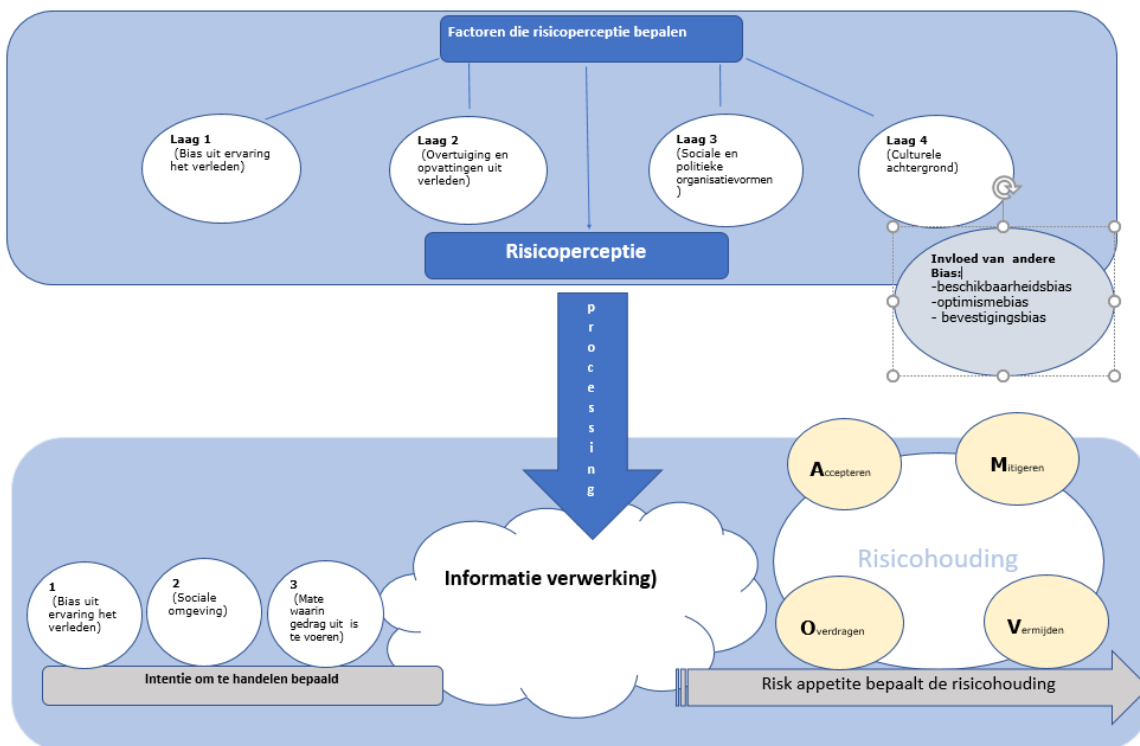
Een sub-conclusie is dat er diverse rijksbrede kaderdocumenten zijn ontwikkeld op het gebied van risicomanagement en TBB door deskundigen. Het lijkt dat de aanname is gedaan dat de documenten toegankelijk zijn voor eenieder. Er is geen training of procesbeschrijving ontworpen om bewustwording te creëren voor niet deskundigen.

3.7 Kritische discussie na de literatuurstudie

Op basis van de literatuurstudie zijn de volgende inzichten vastgesteld:

- Er zijn diverse definities voor de termen risico's en risicomanagement. Uit de literatuurstudie blijkt dat het heel belangrijk is om in de organisatie een standaard risicotaal te bespreken. Zonder een gemeenschappelijk taal is een afdeling/team teveel tijd kwijt aan het oplossen van communicatiestoornissen. Daarnaast is bewezen dat de risicoperceptie van een niet deskundige anders is dan die van een deskundige. Risicomanagement dient gekoppeld te worden aan de doelen van een organisatie. Uit het praktijkonderzoek van Kaplan blijkt dat 80% van de onderzochte organisaties haar strategische doelen niet behaald. Een van de redenen is dat 85% van het management minder dan 1 uur per maand aandacht besteedt aan het bespreken en behalen van de strategische doelen.
- Veiligheid en beveiliging zijn belangrijke aspecten van integrale beveiliging. In de Nederlandse literatuur is weinig te vinden over veiligheid en beveiliging. Door te zoeken op de Engelse terminologie safety and security is veel meer informatie te vinden over de ontwikkeling van beide onderwerpen. In zowel in de Nederlandse als in de Engelse literatuur is te vinden dat beveiliging en veiligheid twee aparte werkvelden zijn en dat de definities door elkaar worden gebruikt. De ontwikkelingen dat dreigingen online en offline plaatsvinden en dat dit effect heeft op de safety- en securitywereld. Over deze ontwikkeling is weinig te vinden in de Nederlandse literatuur.
- Inschatten van risico's is een subjectief proces omdat elk individu een eigen risicoperceptie, opvattingen en ideeën heeft. Er zijn vier lagen die samenhang hebben met risicoperceptie. Laag 1 gaat over het oordelen van een risico op basis van ervaring uit het verleden. Laag 2 gaat over cognitieve- en affectieve factoren (overtuiging en gevoelens) die mee spelen bij de beoordeling van risico's. Bij laag 3 spelen sociale- en politieke organisatievormen een rol bij het beoordelen van risico en bij laag 4 spelen culturele achtergrond bij de beoordeling van risico een rol. Naast de risicoperceptie hebben de bias en intentie ook een rol in het proces. Er zijn er drie belangrijke systematische afwijkingen voor omgaan met risico's de beschikbaarheidsbias (risico inschatten op basis van ervaring uit het verleden),

optimismebias (risico inschatten op basis zelfoverschatting) en de bevestigingsbias (risico inschatten op basis van opvatting en overtuigingen). De attitudes, subjectieve norm en de waargenomen gedragscontrole beïnvloeden de intentie. De intentie is de motivatie van een persoon om het gedrag te vertonen en in risicomanagement is de risk appetite die de risicohouding bepaald. De risicohouding die hieruit voortvloeit is de keuze om risico's te accepteren, het verkleinen van de kans en/of de gevolgen, het verzekeren van het risico of het vermijden van het risico's. Naar aanleiding van de bovenstaande literatuurstudie is een schematisch weergave gemaakt om inzichtelijk te maken hoe het beslissingsproces plaats vindt (figuur 19).



Figuur 19: Schematisch overzicht van factoren die de risicoperceptie bepalen, hoe informatieverwerking plaatsvindt en welke risicohouding wordt aangenomen (bron R. Bhadjan, 2021)

- Risicogestuurd werken legt de nadruk op mens, cultuur, flexibiliteit, leren, aanpassingsvermogen en de realiteit van begrensde maakbaarheid van organisaties. Niet alle 15 beschreven voorwaarden van Van Staveren dienen aanwezig te zijn om risicogestuurd te kunnen werken. Risicogestuurd werken is pas geïmplementeerd als er op cyclisch wijze volgens de 4 G's wordt gewerkt.



- Uit het documentenonderzoek blijkt dat er voldoende wettelijke kaders ontworpen zijn. Echter zijn de wettelijke kaders niet toegankelijk voor iedereen. Het lijkt erop dat de aanname wordt gemaakt dat een uniform kader voldoende is om een verandering te bewerkstelligen in een proces of organisatie.

4 Praktijkonderzoek

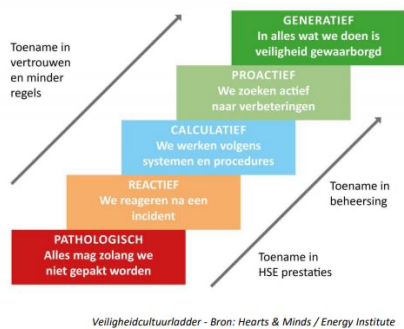
Ter aanvulling van de literatuurstudie en om het eerste beeld uit de bureaustudie te toetsen wordt er ook een praktijkonderzoek uitgevoerd om antwoorden te vinden op deelvraag 3. In dit hoofdstuk wordt het opzet van het praktijkonderzoek besproken daarnaast volgt een analyse van de beschikbare praktijkresultaten. De resultaten die voortvloeien uit de deelvragen 1 tot en met 3 worden gebruikt om de vierde deelvraag vorm te geven. De deelvraag voor het praktijkonderzoek luidt:

Hoe risicogestuurd wordt er momenteel gewerkt op het gebied van integrale beveiliging en is er een ministerie die als voorbeeld kan dienen?

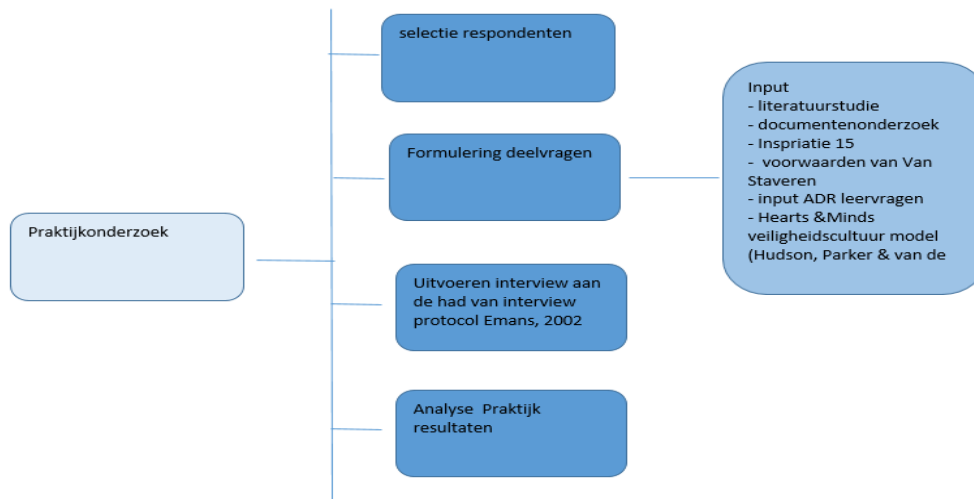
Voor het praktijkonderzoek is er gekozen om drie interviews te houden bij drie verschillende ministeries. De ministeries zijn geselecteerd naar aanleiding van hun maatschappelijke taakveld. Twee ministeries ontwikkelen beleid voor de burgers en het bedrijfsleven en het andere ministerie zorgt voor de nationale veiligheid. Er is bewust een keuze in deze indeling gemaakt om te benchmarken of de nut of noodzaak van risicomanagement verschilt als er verschillende maatschappelijke taakgebieden zijn. De geïnterviewden per ministerie zijn direct of indirect verantwoordelijk voor het risicomanagement en TBB in het proces. Door middel van gestructureerde interviews wordt invulling gegeven aan het praktijkonderzoek.

Voor de interviews is zoveel mogelijk de interview protocol van Emans, 2002 gehanteerd. Voordat de afspraak voor het interview werd ingepland is eerst toestemming gevraagd aan de leidinggevende van de respondenten via de e-mail. In de e-mail werd vermeld dat het gesprek op vertrouwelijk niveau plaatsvindt en dat de gegevens geanonimiseerd worden. Dit omdat de respondenten gevoelige informatie van zijn/haar departement vrijgeeft. De interviews zijn via Webex gehouden i.v.m. Covid-19. Voordat er gestart werd met het interview is nogmaals benadrukt dat het gesprek op vertrouwelijke basis plaats vindt en dat de gegevens geanonimiseerd worden. De interviews zijn opgenomen met de toestemming van de geïnterviewden en zijn na verwerking in het verslag vernietigd. De bevindingen uit de interviews zijn ter afstemming voorgelegd aan de geïnterviewden. De interviewverslagen kunnen opgevraagd worden bij de onderzoeker. In het praktijkonderzoek is gekeken naar de huidige

risicomanagement en of er risicogestuurd wordt gewerkt. Daarnaast ik gekeken of een van de ministeries als voorbeeld kan dienen. De 15 voorwaarden die beschreven zijn door van Staveren, 2015 (bijlage 4) zijn ter inspiratie gebruikt om de interviewvragen en de analyse in paragraaf 4.1 vorm te geven. De set met de interviewvragen zijn te vinden in bijlage 5. Aan de hand van een volwassenheidsmodel wordt ook onderzocht in welke fase een organisatie zit. Er is gekozen voor het Hearts & Minds veiligheidscultuur model (Hudson, Parker & van de Graaf, 2002) (figuur 20). Dit omdat het model ingezet kan worden in diverse profit- en non-profitorganisaties. In figuur 21 wordt het proces schematisch weer gegeven.



Figuur 20: Volwassenheidsmodel van Shell (bron Hudson, Parker & van de Graaf, 2002)



Figuur 21: Schematisch weergave van het praktijkonderzoek

4.1 Analyse en resultaten van het onderzoek

In deze paragraaf wordt de analyse van de interviews beschreven. Op basis van de literatuurstudie en de analyse van de interviews worden de knel- en aandachtspunten benoemd.

Benchmark ministeries

Aan de hand van de gehouden interviews is er eerst een analyse gemaakt of er verschillen zijn te ontdekken tussen de drie geïnterviewde ministeries. Uit de analyse blijkt dat het ministerie die het maatschappelijk taakveld heeft op de nationale veiligheid verder ontwikkeld is op het gebied van risicomanagement omdat de risico's van het ministerie vaak gaat over mensenlevens.

Risicomanagement is bij dit ministerie ook in ontwikkeling, maar is wel ingebed in de organisatie.

Er wordt volgens de 4 G'S gewerkt (continu gestructureerd, geformaliseerd, geïntegreerd en geaccepteerd) met risico's in de organisatie. Daarnaast eist de organisatie van het lijnmanagement dat risicomanagement wordt beheerst. Dit ministerie zit volgens het Hearts & Minds groeimodel in de calculatieve fase.

De ministeries die geen maatschappelijk taak hebben op het gebied van nationale veiligheid geven aan dat ze in de reactieve fase zitten. De ambitie van deze ministeries zijn door te groeien naar de calculatieve fase en de proactieve fase.

Risicomanagement versus risicogestuurd werken

Voor de tweede analyse is gekeken naar de werking van risicomanagement in de praktijk en of er risicogestuurd gewerkt wordt. Voor deze analyse is ook naar de 15 benoemde voorwaarden van Van Staveren gekeken. In het onderstaande tabel (tabel16) staat vermeld welke componenten aanwezig zijn op het gebied van organisatiestructuur, cultuur en methode kant.

Aanwezige elementen aan de organisatiestructuur om risicogestuurd te werken

- Elk ministerie heeft aan de structuurkant de rollen en verantwoordelijkheden goed belegd;
- De beheersing van risico's is formeel gedelegeerd aan de personen die dit als dagelijks activiteit kunnen doen;
- De beheersing van risico's wordt 'formeel' gerapporteerd aan leidinggevende en toezichthouders;

Aanwezige elementen aan de cultuur kant om risicogestuurd te werken

- Er is of wordt gewerkt aan multidisciplinaire teams;

Aanwezige elementen aan de methode kant om risicogestuurd te werken

- De deskundigen trachten te werken volgens een risicomanagement methodiek (ISO 31000, COSO ERM, SRA methodiek).

Tabel 16: Overzicht van aanwezige elementen op het gebied van risicogestuurd werken.

Deelconclusie: Uit de 15 voorgeschreven voorwaarden van Van Staveren zijn er 5 elementen van risicogestuurd werken aanwezig in de Ist-situatie.

Knelpunten van risicogestuurd werken

Voor dit deel van de analyse is de keuze gemaakt om het ministerie die aan nationale veiligheid werkt niet te betrekken in de analyse. Dit omdat het ministerie al in de calculatieve fase zit en aan het bezien is of zij wil doorgroeien naar de proactieve fase. In de aanbeveling zal opgenomen worden dat het ministerie als voorbeeld kan dienen voor de overige ministeries.

In tabel 17 en tabel 18 staan de knelpunten vermeld voor de cultuur en methode kant.

Knelpunten aan de methodologische kant van risicogestuurd werken

- Het risicomanagement wordt vooral benut voor verantwoording (elk ministerie verwijst naar het Besluit BVA-stelsel Rijksdienst 2021. In het besluit wordt risicomanagement gedefinieerd als een verantwoordingsinstrument).
- De 'wettelijk' rijksbrede kader over TBB en risicomanagement is niet toegankelijk en gebruiksvriendelijk verwoord voor alle gebruikers, het is ontwikkeld door en voor deskundigen.
- Niet alle zes risicostappen worden uitgevoerd.
- Risico's worden niet altijd afgeleid door doelen.
- Er is geen uniforme risicotaal.

Tabel 17: Overzicht knelpunten aan de methode kant om risicogestuurd te werken

Knelpunten op gebied van cultuur

- Er wordt onvoldoende urgentie ervaren voor risicomanagement door het lijnmanagement 'risicomanagement is een corvee taak'.
- Het uitwisselen van risico-informatie is niet zelfsprekend. De lijnmanager heeft beperkte capaciteit, er moet aandacht geclaimd worden voor de onderwerpen TBB en risicomanagement.
- De corebusiness van de lijnmanager is uitvoering geven aan de kader/ beleid nota's en het managen van zijn team. Er is veel focus voor risico's op financiën en beleid. Risicomanagement en TBB zijn geen vast onderdeel van de managementtraining.
- Er zijn geen consequenties als de lijnmanager niet in control is bij TBB, we spreken elkaar niet aan.

Tabel 18: Overzicht van knelpunten aan de cultuur kant om risicogestuurd te werken

Op basis van de bovenstaande analyse van de knelpunten en aan de hand van de literatuurstudie zijn een aantal verschillen tussen het praktijkonderzoek en literatuurstudie benoemd in tabel 19. Deze vergelijkingen worden in paragraaf 4.2 meegenomen voor de Gap-analyse.

Praktijkonderzoek	Literatuurstudie
○ Risicomanagement bij integrale beveiliging wordt gezien als een verantwoordingsinstrument.	○ Uit de literatuurstudie blijkt 'risicomanagement doelgericht, expliciet, gestructureerd, communicerend en continu omgaan met risico's' is. Risicomanagement is een instrument die een organisatie kan gebruiken om haar 'strategische doelen te realiseren.
○ Er worden diverse definities gebruikt voor risicomanagement en risico.	○ Uit de literatuurstudie blijkt dat het aangeraden wordt om een uniform risicotaal te spreken anders is men veel tijd kwijt aan het oplossen van communicatiestoornissen.
○ Het lijnmanagement ziet niet altijd het nut van risicomanagement in,	○ Uit de literatuurstudie blijkt dat 80 % van de onderzochte organisaties haar strategische doelen

risicomanagement wordt gezien als een corvee taak.	niet realiseert. Een van de oorzaken is dat het management minder dan 1 uur per maand besteed om de strategische doelen te bespreken. ○ Risicoperceptie is een belangrijke element en bepaalt welk risicohouding men aan neemt en hoe risico's gemanaged worden.
○ Het begrip risicogestuurd werken wordt niet herkend in de praktijk. Onbewust zijn wel een aantal voorwaarden van risicogestuurd werken aanwezig bij de ministeries. Risicostappen beperken zich veelal tot identificeren, classificeren en rapporteren. En er is onvoldoende samenhang met risicomanagement en doelgerichtheid.	○ Uit de literatuurstudie blijkt dat risicogestuurd werken pas is geïmplementeerd als er cyclisch volgens de 4 G's wordt gewerkt (geformaliseerd, gestructureerd, geaccepteerd en geïntegreerd).

Tabel 19: Aandachtspunten uit de literatuurstudie en praktijkonderzoek

Deelconclusie: Er is discrepantie tussen de praktijk en theorie wereld van risicomanagement binnen de Rijksdienst. De onderzochte ministeries geven zelf aan dat ze in de reactieve fase bevinden. Er is onvoldoende basiskennis op bepaalde onderwerpen van risicomanagement.

4.2 Van Theorie en analyse naar ontwerpfase

In hoofdstuk één is het doel geformuleerd voor dit onderzoek.

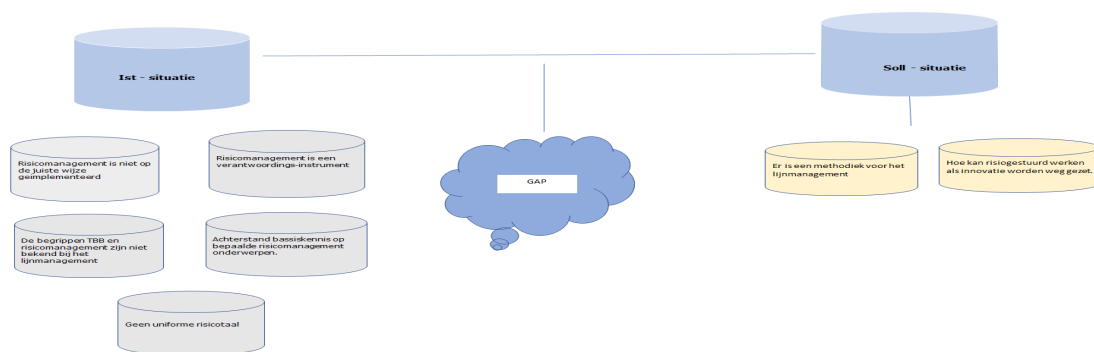
‘Ontwikkel een rijksbrede standaardmethodiek voor het lijnmanagement voor eenduidig en uniform risicomanagement in het kader van integrale beveiliging.

Om een oplossing te vinden voor dit probleem zijn een aantal deelvragen geformuleerd middels het DSRM-model. Voor deelvragen 1 en 2 is data verzameld uit de literatuur en documenten onderzoek. Voor deelvraag 3 is een praktijkonderzoek uitgevoerd. In de derde fase van het

DSRM-model wordt het artefact ontworpen om tot de gewenste resultaat te komen. Hiervoor is deelvraag vier geformuleerd:

Wat is nodig om verder een stap te maken naar risicogestuurd werken in de praktijk en welke aanpassingen zijn nodig om volgens de zes stappen van Van Staveren te werken?

Om van de huidige situatie (Ist-situatie) naar de gewenste situatie te gaan (Soll-situatie) dient eerst het verschil (Gap) bepaald te worden (figuur 22).



Figuur 22: Schematisch overzicht van Ist-situatie naar Soll-situatie

Wat is de Gap?

Om de gewenste situatie te bereiken dienen een aantal maatregelen getroffen te worden om de GAP te dichten. Aan de hand van de literatuurstudie, documenten- en praktijkonderzoek en tabel 17 op pagina 52/53 is gekeken welke handelingen en verbindingen ontbreken op het gebied van risicomanagement om de gewenste situatie te bereiken.

De volgende deelconclusies zijn:

- Er is onvoldoende samenhang tussen het risicomanagement en de **business** (lees: de primair processen of de kernprocessen van de organisatie).
- Er wordt niet volgens de 4 G's gewerkt hierdoor is risicomanagement is niet op de juiste wijze geïmplementeerd;

- Het risicomanagement wordt vooral benut voor verantwoording (achteraf) en nog onvoldoende als kans voor sturing richting doelen (vooraf);
- Bij het lijnmanagement ontbreekt basiskennis over risicomanagement en de basiskennis over TBB;
- Er wordt onvoldoende urgentie ervaren door het lijnmanagement om het risicomanagement (zelf) toe te passen, wellicht heeft dit te maken omdat er weinig mis gaat of het heeft er mee te maken dat men niet weet dat er dingen mis gaan.
- Er zijn diverse kaders en handreikingen ontworpen (hard controls). Een doorvertaling naar menselijk handelen en activiteiten (soft controls) ontbreekt.

Uit het vooronderzoek blijkt dat er voldoende geïnvesteerd is binnen de Rijksdienst aan de hard controls kant, maar het gewenste effect op het gedrag blijft achter. Hierdoor is er momenteel te weinig en wisselend draagvlak voor risicomanagement bij het lijnmanagement. Een ontwerp voor een methodiek voor het lijnmanagement gaat niet zondermeer het probleem oplossen en het gewenste effect opleveren. Gezien de bovenstaande deelconclusies is eerst een goede basis, zingeving en draagvlak voor risicomanagement en TBB nodig. Daarbij moet er niet alleen aandacht zijn voor hard controls maar ook voor soft controls. Uit het literatuuronderzoek blijkt dat de intentie de motivatie is dat een persoon het daadwerkelijke gedrag vertoont. De algemene regel hierbij is hoe sterker de intentie is, des te groter kans is dat het daadwerkelijke uitvoer van het daadwerkelijk gedrag gaat plaatsvinden. Dit is afhankelijk van de positieve- of negatieve beoordeling van de persoon, de subjectieve norm en de zelfeffectiviteit. Daarnaast speelt de bias en risicoperceptie ook hierin een rol.

Omdat er voldoende ontwikkeld is aan de hard control kant op het gebied van risicomanagement en TBB is gekozen om in de ontwerpen de nadruk te leggen op de soft controls zoals bewustwording en training zodat de medewerker/lijnmanagement begrijpen wat het nut en de noodzaak van risicomanagement is. Dit zodat de intentie en intrinsieke motivatie er is om risicomanagement toe te passen bij TBB. Deze aanpak levert ook een bijdrage aan de code van ambtelijk vakmanschap bij het ministerie van BZK (figuur 24). Daarnaast worden een aantal leervragen die de ADR in 2018 heeft meegekregen gedeeltelijk beantwoordt.



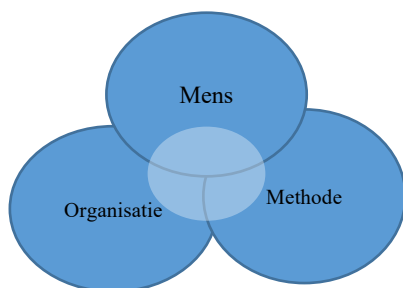
Figuur 23: Schematisch overzicht van de Code voor Ambtelijk vakmanschap van het ministerie van BZK)

Er zijn twee ontwerpen ontwikkeld. Het eerste ontwerp is gericht op de gedragsgerichte methode om bewustwording en draagvlak te creëren op het gebied van risicomanagement en TBB. Het tweede ontwerp is gericht op het menselijk gedrag en daarop invloed uit te oefenen zodat een aantal handelingen worden verricht.

4.3 Ontwerp

Om de ontwerpen vorm te geven, is er gebruik gemaakt van drie dimensies (methode, organisatie en mens). De methode gaat over kaders en bestaande werkprocessen. De mens gaat over competenties en vaardigheden en de organisatie gaat over formele structuur en cultuur. De methode en de organisatie zijn ondersteunend aan de mens (figuur 24).

In bijlagen 6 en 7 zijn de uitwerkingen van de ontwerpen 1 en 2 te vinden.



Figuur 24: Schematisch overzicht van de drie dimensies Mens, Organisatie en Methode.

De geïnterviewden hebben de volgende aanvullende ontwerpvereisten meegegeven (tabel 20).

Ontwerp wensen van de geïnterviewden	
○	Het lijnmanagement heeft weinig kennis over risicomanagement en TBB. De wens is dat er iets ontwikkeld wordt die het management helpt te begrijpen wat risicomanagement en TBB is.
○	De wens is ook dat inzichtelijk gemaakt wordt wat de voortgang is van integrale beveiliging. Het informatiestatuut voorziet momenteel niet in de behoefte.

Tabel 20: Overzicht van ontwerp wensen

In paragraaf 4.2 is aan gegeven dat er gewerkt wordt aan twee ontwerpen.

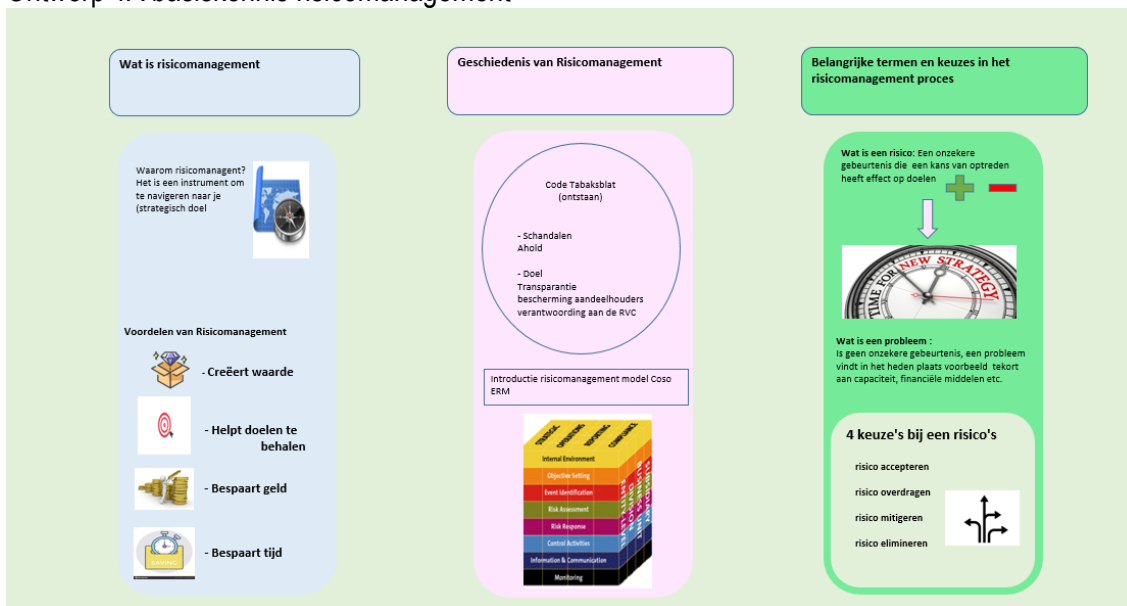
Omdat er ook wensen zijn over het informatiestatuut zal er een aantal aanbevelingen gedaan worden in paragraaf 5.1.

Ontwerp 1 Bewustwording training risicomanagement en TBB

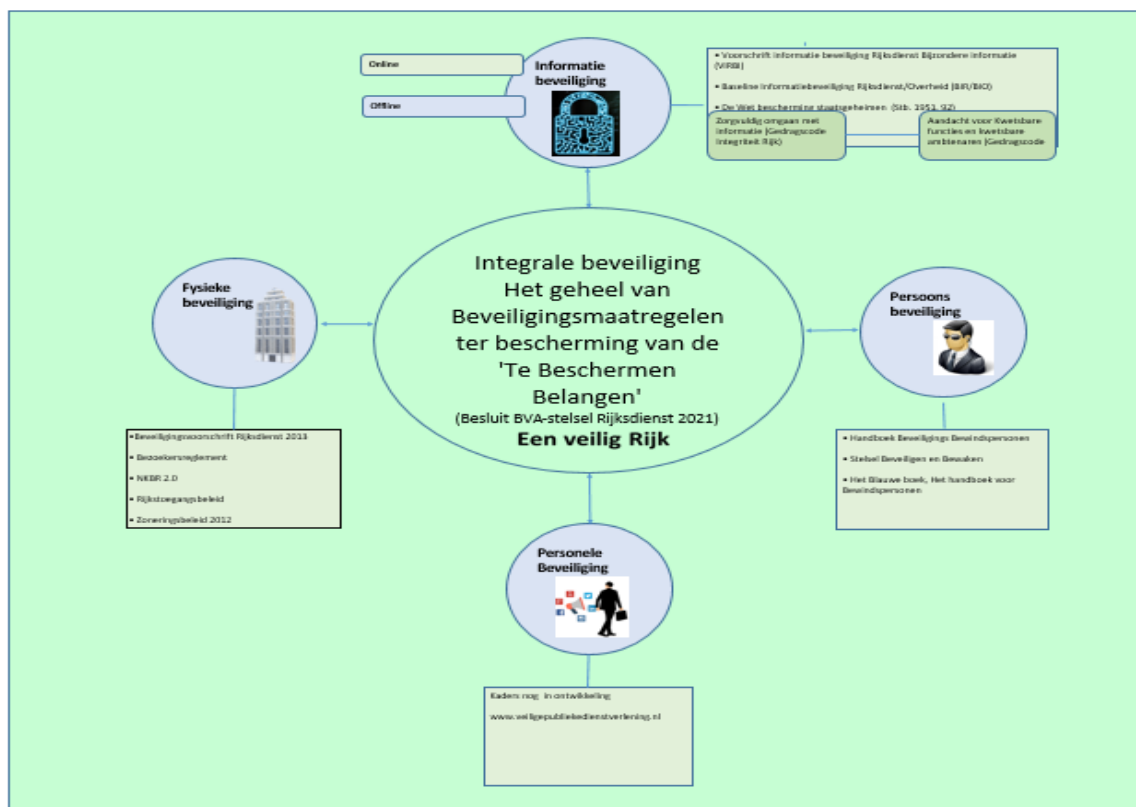
Ontwerp 1 bestaat uit ontwerpen 1A en 1B. beiden ontwerpen zijn gedragsgerichte methode om bewustwording en draagvlak te creëren. Ontwerp 1A is een hulpmiddel om bewustwording te creëren op het gebied van risicomanagement. Het ontwerp kan dienen als training of vooraf aan het risocanalyseproces worden ingezet. De meerwaarde van ontwerp 1A is dat duidelijk wordt dat risicomanagement geen verantwoordingsinstrument is. In het ontwerp staan ook de voordelen om risicomanagement toe te passen benoemd. Daarnaast staan een aantal belangrijke begrippen vermeld die een bijdrage leveren aan een uniform taalgebruik. Dit was ook een van de verbeterpunten die de ADR van respondenten had meegekregen in haar onderzoek.

Ontwerp 1B is gericht op het creëren van bewustwording wat onder het begrip TBB wordt verstaan. Het meerwaarde van het ontwerp is dat inzichtelijk maakt welke middelen onder TBB vallen. In het ontwerp wordt ook aangegeven welke belangrijke kaderdocumenten leidend zijn voor TBB.

Ontwerp 1A basiskennis risicomanagement



Ontwerp 1B basiskennis TBB



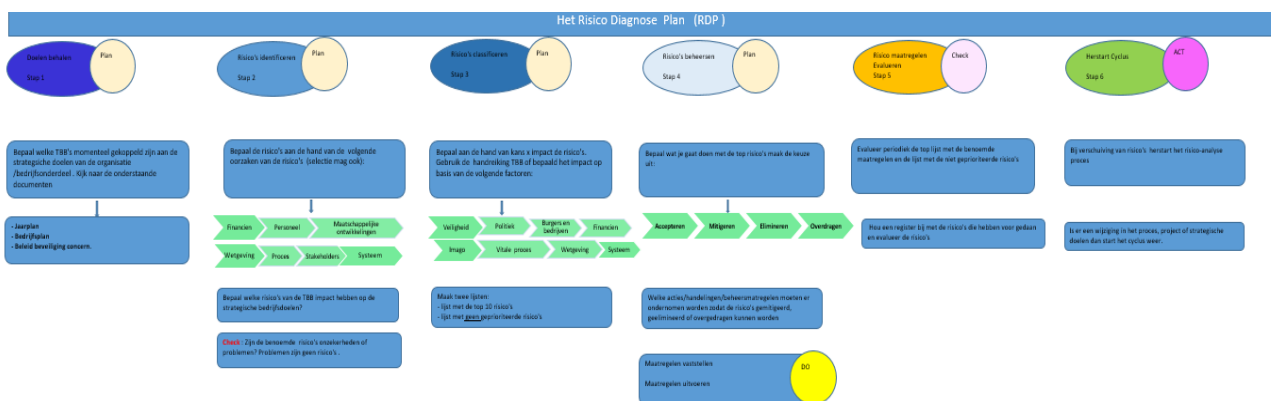
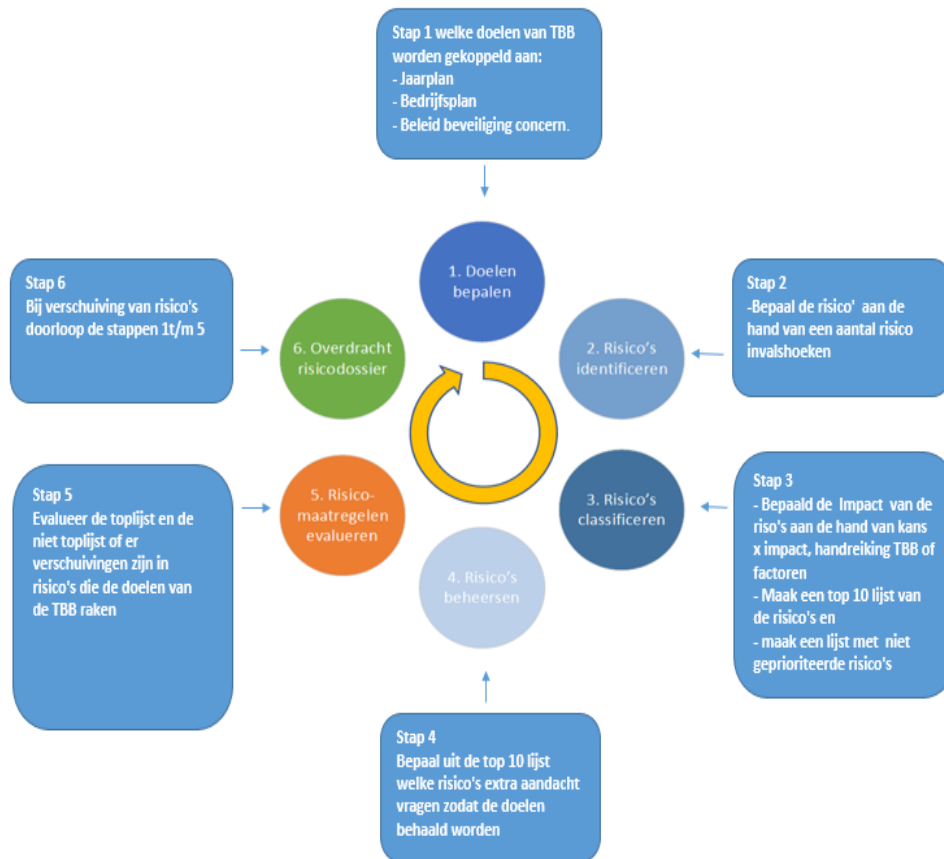
Ontwerp 2 het uniform risicomanagement model

Uit het literatuuronderzoek blijkt dat de PDCA-cyclus verweven zit in de risicoprocesstappen van diverse risicomanagementmodellen, ook in die van risicogestuurd werken (paragraaf 3.5).

In het tweede ontwerp worden de zes risicoprocesstappen van Van Staveren ingezet om invloed uit te oefenen op het menselijk gedrag. Door aan elke risicoprocesstap activiteiten/handelingen te verbinden wordt duidelijk wat bij elke stap nodig is of welke handeling verricht moet worden om over te gaan naar de volgende stap. De keuze is gemaakt om de belangrijkste basis activiteiten/handelingen te vermelden. Dit kan later door andere inzichten uitgebreid of gewijzigd worden. Bij deze keuze speelt ook mee dat één uniform ontwerp de diverse ministeries niet helpt i.v.m. de dynamische karakter en maatschappelijk taakveld van elk ministerie. Omdat risicoprocesstap 6 niet toepasbaar is in de praktijk wordt in het ontwerp risicoprocesstap 6 'overdracht risicodossier' vervangen naar 'Bij verschuiving van risico's dient men over te gaan naar stap 1'. Alle risicoprocesstappen dienen volgordeelijk toegepast/doorlopen te worden. Door de wijziging in processtap 6 door te voeren ontstaat er een generiek cyclisch proces voor risicomanagement die toepasbaar is in de praktijk niet alleen voor TBB. In Tabel 21 is een uitgebreide procesbeschrijving gemaakt van de risicoprocesstappen.



Figuur 1. De zes generieke risicoprocesstappen in de PDCA-cyclus



Procesbeschrijving Ontwerp 2

- Stap 1. Doelen bepalen
De doelen zijn altijd het uitgangspunt voor de risico-inventarisatie. Bij stap 1 wordt gevraagd welke doelen gerelateerd aan TBB behaald moeten worden. Hiervoor kan gekeken worden het jaarplan, bedrijfsplan, beleid concern.
- Stap 2 Risico's identificeren
De risico's dienen geïdentificeerd te worden aan de hand van een aantal risico invalshoeken financiën, personeel, maatschappelijke ontwikkelingen, wetgeving, proces, stakeholders systeem .Bij stap 2 dient bepaald te worden welke risico's impact hebben op de TBB doelen.
- Stap 3 Risico's classificeren
Aan de hand van de risico's dient bepaald te worden wat de impact is van de risico's op de doelen. Hiervoor kan de handreiking TBB gebruikt worden of de factoren veiligheid, politiek, burgers en bedrijven, financiën, imago, vitale processen, wetgeving en systeem. Maak aan de hand van de risico's twee lijsten. Een lijst met top 10 risico's en de tweede lijst met geen geprioriteerde risico's.
- Stap 4 Risico's beheersen
Bepaal welke risico's uit de top 10 lijst worden geaccepteerd, gemitigeerd, geëlimineerd en overgedragen. Verbind acties/maatregelen aan de risico's die gemitigeerd en geëlimineerd moeten worden. Als er commitment is voer dan de acties maatregelen uit. Dit valt onder de 'Do' van het risicomanagement proces.
- Stap 5 Risico maatregelen evalueren
Periodiek moet de top 10 lijst en de lijst met de niet geprioriteerde risico's geëvalueerd worden door de TBB-deskundige en de lijnmanager. Bij deze fase dient ook bij gehouden te worden welke risico's zich hebben voor gedaan.
- Stap 6 Bij verschuiving van risico's ga naar stap 1
Is er wijziging in de risico's dan dient het proces weer gestart te worden bij stap 1 met de lijnmanager en andere deskundigen.

Tabel 21: Uitwerking ontwerp 2 en procesbeschrijving



Meerwaarde Ontwerp 2

- Door per risicoprocesstap activiteiten/handelingen te verbinden en door stap 6 te vervangen ontstaat een cyclus die als uniform model ingezet kan worden voor het lijnmanagement, niet alleen voor TBB.
- Omdat de PDCA-cyclus verweven zit in zes risicoprocesstappen ontstaat er een verbetermethode richting risicogestuurd werken.
- Door activiteiten te verbinden met de risicoprocesstappen wordt ook de leervraag van de ADR voldaan 'Hoe integreer je risicomanagement in de P&C-cyclus'.

5 Validatie ontwerpen

Na de ontwerpfase dient in fase vier een demonstratie plaats te vinden en in fase vijf van het DSRM-model dient het ontwerp te worden gevalideerd. Voor deze activiteit is deelvraag 5 geformuleerd:

Biedt het ontwerp volgens expert voldoende basis om een stap te maken naar risicogestuurd werken?

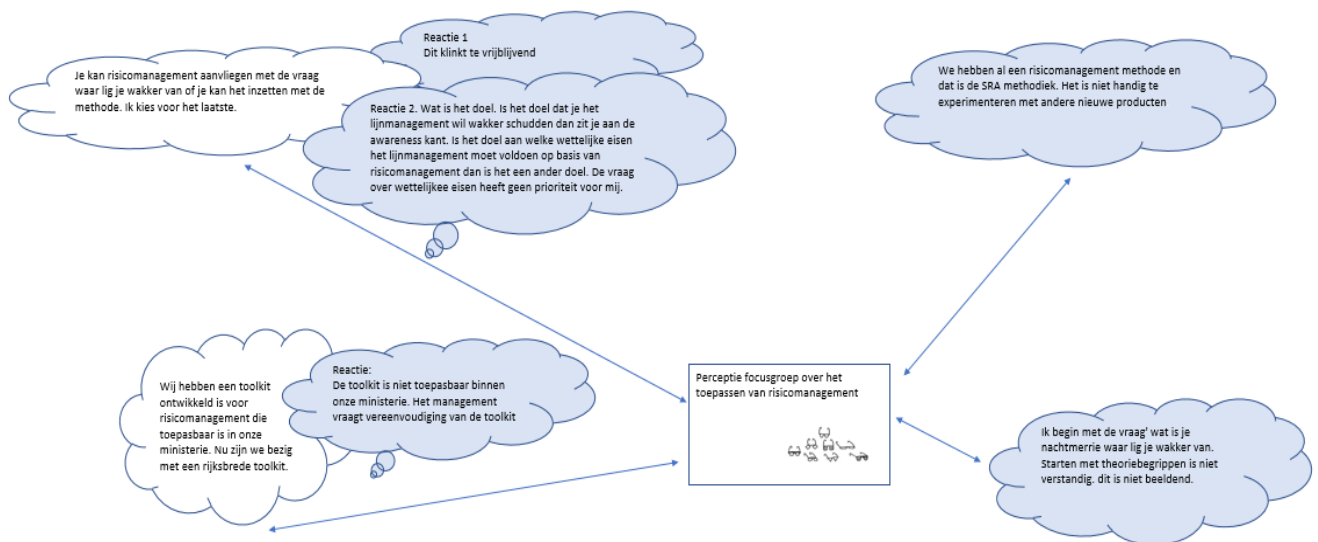
In dit onderzoek is gezien de onderzoeksperiode gekozen om de fasen 4 en 5 van het DSRM-model te combineren. Naast het ontwerp/ontwerpen is een procesbeschrijving toegevoegd worden waarin een aantal handelingen staan vermeld die volgordekelijk uitgevoerd dienen te worden. Dit kan gezien worden als een demo.

Om antwoord te vinden op deelvraag vijf zijn de opgedane inzichten en de ontworpen artefacten virtueel gevalideerd met de focusgroep in verband met COVID-19. Er is gekozen om met een focusgroep te werken omdat het een mooi instrument is om in korte tijd veel data te verzamelen. Het stappenplan van Van Asemma et al, 1992 is gebruikt om de focusgroep te organiseren (bijlage 8). Daarnaast is ook rekening gehouden met de nadelen van de methode. De deelnemers van de focusgroep zijn lid van de interdepartementale werkgroep risicomanagement en zijn allemaal deskundig op het gebied van integrale beveiliging. Deze interdepartementale werkgroep behandelt vraagstukken die betrekking hebben op het risicomanagement ten aanzien van integrale beveiliging binnen de Rijksdienst. De volgende ministeries hebben deelgenomen aan de focusgroep: het ministerie van Economische Zaken en Klimaat / Landbouw, Natuur en Voedselkwaliteit, het ministerie van Financiën, het ministerie van Infrastructuur en Waterstaat, het ministerie van Buitenlandse Zaken, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Justitie en Veiligheid, de Nederlandse Voedsel- en Warenautoriteit en de Rijksdienst voor ondernemend Nederland. De onderzoeker vervult de rol van groepsleider. Omdat de focusgroep beperkt beschikbaar is, is vooraf een e-mail verstuurd met de toelichting op de ontwerpen. Aan de focusgroep is gevraagd vooraf naar de ontwerpen te kijken. Dit zodat tijdens de focusgroep overleg gelijk gestart wordt met de beoordeling van de

ontwerpen op bruikbaarheid, gebruiksvriendelijkheid en toepasbaarheid. Er is maximaal 45 minuten uitgetrokken om de ontwerpen te valideren.

Resultaten validatie ontwerpen met de focusgroep

De ontwerpen, die als interventie dienen, zijn op 20 mei 2021 voorgelegd aan de focusgroep ter beoordeling inclusief toelichting. In bijlage 9 is een uitgebreide weergave van het verslag te vinden. Uit het literatuuronderzoek blijkt dat risicoperceptie en bias een belangrijk elementen zijn bij risicomanagement. Tijdens de evaluatie ontstond er een vergelijkingsproces over de kennis en kunde van risicomanagement. In figuur 25 is een schematisch overzicht gemaakt met een aantal bijzondere quotes. In de figuur staan ook reacties verwerkt die een aantal leden aan elkaar terug heeft gegeven.



Figuur 25: Bijzondere quotes van de focusgroep

Uit het gesprek met de leden van de focusgroep blijkt dat er verschillende aanpakken en ideeën zijn over risicomanagement. Er is ook gesproken over de reeds ontwikkelde producten en hoe de ontwerpen zich met elkaar verhouden. Een deel van de focusgroep begrijpt de opzet en ziet meerwaarde in de ontwerpen. Het andere deel ziet de ontwerpen als een heel nieuw model en

geven aan dat zij nog geen beeld hebben hoe de ontwerpen passen in het geheel van risicomanagement. Zij vragen meer tijd om tot een beoordeling te komen.

De suggestie is gedaan om de ontwerpen op te nemen in de rijksbrede toolkit risicomanagement. Deze toolkit is al in ontwikkeling en men vindt dat de ontwerpen op bepaalde vlakken overlap hebben. De meningen hierover zijn verdeeld. Een ministerie heeft de toolkit voorgelegd aan haar lijnmanagement ter toetsing voor toepassing in de praktijk. Het lijnmanagement heeft aangegeven dat de toolkit vereenvoudigd moet worden. De ontwerpen gemaakt door de onderzoeker zijn een vereenvoudiging. Een andere deelnemer reageert op de suggestie van de toolkit: "We moeten waken dat we geen dubbel werk gaan doen met de stukjes die we al hebben en we moeten waken dat we zelf niet communicatiestoornissen gaan veroorzaken. Dit omdat we denken dat de ontwerpen iets anders zijn terwijl de belangrijke elementen er wel in zit. Ik heb het gevoel dat de ontwerpen een verbindende schakel vormen richting het lijnmanagement.

Doordat de meningen zijn verdeeld en omdat de focusgroep als expertgroep risicomanagement functioneert voor het BVA-beraad, vraagt de projectleider de focusgroep het volgende te onderzoeken: "Tijdens het komende overleg, in juli 2021 wordt stilgestaan bij de overview. Hoe ziet het grote plaatje van risicomanagement eruit en welke producten/instrumenten zijn er opgeleverd voor welke doelgroep?" Daarnaast is gevraagd suggesties te doen hoe de ontwerpen gebruikt kunnen worden in de werkgroep. De intentie is om tijdens het overleg in juli tot een besluit te komen ten aanzien van de vervolgstappen voor de werkgroep gezien de managementopdracht die gekoppeld is aan dit vraagstuk.

Evaluatiegesprek met de opdrachtgevers/projectleiders.

Opdrachtgever 1 tevens projectleider

Op 20 mei 2021 heeft, direct na het overleg met de focusgroep, een kort evaluatiegesprek plaatsgevonden met projectleider 1. De projectleider geeft aan dat de aangeboden ontwerpen eigenlijk de basis vormen voor de overige ontwerpen. Deze hadden er al moeten zijn voordat de expertgroep aan het ontwerp van de overige producten begon. De projectleider geeft aan dat de vervolgvragen zijn geformuleerd om de opdracht verder te brengen.

Opdrachtgever 2 tevens projectleider

De projectleider geeft aan dat de uitkomsten uit het praktijkonderzoek herkenbaar zijn en begrijpt de reactie en de beleving van de focusgroep. Een gegeven is dat risicomanagement wordt uitgevoerd onder begeleiding van deskundigen van TBB, deze deskundigen begeleiden het management bij het maken van keuzes en het doel van TBB in kaart te brengen, te beschermen en schade te voorkomen. Bij de meeste departementen komt risicomanagement, plat gezegd neer op de eerste belangrijke stap van de beveiligingscyclus; het voorkomen van schade aan de kroonjuwelen. Dat is vooralsnog het belangrijkste. Deze beveiligingscyclus zal een tijd moeten draaien voordat ministeries verder kunnen evolueren naar hun fysieke risicomanagement. Financieel risicomanagement en risico-oriëntatie op de gehele bedrijfsvoering is vaak onderdeel van de Directie Financieel Economische Zaken (FEZ) en is goed ingericht. De aangeboden ontwerpen en aanpak zijn wel degelijk een toevoeging. Echter is deze voor veel departementen nu nog niet opportuun. Er is over het algemeen wat achterstand met het beveiligen van TBB en weinig aandacht van het management voor dit thema. Er is ook geen langdurige cyclus ingericht bij een aantal ministeries. De cyclus, waarbij de TBB's worden aangewezen en jaarlijks wordt doorlopen. Het bijbehorende volwassenheidsstadium moet eerst een aantal jaren doorlopen zijn om op orde te komen. De onderzoeker biedt ontwerpen aan wat die in de toekomst gebruikt kunnen worden voor verdere volwassenheid. Na de bijeenkomst met de focusgroep zijn er korte evaluatiegesprekken gevoerd met een aantal deelnemers over de bijeenkomst en ontwerpen, de reacties staan in bijlage 10 vermeld.

Deelconclusie:

- De meningen over de ontwerpen zijn verdeeld. Een aantal leden zien meerwaarde in de ontwerpen. Andere leden vinden de ontwerpen een nieuw model en zien nog niet de samenhang in het geheel. De focusgroep heeft nog meer tijd nodig om tot een beslissing te komen.
- De suggestie is gedaan vanuit het ministerie dat aan het praktijkonderzoek heeft deelgenomen om ontwerp 2 te vereenvoudigen en te verfijnen.

- Er is niet alleen een kloof tussen de 'academische wereld' en 'praktijk wereld' op het gebied van risicomanagement bij het lijnmanagement maar ook bij een aantal experts die het lijnmanagement adviseren.

5.1 Conclusies, vervolgonderzoek en aanbevelingen

Conclusies:

Dit rapport beschrijft het onderzoek wat is uitgevoerd om antwoord te vinden op de onderzoeksvraag 'ontwikkel een rijksbrede standaardmethodiek voor het lijnmanagement voor eenduidig en uniform risicomanagement in het kader van integrale beveiliging'. Om antwoord te vinden op het probleem zijn vijf deelvragen geformuleerd. Uit de deelvragen zijn twee ontwerpen voortgevloeid.

Om het risicomanagement proces goed te doorlopen komen naast de hard controls soft controls om de hoek kijken. Omdat uit eerdere onderzoeken blijkt dat de ontwikkelde kennis van informatie aan de hard controls kant over risicomanagement en TBB, niet automatisch tot het gewenst gedrag heeft geleid. Is ervoor gekozen om twee ontwerpen te ontwikkelen die gericht zijn op bewustwording en training, meer aan de soft controls kant. Deze aanpak is het geschikt omdat aan de hand van de soft controls men bij de medewerker tracht een situatie te creëren waarbij er gehandeld wordt naar de belangen van de organisatie. Relevante wetenschappelijke kennis van systemen en methodes van risicomanagement zijn vertaald naar bruikbare, concrete acties en veranderingen die in de praktijk toegepast kunnen worden voor en door het lijnmanagement.

Uit het literatuuronderzoek blijkt dat volgens het Gedragsmodel de '*Theory of planned behavior*' (Ajzen, 1991) dat motivatie een belangrijke factor is of een individu daadwerkelijk het gewenst gedrag uitvoert. Daarnaast geven verschillende wetenschappelijk onderzoekers aan dat uniform taalgebruik voor risicomanagement een van de succesfactoren is om in de praktijk toe te passen. Ook blijkt dat niet-deskundigen niet altijd de taal van de expert spreken.

De opdrachtgevers en een aantal leden van de focusgroep zien meer waarde in de ontwerpen. Uit de reactie van een van de projectleiders blijkt dat voor de Rijksdienst nog te vroeg is om met het gebruik van de ontwerpen te starten wegens "wat achterstand met het beveiligen van TBB" en het "ontbreken van een cyclus". Deze uitspraken trokken de aandacht. Door de ADR is in 2012 een eerste stap gezet met het onderzoek hoe risicomanagement in de praktijk is vormgegeven. In 2018 is het onderzoek herhaald waarbij de resultaten bijna gelijkwaardig waren met de resultaten uit 2012. Uit dit onderzoek blijkt dat er minimale stappen zijn gezet op het gebied van risicomanagement en risicogestuurd werken.

Door de bovenstaande uitspraken van de projectleider is de onderzoeker van mening dat dit onderzoek gekaderd/begrensd is. Omdat dit onderzoek breed opgepakt kan worden is omwille van de tijd niet gekeken naar gewoontes, houding en gedrag van medewerkers die de organisatiecultuur vormen. Tevens is de wijze van leiderschap, structuur en omgeving waarin de Rijksdienst opereert, niet in dit onderzoek meegenomen. Het lijkt erop dat er niet alleen transformatieproblemen zijn van theorie naar praktijk, maar dat er andere belemmerende factoren zijn binnen de Rijksdienst waardoor een aantal innovaties en ontwikkelingen moeizaam van de grond komen op het gebied van integrale beveiliging. Verder onderzoek is nodig omdat het ontwerp van een uniform methodiek niet voldoende is om het probleem op te lossen.

Eindconclusie: De voorgaande onderzoeken en dit onderzoek geven aan dat er minimale progressie is te zien op het gebied van risicomanagement en dat een aantal ministeries nog steeds reactief met integrale beveiliging bezig zijn. De ontwerpen kunnen een bijdrage leveren om de toepassing van risicomanagement te verbeteren binnen integrale beveiliging. Elke vernieuwing heeft tijd nodig om te rijpen. Echter er is wel vervolgonderzoek nodig. Het lijkt erop dat de Rijksdienst moeite heeft om te functioneren als een open organisatie. De cultuur en structuur van de organisatie kunnen een grote rol spelen en belemmerend werken bij het zetten van een stap voorwaarts op het gebied van integrale beveiliging. Er kunnen hiervoor diverse redenen zijn. Er is meer nodig dan alleen een uniform risicomanagement methodiek voor het organisatieprobleem.

Vervolgonderzoek:

De Rijksdienst is een open organisatie, die niet alleen te maken heeft met de VUCA-wereld maar ook met veeleisende burgers en bedrijven. Daft (2016) geeft aan dat open systemen bijzonder ingewikkeld zijn. De organisatie moet de benodigde middelen vinden, omgevingsveranderingen interpreteren en erop reageren, output distribueren en interne activiteiten beheersen, controleren terwijl de omgeving onzeker en turbulent is (Daft, 2016, p. 15). Daarnaast geven B. Johansen, 2012 en van Staveren 2018 (figuur 26) geven aan dat risico's managen in de VUCA-wereld een ander mindset, een andere vorm van 'leiderschaps' stijl en 'leiderschaps' vaardigheden vraagt.



Figuur 26: De competenties voor de Risicoleider (van Staveren, 2017)

Er hebben een aantal crisissen voorgedaan binnen de Rijksdienst waarbij het menselijke handelen een rol speelden. Enkele voorbeelden in 2021 zijn: De toeslagaffaire bij de Belastingdienst, het handelen van een minister die tijdens zijn bruiloft zijn eigen ontwikkelde regels ten aanzien van Covid-19 niet in acht nam en een minister die belangrijke geheime informatiestukken onder de arm naar buiten droeg waarbij de tekst leesbaar was. Deze handelingen hebben grote verontwaardiging in de maatschappij veroorzaakt. De vraag is dan ook of de Rijksdienst volledig verbonden is met de externe omgeving en daadwerkelijk kenmerken van een open systeem vertoont. Gezien de beperkingen van het onderzoek en de bovenstaande crisissen die hebben plaatsgevonden, is het advies de volgende vervolgonderzoeken op te starten:

- Onderzoek welke belemmerende factoren aan de cultuur en structuur kant de Gap veroorzaken tussen de academische- en praktijkwereld op het gebied van risicomanagement.
- Onderzoek hoe de Rijksdienst functioneert binnen de keten van integrale beveiliging (functioneert het als een open systeem en wat is de invloed van het politieke krachtenveld).
- Onderzoek welke leiderschapsstijl en vaardigheden nodig zijn op het gebied van integrale beveiliging om te kunnen opereren in een open systeem en VUCA-wereld.

Aanbevelingen om het proces verder te brengen:

Op basis van de conclusies in dit onderzoek kunnen een aantal concrete aanbevelingen gemaakt worden:

- Bevorder de rijpheid bij de interdepartementale werkgroep risicomanagement.
Binnen de interdepartementale werkgroep risicomanagement zijn een aantal risicomanagement experts aanwezig. Deze experts hebben dezelfde opleiding gevolgd als de onderzoeker en hebben ook jarenlange praktijkervaring. Binnen de werkgroep kunnen zij ingezet worden door de projectleiders om de rijpheid van risicomanagement te bevorderen. Hiervoor kunnen diverse themasessies belegd worden over de volgende onderwerpen: de recente ontwikkelingen van risicomanagement, het risicomanagement model versus de PDCA-cyclus, de hard en soft control kant bij risicomanagement.
- Organiseer themadagen voor risicomanagement bij Integrale beveiliging waarbij elk expert van de werkgroep wordt gevraagd een bijdrage te leveren.
- Nodig de ministeries met een maatschappelijk taakveld op het gebied van nationale veiligheid om kennis uit te wisselen.
- Er zijn twee ministeries gestart met een pilot risicogestuurd werken. Beide ministeries zijn bereid de best practices te delen op termijn (informatie en contactpersonen kunnen opgevraagd worden bij de onderzoeker).
- Het Besluit BVA-stelsel Rijksdienst 2021 geeft aan dat risicomanagement een verantwoordingsinstrument is. De recente ontwikkeling is dat risicomanagement een instrument is die ingezet kan worden om je doelen te bereiken. Tegenwoordig wordt risicomanagement ook succesmanagement genoemd. Het advies is de definitie te wijzigen in



Risicomanagement: is doelgericht, expliciet, gestructureerd, communicerend en continu omgaan met risico's (van Staveren 2015, p.60)

- Aangezien er wensen zijn over het informatiestatuut. Is het advies het informatiestatuut te evalueren in het BVA-beraad en het doel ervan vast te stellen. Is de wens het informatiestatuut als stuurinstrument in te zetten dan is het advies eerst key performance indicators (KPI) te benoemen die gerelateerd zijn aan de strategische doelen/jaarplan van het BVA-beraad. Daarnaast dient er een PDCA-cyclus ingebouwd te worden waarbij niet alleen wordt teruggeblikt, maar ook vooruit wordt gekeken.
- Als de Rijksdienst besluit om tot een implementatieplan over te gaan is het advies het Kotter's 8 stappen model voor verandermanagement toe te passen. In dit model staan de acht veranderstappen centraal die leiden tot het borgen van de veranderingen, zij bijlage 11 voor een korte toelichting over het model.
- Voer de bovenstaande vervolgonderzoeken uit.



Bijlagen

Bijlage 1 [Global Risk Management Survey 2019](#) De top 15 risico's wereldwijd

Risico's	2019	2017
Economische achteruitgang	1	2
Reputatieschade	2	1
Snel veranderende marktfactoren	3	38
Bedrijfsonderbreking	4	8
Toenemende concurrentie	5	3
Cyberaanvallen / datalekken	6	5
Grondstofprijzen	7	11
Cash flow / liquiditeitsrisico's	8	12
Onvoldoende Innovatief vermogen	9	6
Veranderende wet- en regelgeving	10	4
Aantrekken en behoud toptalent	11	7
Distributie en leveranciers	12	19
Kapitaal / kredietrisico	13	21
Disruptieve technologie	14	20
Politieke onzekerheid	15	9

Bijlage 2. Leervragen en praktijkvoorbeelden van verbeterpunten volgens de respondenten

Leervragen van de respondenten

Cultuur

1. Hoe meer draagvlak in de organisatie te creëren?
2. Hoe krijg je het (top)management mee?
3. Wat is nodig in de cultuur om het effectief te laten zijn?
4. Hoe houd je de aandacht vast voor risicomanagement?
5. Hoe als collegiaal bestuur, DG-overstijgend over risico's spreken?
6. Hoe krijg je het goede gesprek

Structuur

7. Hoe integreer je risicomanagement in de P&C-cyclus?
8. Hoe maak je de slag van risico-analyse naar risicomanagement?
9. Hoe sluit je risicomanagement van verschillende niveaus in de organisatie op elkaar aan?
10. Hoe is het risicomanagement bij andere ministeries ingericht?
11. Welke *best practices*/successen zijn er?

Methode

12. Welke risico indelingen kun je het beste gebruiken?
13. Welke *tooling* kun je het beste gebruiken?
14. Hoe kun je een *risklog* gebruiken?
15. Moeten we restrisico's concreet kunnen/willen maken?
16. Hoeveel inspanning moet je erin steken om risicomanagement te laten werken?

Praktijkvoorbeelden van verbeterpunten volgens de respondenten:

1. Onduidelijke, tegenstrijdige of niet voldoende gedragen doelstellingen (t.a.v. organisatie & beleid).
2. Lijnmanagement heeft geen gedeeld beeld over risicomanagement en de integratie in sturingsprocessen en overeenkomstig (voorbeeld)gedrag.
3. Het hoger management neemt te weinig tijd voor het bespreken van een departementsbrede risicoanalyse, de follow-up van de strategische risicoanalyse naar prioritering en beheersing schiet erbij in.
4. Nog geen gemeenschappelijke taal en begrippenkader over risico's en risicomanagement.
5. De kwaliteit van de risicoformulering laat te wensen over waardoor er te weinig focus komt in een risicosessie en aggregatie van risico's op departementaal niveau lastig is.
6. Met name strategische risico's worden soms op een te abstract niveau geformuleerd waardoor het eigenaarschap collectief blijft en daardoor onduidelijk.
7. Hoog knelpuntengehalte van de risico-inventarisatie, waardoor er een gevoel van herhaling ontstaat (de knelpunten zijn al geadresseerd in andere overleggen).
8. Teveel risico's in beeld gehouden.
9. Geen prioritering maken (keuzes maken) over risico's en beheersmaatregelen.



10. Te weinig aandacht voor samenhang tussen risico's van verschillende organisatieonderdelen in de analyse.



Bijlage 3 Overzicht Wettelijk/Rijksbreed Kader

Thema's	Wettelijk/Rijksbreed Kader
Algemene organisatie van Integrale Beveiliging	• Besluit BVA stelsel Rijksdienst 2021 (voorheen Beveiligingsvoorschrift Rijksdienst 2013), • Leidraad Te Beschermen Belangen (TBB), • Rijksbreed kaderdocument “ Risicomanagement Integrale Beveiliging”
Incidenten en/of bedreigingen	• Beveiligingsvoorschrift Rijksdienst 2013
Veiligheid van personeel (o.a. agressie en geweld tegen ambtenaren)	• Beveiligingsvoorschrift Rijksdienst 2013, Handreiking is in ontwikkeling
Fysieke beveiliging gebouwen	• Beveiligingsvoorschrift Rijksdienst 2013, Bezoekersreglement, NKBR 3.0, Rijkstoegangsbeleid, Zoneringsbeleid 2012,
Informatiebeveiliging	• Voorschrift Informatiebeveiliging Rijksdienst Bijzondere informatie (VIRBI) De wet bescherming staatsgeheimen (Stb.1951,92), Baseline Informatiebeveiliging Rijksdienst/overheid (BIR/BIO)
Integriteit	• Gedragscode Integriteit Rijk, CAO RIJK 2020, Leidraad aanwijzing vertrouwensfuncties, Personeelsreglement
Vertrouwensfuncties	• Leidraad aanwijzing vertrouwensfuncties, De Wet bescherming staatsgeheimen (Stb. 1951, 92), Wet Veiligheidsonderzoeken
Compliance	• CAO Rijk 2020,
Privacy en AVG	• Algemeen Verordening Gegevensbescherming, Leidraad aanwijzing vertrouwensfuncties, Uitwisseling persoonsgerelateerde beveiligingsinformatie



Business Continuïteit Management en Calamiteitenmanagement	• Business Continuïteit Management (BCM) (conform ISO22301 en de ISO High Level Structure)
---	--

Bijlage 4 15 voorwaarden van Van Staveren

Snelle inzage in voorwaarden aan risicogestuurd werken

Nr.	Voorwaarden aan de organisatiestructuur voor risicogestuurd werken	Aanwezig		
		1 Nee	2 Deels	3 Ja
1	Rollen, taken en verantwoordelijkheden voor risicosturing zijn formeel afgesproken.			
2	De beheersing van risico's is formeel gedelegeerd aan personen die dit als onderdeel van hun dagelijkse activiteiten kunnen doen.			
3	De beheersing van risico's wordt formeel gerapporteerd aan leidinggevenden en toezichthouders.			
4	Er zijn formele afspraken gemaakt om het werkproces van risicosturing aan te passen.			
5	Er is formeel afgesproken dat de externe omgeving van de organisatie bij het risicogestuurd werken wordt betrokken.			

Nr.	Voorwaarden aan de methode voor risicogestuurd werken	Aanwezig		
		1 Nee	2 Deels	3 Ja
1	De methode is beschikbaar en toegankelijk voor alle beoogde gebruikers.			
2	De beoogde gebruikers ervaren de methode als gebruiksvriendelijk.			
3	Gebruik van de methode levert relatief voordeel voor de beoogde gebruikers op.			
4	De methode sluit naadloos aan op de werkprocessen van de beoogde gebruikers.			
5	De kosten voor aanschaf, ontwikkeling en gebruik van de methode zijn acceptabel.			

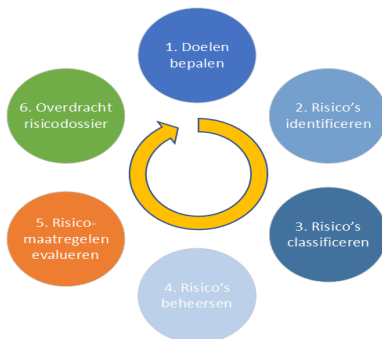
Nr.	Voorwaarden aan de organisatiecultuur voor risicogestuurd werken	Aanwezig		
		1 Nee	2 Deels	3 Ja
1	Binnen de hele organisatie worden eenduidige begrippen voor risicogestuurd werken gebruikt.			
2	Binnen de hele organisatie wordt beseft dat risico-inschattingen deels subjectief zijn.			
3	Binnen de hele organisatie worden verschillen in risicoperceptie en risicohouding expliciet besproken.			
4	Risicogestuurd werken wordt door samenwerking in multidisciplinaire teams met leden van binnen en buiten de organisatie uitgevoerd.			
5	Binnen de hele organisatie is uitwisselen van risico-informatie vanzelfsprekend.			



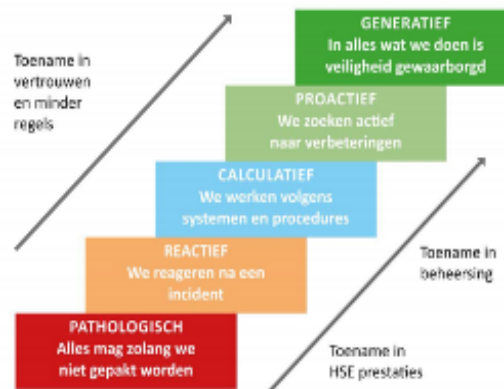
Bijlage 5 Interview vragen

1. Welke definitie voor risicomanagement wordt gehanteerd;
2. Welke definitie van risico wordt gehanteerd;
3. Hoe vindt het proces rond risicomanagementbeleid plaats (wordt er aandacht besteed aan de doelstelling, definitie van risico, risicoperceptie (hoe kijken we tegen risico aan) en risicotolerantie (wat is je risicobereidheid) en de samenstelling van het team waarmee de risicosessie wordt uitgevoerd)
4. Welke risicomanagement model wordt ingezet om de TBB-risico's in kaart te brengen;
5. Welke wettelijk/ rijksbreed kaders worden gebruikt om de TBB-en te classificeren;
6. Hoe wordt de Leidraad te beschermen belangen ervaren
7. Welk effect veroorzaakt de Leidraad te beschermen belangen in de praktijk en zijn er verbeterpunten;
8. Hoe vindt de of indeling van de TBB-risico's plaats in de praktijk (strategisch, tactisch, operationeel) en hoe bereiken de strategische en tactische risico's het lijnmanagement.
9. Welke processtappen (volgens de Demingcyclus van PDCA van Van Staveren) worden doorlopen in de praktijk om de TBB-en te classificeren.
10. Welke processtappen worden niet doorlopen volgens Demingcyclus van het PDCA van Van Staveren, is er een verklaring hiervoor.
11. Welke activiteiten zijn nodig om elke procestap van, Van Staveren te doorlopen op het gebied van TBB?
12. Welke skills hebben de deskundigen nodig om risicomanagement op het gebied TBB's verder te brengen in de organisatie.
13. Welke ontwikkeling maakt het kerndepartement op het gebied van risicomanagement en Te Beschermen Belangen momenteel (groeimodel Shell)

Model van Van Staveren
voor vragen 18, 19



Heart & Minds model voor
vraag 22



Veiligheidskultuurschijf - Bron: Hearts & Minds / Energy Institute



Bijlage 6 Ontwerp 1 volgens de drie dimensies (methode, organisatie en mens).

Ontwerp 1 Basiskennis risicomanagement en TBB	
○ Methode.	Ontwerp 1 is een gedragsgerichte methode om bewustwording en draagvlak te creëren doormiddel van training op het gebied van risicomanagement en TBB. Dit omdat uit het onderzoek blijkt dat er geen sence of urgency is voor risicomanagement en dat het begrip TBB onbekend is. In het ontwerp voor risicomanagement wordt ook een algemeen begrippenkader/één risicotaal gecreëerd. Het ontwerp kan in het proces in de voorfase ingezet worden maar ook in de uitvoeringsfase.
○ Mens	Door de voorbereidende cyclus te ontwerpen wordt er algemene kennis en vaardigheden voor risicomanagement ontwikkeld. Door aan de soft control te werken wordt de medewerker uitgedaagd een bepaalde houding/gedrag en handeling eigen te maken. Het ontwerp moet gebruiksvriendelijk zijn.
○ Organisatie	In de huidige cultuur is risico eigenaarschap vast gelegd in the three lines of defence model echter dit is niet merkbaar in het gedrag van het lijnmanagement. In een gezond bedrijf is er structureel aandacht voor risicomanagement. In het rapport zal de aanbeveling gedaan worden dat er een basistraining risicomanagement opgenomen dient te worden in de managementopleiding



Bijlage 7 Ontwerp 2 volgens de drie dimensies (methode, organisatie en mens).

Ontwerp 2 Zes risicoprocesstappen volgens het PDCA-cyclus	
○ Methode.	Per risicostap dient uitgelegd te worden welke handelingen verricht moet worden. Het proces dient helder, begrijpelijk en uitgelegd te worden. In dit ontwerp dient TBB ook gekoppeld te worden aan de cyclus zodat er een routinematig (samen)werken ontstaat.
○ Mens	Door het ontwerp aan te passen ontstaat er bewustwording en ook begrip waarom de TBB's beschermt dienen te worden en is het effect dat de samenwerking en begrip voor elkaars belangen versterkt wordt tussen deskundigen en het lijnmanagement. Het ontwerp moet gebruiksvriendelijk zijn
○ Organisatie	Zie opmerking bij ontwerp 1

Bijlage 8 Methodologische verantwoording stappenplan 'Van Asemma et al, 1992' focusgroep

Voorbereiding
Doel omschrijven
Randvoorwaarden vaststellen
Deelnemers kiezen/selectiecriteria bepalen
Aantal interviews bepalen
Omvang van de groepen bepalen
Vraagroute formuleren en voorleggen aan anderen
Gespreksleider kiezen/trainen
Ruimte regelen
Opname-apparatuur regelen
Vergoeding deelnemers regelen
Deelnemers werven
Groepen samenstellen
Deelname bevestigen
Uitvoering
Ontspannen sfeer creëren
Inleiding geven
Vraagroute doorlopen/discussie leiden
Aantekeningen en bandopnamen maken
Afsluiten
Uitwerking
Eerste indrukken opschrijven
Band uitschrijven
Resultaten samenvatten/coderen
Resultaten voorleggen aan anderen
Resultaten rapporteren

Schema 2 Stappenplan voor
de uitvoering van focusgroep-interviews

Voordelen	Nadelen
Eenvoudig	Weinig controle
Open	Moeilijk te analyseren
Interactief	Ervaren gespreksleider vereist
Flexibel	Niet voor controversieel onderwerp
Hoge 'face validity'	Geen statistische toetsing mogelijk
Relatief grote onderzoeksgroep	Beperkt generaliseerbaar
	Werven deelnemers mogelijk probleem

Schema 1
Voor- en nadelen van de
focusgroep-methode

Bijlage 9 Verslag focusgroep

Bijlage

Op 20 mei 2021 is er is eerst een toelichting gegeven over het onderzoek voordat er met de focusgroep naar de ontwerpen is gekeken. Daarnaast geeft de onderzoeker aan welke uitkomsten uit het onderzoek zijn gebruikt om tot de ontwerpen te komen. De onderzoeker benadrukt dat de ontwerpen gemaakt is voor het lijnmanagement en gericht is op bewustwording en training. De focusgroep heeft naar de ontwerpen gekeken en hebben de volgende reacties gegeven op de ontwerpen: De ministeries zijn geanonimiseerd met A, B, C, D, E en F. Het gesprek is opgenomen en na verslaglegging verwijderd.

Reactie van de focusgroep

- Binnen ministerie A wordt bewustwording van het management al meegenomen in de risicoanalyse. Ik snap wat je wil bereiken maar dit is al in werking gezet. Als men wil dat er stappen worden gezet op het gebied van risicomanagement dan is de tip dat de ministeries gebruik maakt wat de werkgroep heeft ontwikkeld en verstuurd. De afspraak is dat we werken met de rijksbrede Security Risk Assessment risicoanalysemethodiek (SRA). Experimenteren met andere nieuwe producten is niet handig.
- Ministerie B geeft aan dat het niet verstandig is met de theoriebegrippen te starten. Ministerie B meldt dat in workshopsessies gestart wordt met de vraag 'wat is je nachtmerrie, waar lig je wakker van'. Aan de hand van deze vraag is de ervaring dat een gesprek tot stand komt en dat het helpt inschatting te maken van risico's die plaatsvindt of gaat vinden. Volgens ministerie B is risicomanagement 'het investeren/nemen van maatregelen om dat je bang bent dat je iets overkomt dat je werk kan beïnvloeden'. Dit werkt beeldend en dit is risicomanagement. De crux zit hoe benader je als expert het management. De vraag 'waar lig je wakker van' kan de theorie aanvullen.
- Ministerie C meldt dat je risicomanagement op 2 manieren kan benaderen. Je kan het aanvliegen met de vraag 'waar lig je wakker of wat is je nachtmerrie' om het proces te starten. Of



je kan een risicomangentmethodiek gebruiken om het proces te starten voor draagvlak. De tweede optie werkt bij ministerie C tot op heden het best.

- Op de reactie van ministerie C geeft ministerie A aan dat de gekozen aanpak te vrijblijvend klinkt. Ministerie B vindt dat de vraag moet zijn wat je wil bereiken. Is het doel dat je het lijnmanagement wil wakker schudden dan zit je aan de awareness kant. Is het doel aan welke wettelijke eisen het lijnmanagement moet voldoen op basis van risicomangement dan is dat een ander doel. Bij ministerie B heeft de vraag over de wettelijke eisen geen prioriteit. Het is verstandig om te starten wat vast te grijpen is bij risicomangement wat het voor je betekent voordat aan je aan de eisen van risicomangement start. Je moet denken dat meerdere doelen bereikt kunnen worden door meerdere instrumenten in te zetten.

- Ministerie D geeft aan dat risicomangement gaat over het beheersen en bereiken van je doelstellingen. TBB gaat over het beveiligen van de TBB-middelen om de doelstelling te kunnen bereiken. De crux is het maken van verbinding met het lijnmanagement want hij/zij moet zorgen dat de doelen bereikt worden. Om de doelen te bereiken moeten de TBB in de smiezen houden. Dan krijg je een piramide wat je moet beheersen. Dat is inherent aan het managementproces.

- Ministerie E geeft aan dat het ministerie bezig is met de ontwikkeling van een toolkit voor risicomangement. Dit toolkit is ontwikkeld voor het lijnmanagement en medewerkers die weinig kennis hebben van risicomangement en TBB. De ontwerpen vertonen overlap met de toolkit. Misschien moeten de ontwerpen geïntegreerd worden in de toolkit. Het is niet verstandig diverse producten naast elkaar te hebben. De ADR heeft meegekeken en er is een toets gedaan bij het lijnmanagement (geen brede toets). Het lijnmanagement geeft aan dat de toolkit begrijpelijk opgesteld is en werkbaar is voor deze ministerie. We moeten geen meerdere producten naast elkaar willen hebben, het beste is te werken naar 1 product.

- Ministerie D geeft aan dat er geen zorgen moeten zijn over de ontwikkelde producten. Alles wat tot nu toe ontwikkeld is sluit aan met ISO 31.000. We moeten waken dat we geen dubbele werk gaan doen met de stukjes die we al hebben en we moeten waken dat we zelf niet

communicatiestoornissen gaan veroorzaken. Dit omdat we denken dat de ontwerpen iets anders zijn terwijl de belangrijke elementen er wel in zit. Ik heb het gevoel dat de ontwerpen een verbindende schakel vormen.

Ministerie F geeft ministerie E terug dat de ontwerpen een vereenvoudiging zijn van TBB en risicomanagement. Omdat de toolkit eerder is gedeeld met de werkgroep heeft ministerie F gevraagd aan haar lijnmanagement om de toolkit te beoordelen. Het lijnmanagement heeft teruggegeven dat de toolkit te ingewikkeld is om ermee te werken. Ministerie F geeft aan dat men goed voor ogen moet hebben dat je het zo eenvoudig mogelijk maakt voor het lijnmanagement. Ministerie F is bezig om de toolkit te vereenvoudigen voor haar lijnmanagement. Ministerie E geeft aan als we een rijksbrede toolkit willen dat alle ministeries ernaar moet kijken. Ministerie B merkt op dat sommige rijksbrede kaders/handreikingen soms verder uitgewerkt moeten worden om het passend te maken voor een ministerie. Dit is afhankelijk van je doelgroep en cultuur van de organisatie. Daarom is het verstandig naar de doelgroep te kijken wil je met wat met je experts of lijnmanagement voor je ministerie. Het gevaar is dat je allerlei ontwerpen ontwikkeld met veel energie en achteraf blijkt het dat de ontwerpen niet toepasbaar is en niet aansluit bij de doelgroep. Dit is zonde.

Gezien de bovenstaande reacties en omdat de gereserveerde tijd eindigt is het volgende afgesproken.

-De projectleider geeft aan dat het goed is bij het volgend overleg stil te staan wat het grote plaatje is en dan te kijken welke producten/instrumenten zijn opgeleverd voor welke doelgroep. Daarnaast is de vraag aan de focusgroep 'hoe ziet eenieder de ontwerpen hoe kunnen deze gebruikt worden in de werkgroep'. Dit zodat we het volgend overleg een besluit kunnen nemen. Er ligt een management vraagstuk waar aan gehoor gegeven moet worden. Omdat de onderzoeksvraag niet meer helder is, is aan de onderzoeker gevraagd de onderzoeksvraag en het doel te delen met de werkgroep.

Reactie van de onderzoeker op de gestelde vragen en aandachtspunten



- De ontwerpen zijn gemaakt voor het lijnmanagement. De ontwerpen kunnen ook ingezet worden bij medewerkers die niet veel affiniteit met risicomanagement hebben.
- De ontwerpen zijn geen nieuwe risicomanagementmodellen. De ISO 31.000 is als uitgangspunt genomen waarin de PDCA-cyclus in verweven zit. Afgesproken is in het kaderdocument (die de werkgroep ontworpen heeft in 2020) dat de ISO 31.000 en de COSO-ERM risicomanagementmodellen zijn die we inzetten binnen de Rijksdienst. Er zijn handelingen en activiteiten gekoppeld aan de PDCA-cyclus en de zesde risicostap is vervangen zodat er een cyclisch proces ontstaat die ingezet kan worden als uniform model.
- Het is belangrijk om uniforme risicomanagement taalgebruik te hebben om miscommunicatie te voorkomen. Een risico is geen probleem!
- Het is belangrijk om je doelgroep te differentiëren bij het ontwikkelen voor je producten, 'one size fits' all is niet de oplossing. Hier was de doelgroep het lijnmanagement.
- De opdracht van 2017 is dat er een uniform model komt voor het lijnmanagement. Dat was de opdracht die in 2017 geformuleerd is en er was nog geen invulling aangegeven aan de vraag. Dit heeft de onderzoeker opgepakt als haar afstudeeropdracht in afstemming met de BVA Rijk en de projectleiders van dit werkgroep.
- De ontwerpen die zijn gemaakt vullen de overige ontwerpen aan, het begint met de basis en dan komen de overige ontwerpen. Nogmaals de ontworpen initiatieven vullen de overige gemaakt ontwerpen aan ze bijten elkaar niet. De doelgroep van de onderzoeker is het lijnmanagement geweest de overige ontwerpen die gemaakt zijn, zijn voor de experts.

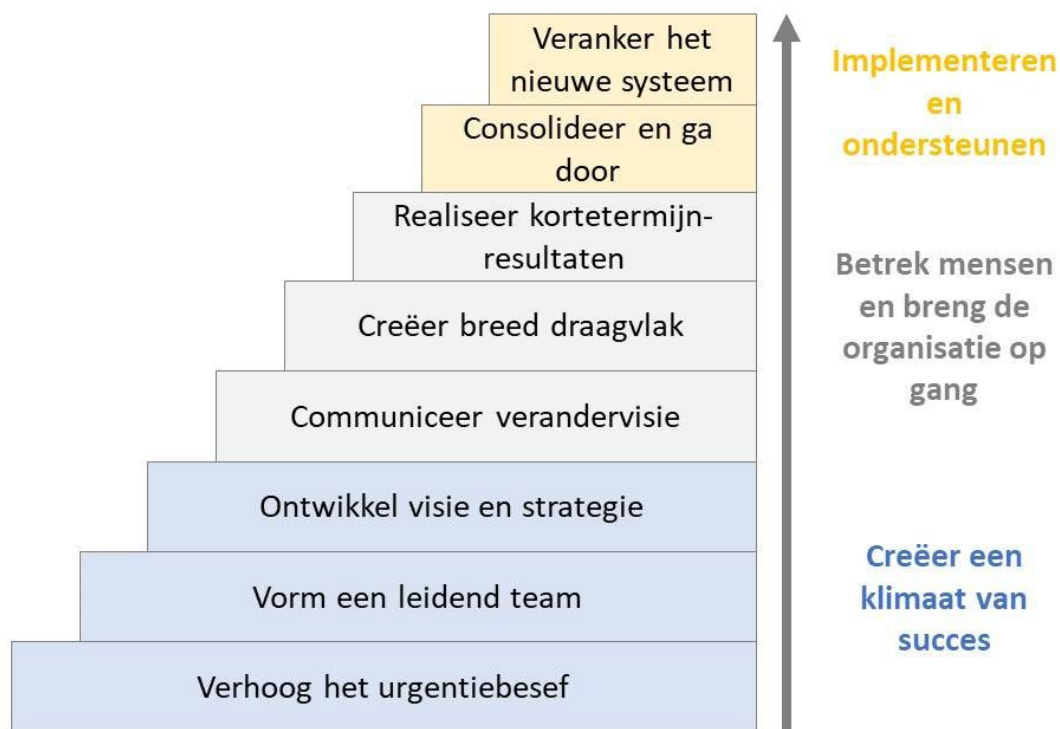


Bijlage 10 Evaluatiegesprek deelnemers focusgroep

Evaluatiegesprek deelnemers focusgroep

- Na het overleg met de focusgroep heeft op 24 juni 2021 een korte evaluatie plaatsgevonden met twee deelnemers van de focusgroep via de telefoon. Beide deelnemers gaven afzonderlijk aan dat de toelichting duidelijk was en dat ze wel toegevoegde waarde zien in de ontwerpen. Tegelijkertijd gaven ze terug dat goed te merken was tijdens de bijeenkomst met de focusgroep dat iedereen een eigen beleving heeft wat risicomanagement is, uniform taal voor risicomanagement ontbreekt binnen de expertgroep.
- Een aantal dagen na de bijeenkomst van de focusgroep belde een deelnemer van de focusgroep dat ze graag meer toelichting wilde over de ontwerpen. De toelichting is gegeven door de onderzoeker. De deelnemer gaf aan dat ze de samenhang met risicomanagement en soft- en hard controls en uniform taalgebruik niet ziet. Ze kiest voor haar eigen aanpak binnen het ministerie.
- Het ministerie die een bijdrage heeft geleverd aan het praktijkonderzoek heeft als suggestie meegegeven om ontwerp 2 te vereenvoudigen. De wens is dat voor elk risicoprocesstap per op een pagina toelichting wordt gegeven. De interviewer van het ministerie wil bij vervolgoopdracht hiervoor wel suggesties aandragen.

Bijlage 11 Het verandermodel van Kotter



De eerste drie stappen zijn gericht om de juiste klimaat te creëren

De vierde tot de zesde stappen zijn gericht om draagvlak te creëren in de organisatie

De zevende en achtste stappen zijn gericht om de implementatie in werking te zetten.



Bronvermelding

Aven, T. (2015). *Risk analyses*. John Wiley & Sons Ltd

Appelman, A (2010). *Integrale Beveiliging; Een security management system in 7 stappen*.
Wolters Kluwer / Vakmedianet

Ajzen, I. (1991). The Theory of Planned Behavior.
https://www.researchgate.net/publication/272790646_The_Theory_of_Planned_Behavior/link/5d508e5ba6fdcc370a8ec4ca/download

Baarda, D., Goede, M (2006). *Basisboek Methoden en Technieken*. Wolters- Noordhoff
Groningen/Houten

Baseline Informatiebeveiliging Overheid versie 1.04 Staatscourant 2020, 7857

Bernstein, P (1996). *Against the Gods: The Remarkable Story Of Risk*. John Wiley & Sons, INC

Besluit BVA stelsel Rijksdienst 2021, Staatscourant. 2020, 62845, nr 1

Daft, R. (2016), *Organisatietheorie en- ontwerp*. Boom uitgevers Amsterdam,

De Auditdienst Rijk, *Inventarisatie risicomanagementpraktijken bij het Rijk*, 2018

De Auditdienst Rijk, *Risicomanagementproces integrale beveiliging*, 2018

Griffin, D., Kahneman D. (2002) *Heuristics and biases: The psychology of Inuitive Judgement*.
Cambridge University Press

Gutteling, J. M. (2017). *Determinanten van risicoperceptie*. Geraadpleegd van
https://scholar.google.com/scholar?hl=nl&as_sdt=0%2C5&q=bias+risicowereld&btnG=.

Het circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten
2019, Staatscourant. 2019, 39608



Hopkin, P. (2017). *Fundamentals of Risk Management : Understanding, evaluating and implementing effective risk management*. Kogan Page Limited

Hoogendonk, M (2018) *Uitwerking ICBR-opdracht Jaarplan IBR, 2018*

Johanson, B, *Leaders make the future. TenNnew Leadership Skills for an Uncertain World*

Berett-Koehler Publishers Inc

[https://books.google.nl/books?id=Njzf-](https://books.google.nl/books?id=Njzf-HyOsHUC&pg=PR2&lpg=PR2&dq=Bob+Johansen+geeft+in+zijn+boek+Leaders+Make+the+Future&source=bl&ots=EcZIIYFYZb&sig=ACfU3U1UH6nwM1roW_IGQo3stp_puZJaIA&hl=nl&sa=X&ved=2ahUKEwiso9v1spXxAhULqBQKHYSXDDoQ6AEwEnoECAQQA#v=onepage&q=Bob%20Johansen%20geeft%20in%20zijn%20boek%20Leaders%20Make%20the%20Future&f=false)

[HyOsHUC&pg=PR2&lpg=PR2&dq=Bob+Johansen+geeft+in+zijn+boek+Leaders+Make+the+Future&source=bl&ots=EcZIIYFYZb&sig=ACfU3U1UH6nwM1roW_IGQo3stp_puZJaIA&hl=nl&sa=X&ved=2ahUKEwiso9v1spXxAhULqBQKHYSXDDoQ6AEwEnoECAQQA#v=onepage&q=Bob%20Johansen%20geeft%20in%20zijn%20boek%20Leaders%20Make%20the%20Future&f=false](https://books.google.nl/books?id=Njzf-HyOsHUC&pg=PR2&lpg=PR2&dq=Bob+Johansen+geeft+in+zijn+boek+Leaders+Make+the+Future&source=bl&ots=EcZIIYFYZb&sig=ACfU3U1UH6nwM1roW_IGQo3stp_puZJaIA&hl=nl&sa=X&ved=2ahUKEwiso9v1spXxAhULqBQKHYSXDDoQ6AEwEnoECAQQA#v=onepage&q=Bob%20Johansen%20geeft%20in%20zijn%20boek%20Leaders%20Make%20the%20Future&f=false)

Kahneman, D. (2016). *Ons feilbare denken* (26ste editie). Amsterdam / Antwerpen: Business Contact.

Kotter, J (2008). *Leiderschap bij verandering*. Sdu Uitgevers bv

Leidraad Te Beschermen Belangen, 2015

Nen-ISO-31000-2018

<https://www.nen.nl/nen-iso-31000-2018-nl-259009>

Robert S, Kaplan B. (2013) *The Strategy Execution System*. Harvard Business school

Renn, O., Klinke, A., & Van Asselt, M. (2011). *Coping with complexity, uncertainty and ambiguity in risk governance: A synthesis*. *Ambio*. <https://doi.org/10.1007/s13280-010-0134-0>

Rijksbreed kaderdocument 'Risicomanagement integrale beveiliging 'Goed risicomanagement geeft vertrouwen', 2020

Slovic, P, (1987), Perception of risk.

https://www.researchgate.net/publication/271767726_Perception_of_Risk

Staveren, M. van (2015). *Risicogestuurd werken in de praktijk*. Deventer Vakmedianet



Staveren, M. van (2018). *Risicoleiderschap. Doelgericht omgaan met onzekerheden*. Amsterdam University Press

Stol, W., & Tielenburg, C. (2011). *Boom studieboeken criminologie - Basisboek integrale veiligheid*. Boom Lemma.

Tiemijer, W. (2010). *Hoe mensen Keuzes maken: De psychologie van beslissen*. Amsterdam University Press

'T Hart, R. (2021, 23 april). *'Three Lines of Defense' risicomangement model*.
<https://robertthart.risicomangement.nl/2019/03/23/three-lines-of-defense-risicomangement-model/>

Verschuren, P., Doorewaard, H. (2015). *Het ontwerpen van een onderzoek*. Utrecht/ Boom/Lemma

Waal, D (2019) *Inleiding Risicomangement*. Coutinho

Lijst met figuren

Figuurnummer	Onderwerp	pagina
Figuur 1	De 12 ministeries binnen de Rijksdienst	14
Figuur 2	Overzicht TBB	15
Figuur 3	Besluitvormingsstructuur van Rijksbrede Bedrijfsvoering	15
Figuur 4	COSO-ERM (Bron ministerie van EZK/LNV)	16
Figuur 5	The Three Lines Model van het IIA, die binnen de Rijksdienst wordt toegepast	17
Figuur 6	Oorzaak- en gevolg diagram	20
Figuur 7	Model problem solving cycle	23
Figuur 8	Het DSRM-model	23
Figuur 9	Schematische weergaven fases DRSM versus onderzoeksmethoden	28
Figuur 10	Schematische weergave deelvragen versus fases van het DRSM-model	29
Figuur 11	Model voor systematisch gericht literatuuronderzoek (bron Frank & Hatak, 2013)	30
Figuur 12	Overzicht van vier belangrijke oorzaken waarom een organisatie haar doelen niet realiseert (bron, Kaplan, 2013)	34
Figuur 13	Overzicht dat laat zien dat er een overlap zit tussen veiligheid en beveiliging (bron A.Appelman)	37
Figuur 14	Overzicht wat onder safety en security wordt verstaan	37
Figuur 15	De zes risicostappen in het PDCA-cyclus	39
Figuur 16	Overzicht van de 4G's	40
Figuur 17	Overzicht van vierlagen van risicoperceptie (bron Renn en Rohrmann, 2000)	42
Figuur 18	The theory of planned behavior (bron I. Azjen, 1985)	44
Figuur 19	Schematisch overzicht van factoren die de risicoperceptie bepalen, hoe informatieverwerking plaatsvindt en welke risicohouding wordt aangenomen (bron R. Bhadjan, 2021)	46
Figuur 20	Volwassenheidsmodel van Shell (bron Hudson, Parker & van de Graaf, 2002)	49
Figuur 21	weergave van het praktijkonderzoek	49
Figuur 22	Schematisch overzicht om de Gap te bepalen	54
Figuur 23	Schematisch overzicht van de Code voor Ambtelijk vakmanschap van het ministerie van BZK)	56
Figuur 24	Schematisch overzicht van Mens, Organisatie en Methode die gebruikt wordt om te ontwerpen	56
Figuur 25	Schematisch overzicht met bijzondere quotes	64
Figuur 26	Competenties voor risicoleiderschap	69

Lijst met tabellen

Tabel nr	Onderwerp	pagina
Tabel 1	Conclusies van de ADR uit het onderzoek 1	19
Tabel 2	Conclusies van de ADR uit het onderzoek 2	19
Tabel 3	Deelvragen met inzichten	25
Tabel 4	Onderzoeksmethoden	25
Tabel 5	Aangereikte literatuur door de Universiteit van Twente	30
Tabel 6	Overzicht onderzoekstermen voor deelvraag 1A	31
Tabel 7	Overzicht gevonden onderzoeksrapporten in database	32
Tabel 8	Onderzoeksrapporten die gebruikt zijn in dit onderzoek	32
Tabel 9	Overzicht van verschillende definities van risico (bron S. Hannsson ,2004)	33
Tabel 10	Overzicht onderzoekstermen voor deelvraag 1B	37
Tabel 11	Overzicht onderzoeksrapporten in database	38
Tabel 12	Onderzoeksrapporten die gebruikt zijn in dit rapport	38
Tabel 13	Overeenkomst risicoprocestappen (bron van Staveren,2015 p.70)	39
Tabel 14	Kenmerken conventioneel risicomanagement versus kenmerken van Risicogestuurd werken (bron van Staveren, 2015 p. 33)	40
Tabel 15	Determinanten die een rol spelen bij risicoperceptie (bron Gutteling 2014)	43
Tabel 16	Overzicht van aanwezige elementen op het gebied van risicogestuurd werken.	50/51
Tabel 17	Overzicht van knelpunten aan de methode kant	51
Tabel 18	Overzicht van knelpunten aan de cultuur kant	52
Tabel 19	Overzicht verschillen tussen literatuurstudie en praktijkonderzoek	53
Tabel 20	Ontwerp eisen	57
Tabel 21	Uitwerking ontwerp 2 en procesbeschrijving	61



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties