“Van inzicht tot beheersing: Cybersecurity risico’s bij de Koninklijke Marechaussee”

Een ontwerponderzoek naar een risicomanagement benadering voor de Koninklijke Marechaussee waarmee de organisatie in staat wordt gesteld effectief en efficiënt risicomanagement toe te passen op cybersecurity risico.

Masterthesis Risicomanagement

Vincent Bijlard

Datum publicatie 14-Juni-2023

Masterthesis Risicomanagement cohort 10

Vincent Bijlard

Datum publicatie 14-Juni-2023

Wetenschappelijke begeleidingscommissie

Dr. Ir. M. Th. (Martin) van Staveren

Prof. Dr. Ir. J.I.M. (Joop) Halman

Universiteit Twente

Drienerlolaan 5

7522 NB Enschede

Opdrachtgever

Ministerie van Defensie

Koninklijke Marechaussee

Plein Kalvermarkt Complex, Kalvermarkt 32, 2411 CB Den Haag

Cybersecurity is een vertrouwelijk onderwerp binnen de Koninklijke Marechaussee (KMar). Ten slotte brengt de publieke bekendheid van beleid en procedures risico's met zich mee. Er zijn daarom twee versies van dit rapport geschreven: Een vertrouwelijke versie voor de KMar en de begeleidingscommissie van de Universiteit Twente en een ongerubriceerde versie die openbaar zal worden gepubliceerd.

Dit is de publieke versie van het rapport, de uitwerking van de interviews en enkele vertrouwelijke passages zijn verwijderd.

Voorwoord

Geachte lezer,

Voor u ligt mijn masterthesis ter afronding van de Master Risicomanagement aan de faculteit Behavioural Management and Social Sciences van de Universiteit Twente. De masteropleiding heeft mij geleerd hoe ik als leidinggevende bij de overheid op een gestructureerde wijze risico's kan beheersen. Het volgen van uiteenlopende colleges, het schrijven van praktijkopdrachten en research papers hebben risicomanagement vanuit verschillende invalshoeken belicht en mijn geïnspireerd het geleerde in mijn dagelijkse praktijk toe te passen.

Deze masterthesis vormt het sluitstuk en gaat in op risicomanagement in het cyber domein van de Koninklijke Marechaussee (KMar).

"Cyber" is de laatste jaren een term die veelvuldig de revue passeert, in de media lezen we over cybercriminelen, phishing en ransomware. Op de radio horen we commercials over cybersecurity en binnen organisaties staat het onderwerp steeds prominenter op de agenda, zo ook bij de Koninklijke Marechaussee.

In een snel veranderende omgeving waarin dreiging en onzekerheid toenemen is de vraag naar veiligheid groter dan ooit. De druk op de Defensie en daarmee de Koninklijke Marechaussee is enorm, zowel Nationaal als Internationaal vinden er een groot aantal operaties plaats. Juist nu is het belangrijk om de vaak onzichtbare cyberdreiging het hoofd te bieden en daarmee de continuïteit van de operaties te waarborgen. De in dit onderzoek ontworpen risicomanagement benadering moet de KMar helpen om op een gestructureerde wijze cybersecurity risico's te identificeren en te beheersen.

Vincent Bijlard

Mei 2023

Inhoudsopgave

Voorwoord ... 3
Inhoudsopgave ... 4
Samenvatting ... 6
1. Onderzoeksopzet ... 7
1.1 Aanleiding en probleemstelling ... 7
1.2 Probleemstelling ... 9
1.3 Doelstelling ... 10
1.4 Onderzoeksmodel ... 10
1.5 Onderzoeksvragen ... 12
1.6 Methodologie ... 13
2. De Theorie: literatuur onderzoek ... 15
2.1 Kernbegrippen in dit onderzoek ... 16
2.2 Cyber security risico ... 18
2.3 Cybersecurity risicomanagement ... 21
2.4 Risicomanagement benaderingen ... 25
2.4.1 INK EFQM model ... 27
2.4.2 COSO ... 28
2.4.3 ISO 31000 ... 29
2.4.4 ISO 27000 series ... 30
2.4.5 NIST series ... 31
2.4.6 BSI Germany Standard ... 31
2.4.7 Benaderingen in gebruik binnen Defensie ... 32
2.5 Criteria voor risicomanagement uit de literatuur ... 33
2.6 Samenvatting en deelconclusie ... 35
3. De praktijk: Risicomanagement binnen de Koninklijke Marechaussee ... 36
3.1 Methodologie praktijkonderzoek ... 36
3.1.1 Empirisch onderzoek / Interviews ... 36
3.1.2 Analyse en verwerking van data ... 37
3.2 Risicomanagement binnen de KMar, het beleid vanuit documentanalyse ... 38
3.3 Criteria vanuit het beleid ... 39
3.4 Risicomanagement binnen de KMar, de interviews ... 40

3.4. Criteria uit interviews 41
3.5 Conclusie hoofdstuk 3 42
4. Het ontwerp 44
4.1 Inleiding ontwerp 44
4.2 Definitieve selectie ontwerpcriteria 45
4.3 Score bestaande benaderingen 46
4.4 Keuze definitief ontwerp 48
5. Conclusie en aanbevelingen 51
5.1 Conclusie en beantwoording hoofdvraag 51
5.2 Aanbevelingen en vervolgonderzoek 52
5.3 Aanbevelingen voor vervolgonderzoek 54
5.4 Wetenschappelijke en praktische relevantie 54
5.5 Betrouwbaarheid en Validiteit 55
6. Bijlagen 56
6.1 Bibliografie 56
Bijlage 1: Interviewprotocol 63
Bijlage 2: Overzicht figuren en tabellen 64

Samenvatting

Dit rapport beschrijft een onderzoek naar cybersecurity risicomanagement binnen de Koninklijke Marechaussee. Het doel in het onderzoek is om een risicomanagement benadering te ontwerpen waarmee de Koninklijke Marechaussee in staat wordt gesteld om op een effectieve wijze cybersecurity risico's te beheersen. Hiermee wordt de cyber weerbaarheid, wendbaarheid en veerkracht van de Koninklijke Marechaussee verhoogd waarmee de continuïteit in de uitvoering van de wettelijk opgedragen taken kan worden gegarandeerd.

De taken van de Koninklijke Marechaussee zijn breed en veelomvattend. De organisatie voert haar taken uit in een complexe omgeving en in een tijd waarin de veiligheid van onze samenleving belangrijker is dan ooit. Ontwikkelingen als *Artificial Intelligence,* een steeds snellere digitalisering en daaraan verwante afhankelijkheid van IT maken de KMar kwetsbaar voor cyber verstoringen. De afhankelijkheid van IT is anno 2023 groot, onontkoombaar en vraagt om doeltreffend risicomanagement. Ondanks dat dit door de KMar wordt onderkent en er diverse initiatieven zijn ontplooit ontbreekt het de KMar aan een risicomanagement benadering om cybersecurity risico's effectief te identificeren en beheersen.
De in dit onderzoek ontworpen benadering stelt de KMar in staat de noodzakelijke stappen te zetten in de richting van integraal risicomanagement in het cyberdomein. Binnen het onderzoek is voortdurend aandacht besteed aan de behoefte van de organisatie en is getracht het ontwerp zoveel als mogelijk aan te laten sluiten op bestaande werkprocessen.

Het definitieve ontwerp is een synthese van de ISO 31000 en ISO 27005 standaarden waaraan het NIST Cyber Security Framework (NIST CSF) is toegevoegd. Deze verrijking dient de KMar in staat te stellen het gewenste overzicht en inzicht in het IT landschap te creëren en de daarbij behorende risico's ten aanzien van het primaire proces te identificeren. Het NIST CSF is een breed toegepaste cyber security risicomanagement benadering en geschikt voor organisaties als de KMar waarin de risicovolwassenheid laag is.

1. Onderzoeksopzet

1.1 Aanleiding en probleemstelling

Deze masterthesis start met een citaat uit het Nationaal Cyber Security Beeld Nederland (2022) uitgegeven door de Nationaal Coördinator Terrorismebestrijding en Veiligheid, kortweg de NCTV.

> "Om ongestoord te kunnen functioneren, moeten we onze samenleving zo goed als mogelijk beschermen tegen digitale dreiging. Ondanks de inspanningen om de weerbaarheid te verhogen, is er sprake van scheefgroei met de toenemende dreiging. Die scheefgroei vergroot het risico op ontwrichting van onze samenleving. Denk hierbij aan de bankensector, het openbaar vervoer of drinkwater, het is niet zozeer de vraag of bedrijven worden aangevallen, maar wanneer. Datzelfde geldt voor de overheid, kennisinstellingen en andere organisaties. De basismaatregelen op orde hebben helpt, maar deze zijn nog lang niet overal goed doorgevoerd." (NCTV, 2022)

De Koninklijke Marechaussee (KMar) waakt over de veiligheid van Nederland. De KMar wordt wereldwijd ingezet op plaatsen van strategisch belang; van de Koninklijke paleizen tot aan de buitengrenzen van Europa, van luchthavens in Nederland tot oorlogs- en crisisgebieden overal ter wereld. De Koninklijke Marechaussee is veelzijdig inzetbaar voor veiligheid, juist als het erop aankomt (Koninklijke Marechaussee, 2017). Maatschappelijke veranderingen hebben gevolgen voor de inzet en taakstelling van de KMar. Instabiliteit aan de buitengrenzen, extremisme en activisme zijn van invloed op het gevoel van veiligheid binnen de samenleving. Daarnaast volgen wereldwijd de ontwikkelingen in het digitale domein elkaar in een rap tempo op. Digitalisering en nieuwe technologieën hebben steeds meer invloed op het werk dat de KMar uitvoert. De KMar wordt geacht mee te bewegen met de maatschappelijke- en technologische ontwikkelingen en daar passend op te reageren. Zo schrijft de KMar eind 2021 in een fiche[1] ten aanzien van de kabinetsformatie van het huidige kabinet Rutte IV;

> *"Om een betrouwbare ketenpartner in het veiligheidsdomein te zijn en blijven moet de KMar investeren in cyber. Dit is nodig om de veiligheidsketen sterk te houden en daarmee actief een bijdrage te kunnen leveren aan een weerbare en veilige samenleving, de Marechaussee is niet adequaat toegerust om Nederland te beschermen tegen huidige en toekomstige dreigingen"* (Koninklijke Marechaussee, 2021)

[1] Fiches zijn informatiebladen over de kernonderwerpen van de comptabele wet- en regelgeving zoals de begrotingswetten, budgetrecht, schatkistbankeren etc. Ze zijn als aanvulling bedoeld op de voorschriften en als informatieve documenten opgenomen (Bron: Website Ministerie van Financiën)

Het citaat waarmee dit onderzoeksvoorstel begint geeft een actueel en verontrustend beeld van de dreiging waarmee onze samenleving te maken heeft. Vele bedrijven en instanties voelen zich meer en meer genoodzaakt tot het investeren in cybercapaciteiten en het nemen van daar aan gerelateerde maatregelen, zo ook de KMar (Koninklijke Marechaussee, 2020). De organisatie staat komende jaren voor een grote uitdaging, dit wil echter niet zeggen dat er tot op heden nog niets is gebeurd.

De KMar heeft de afgelopen jaren een start gemaakt met het inbedden van cybercapaciteit binnen de organisatie, zo is er een doctrine geschreven waarmee de KMar richting beoogt te geven aan hoe de organisatie denkt over cyberactiviteiten binnen haar taakstelling (Koninklijke Marechaussee, 2020). Dit document beschrijft de grondslagen, principes en voorwaarden voor cyber activiteiten binnen het optreden van de KMar op verschillende niveaus, daarnaast draagt de doctrine bij aan de plaatsbepaling van de KMar binnen het veiligheidsbestel. De doctrine heeft als doel een gemeenschappelijk beeld te creëren van cyber activiteiten in het optreden van de KMar. Op basis van deze doctrine worden afgeleide publicaties geschreven die gedetailleerd richting geven aan procedures en toepassingen in de praktijk (Koninklijke Marechaussee, 2020)

Samengevat staat de samenleving voor een grote uitdaging, maatschappelijke ontwikkelingen dwingen organisaties als de KMar zich te concentreren op digitale transformatie. De maatschappij digitaliseert en dat heeft impact op huidige en toekomstige veiligheidsvraagstukken, er dienen zich continue nieuwe risico's aan. De KMar beschrijft de noodzakelijke transformatie in een beleidsstuk met de titel 'future proof KMar" (Koninklijke Marechaussee, 2017).

In dit visiedocument wordt onder andere beschreven welke stappen, rollen en verantwoordelijkheden er nodig zijn voor de implementatie van thema's als; het leiderschap van de toekomst, cyber en digitale transformatie. Er wordt in dit visiedocument geen aandacht besteed aan risicomanagement.

Cyberspace

Binnen de wetenschap is veel discussie over de definitie cyberspace. In een *review article* geschreven door Starodubtsev et al. (2020) worden drieëntwintig definities uit verschillende wetenschappelijke artikelen vergeleken. Uit de conclusie blijkt dat de eigenschappen van cyberspace zijn geïdentificeerd maar nog niet hebben geleid tot een wetenschappelijke definitie. Toch wordt het begrip cyberspace veelvuldig gebruikt in zowel wetenschappelijke als niet-wetenschappelijke literatuur. Binnen dit onderzoek is gekozen voor de definitie als gebruikt door de international organization for standardization (ISO): "***Cyberspace is a complex medium that does not exist in any physical form and emerges as a result of interactions of people, software, and Internet services via technical devices and network connections (International Organisation for Standardization, 2012)".***

Risicomanagement

Het Ministerie van Defensie waarvan de KMar een onderdeel is heeft in het jaar 2019 een eerste aanwijzing Secretaris Generaal uitgegeven waarin integraal risicomanagement wordt beschreven (Ministerie Van Defensie, 2019). Een dergelijke aanwijzing is binnen Defensie de belangrijkste vorm van beleid en dient als basis voor gedetailleerde uitwerking binnen de diverse Krijgsmachtonderdelen, zoals de KMar. Van deze uitwerking is helaas weinig van de grond gekomen oordelen zowel de commissie van de Veer (van de Veer, 2018), als ook Gerry Verbeet, oud-Kamervoorzitter en voorzitter van de visitatiecommissie Defensie en Veiligheid (VCD). De visitatiecommissie is in 2018 ingesteld na het rapport van de commissie van de Veer waaruit bleek dat de algehele veiligheid binnen Defensie ernstig te kort schiet (van de Veer, 2018; Visitatiecommissie Defensie en Veiligheid, 2020.) Anno 2021 is de eindconclusie van de VCD dat veiligheid meer aandacht heeft gekregen maar “kritische randvoorwaarden ontbreken”, als voorbeelden worden genoemd; “een goed risicomanagement systeem en het ontbreekt aan heldere doelen, verantwoordelijkheden en financiën” (Visitatiecommissie Defensie en Veiligheid, 2021). Gelijktijdig aan de uitvoering van dit onderzoek (januari 2023 – juni 2023) loopt er een programma om een plan op te stellen voor de implementatie van Integraal Risico Management (IRM) in het jaar 2025 en verder. Er wordt gestart met een aantal deelgebieden, cyber- maakt geen deel uit van deze eerste fase.

1.2 Probleemstelling

De rapporten van de commissie van de Veer en de Visitatiecommissie Defensie bevatten diverse aanbevelingen. In een samenleving waar onzekerheid toeneemt en risico’s zich manifesteren, tezamen met de verontrustende conclusies uit het Nationaal cyber security beeld laten een urgente roep om actie zien. De KMar laat middels een aantal hiervoor genoemde beleidsvoornemens zien dat ze deze roep wilt beantwoorden.

De eerste verkenning voor dit onderzoek toont aan dat er een lacune bestaat tussen de noodzakelijke digitale transformatie van de organisatie en het beleid om integraal risicomanagement onderdeel uit te laten maken van alle processen. Het is noodzakelijk in kaart te brengen waarom deze lacune bestaat en welke factoren hier op van toepassing zijn.

Samenvattend leidt dit tot de volgende probleemstelling. Door het ontbreken van volledig inzicht in de risico’s die de KMar loopt ten aanzien van cybersecurity is de organisatie kwetsbaar voor cyberincidenten. Dergelijke incidenten kunnen zorgen voor verstoring van het primaire proces en in ernstige gevallen leiden tot schade aan de belangen van de Staat en/of haar bondgenoten.

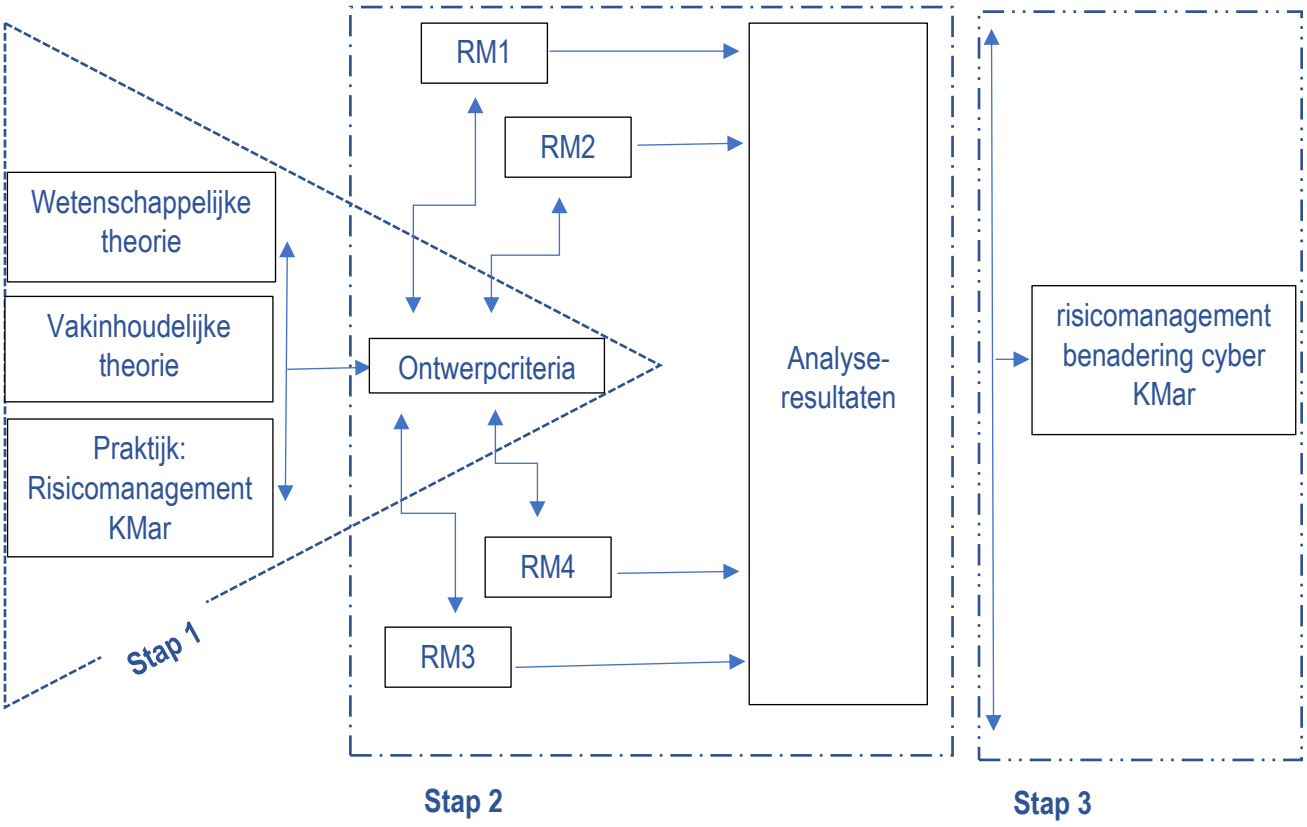
1.3 Doelstelling

Het doel van het onderzoek is om de cyber weerbaarheid, wendbaarheid en veerkracht van de Koninklijke Marechaussee te verhogen waarmee de continuïteit in de uitvoering van de wettelijk opgedragen taken kan worden gegarandeerd.

Het doel in het onderzoek is om een risicomanagement benadering te ontwerpen waarmee de Koninklijke Marechaussee in staat wordt gesteld om op een effectieve wijze cybersecurity risico's te beheersen.

1.4 Onderzoeksmodel

Aan de hand van Verschuren & Doorewaard (2021) is er een onderzoeksmodel ontwikkeld, de stappen zijn in tekst uitgeschreven na het model. Een onderzoeksmodel is een schematische weergave van het doel in het onderzoek en de stappen die gezet dienen te worden om dit doel te bereiken. Ook helpt het onderzoeksmodel bij het vaststellen van de noodzakelijke theoretische achtergronden.



Figuur 1: Onderzoeksmodel

Het doel van stap 1 in het onderzoeksmodel is het vormen van een theoretische basis op basis waarvan dit onderzoek is vormgegeven. Na de vaststelling van de probleemsituatie en de doelstelling van het onderzoek is een geschikte onderzoeksmethodologie geselecteerd. Op basis van het theoretisch kader is een interviewprotocol ontworpen waarmee empirische data is verzameld. Stap 1 is voltooid met het vaststellen van drie sets ontwerpcriteria, te weten;

(1) Criteria vanuit de wetenschappelijke literatuur.
(2) Criteria vanuit vakinhoudelijke en interne documentatie.
(3) Criteria vanuit empirisch onderzoek door middel van interviews.

Stap 2: In deze stap zijn de ontwerpcriteria beschouwd in het licht van de wetenschappelijke literatuur over cybersecurity risico management. Aan de hand van een selectie van risicomanagement raamwerken, standaarden en modellen[2] is bepaald in welke benaderingen aanknopingspunten zitten voor de te ontwerpen benadering voor de KMar. *(Noot: in het model zijn deze raamwerken afgekort tot RM 1 t/m 4, het aantal raamwerken dat is onderzocht is groter dan 4).*

In stap 3 is aan de hand van de in stap 2 uitgevoerde analyse uitgewerkt hoe de risicomanagement benadering er voor de KMar uit ziet en is het ontwerp uitgewerkt. Tot slot zijn er aanbevelingen gedaan.

[2] In dit onderzoek is omwille van de leesbaarheid gekozen voor het begrip **benadering**. Hiermee worden zowel raamwerken, als standaarden als methoden bedoeld. Een nadere toelichting volgt in hoofdstuk 2

1.5 Onderzoeksvragen

In deze paragraaf zijn de onderzoeksvragen van dit onderzoek uiteengezet. Eerst is aan de hand van de probleemstelling en doelstelling zoals beschreven in paragraaf 1.1 een centrale vraagstelling afgeleid. Deze luidt:

Hoe kunnen cybersecurity risico's van de Koninklijke Marechaussee doeltreffend worden beheerst?

Vervolgens is deze vraag gedecomponeerd in een aantal deelvragen, deze vragen zijn in lijn gebracht met de in dit onderzoek gebruikte methodologie. Onder elke vraag zal dit worden toegelicht.

In de doelstelling van dit onderzoek is beschreven dat de praktische toepasbaarheid en integratie van de benadering in dit onderzoek centraal staat. Om een analyse te kunnen uitvoeren is het van belang om de verschillende uit de hoofdvraag voortkomende concepten te operationaliseren en de hoofdvraag uit te splitsen in een drietal deelvragen, de gebruikte methodologie is weergegeven in tabel 1 en uitgewerkt in de paragraven 1.6 en 3.1.

Deelvraag 1: Wat is de stand van de wetenschappelijke en vakliteratuur over risicomanagement in relatie tot cybersecurity?

Toelichting: De eerste deelvraag binnen dit onderzoek is een kennisvraag en draagt bij aan de noodzakelijke wetenschappelijke- en inhoudelijke theoretische onderbouwing. Het antwoord op deze deelvraag is tevens richtinggevend en bepalend voor de vaststelling van het interviewprotocol dat is gebruikt voor de beantwoording van deelvraag 2. Tevens levert deze deelvraag de eerste set ontwerp criteria vanuit de literatuur op.

Deelvraag 2: Op welke wijze wordt risicomanagement ten aanzien van cybersecurity toegepast binnen de Koninklijke Marechaussee?

Toelichting: Deze deelvraag is praktijkgericht en heeft als doelstelling te komen tot een uiteenzetting van de wijze waarop risicomanagement ten aanzien van cybersecurity wordt toegepast binnen de KMar en welke criteria relevant zijn voor een ontwerpbenadering. Daarna zal uit de analyse van de empirische resultaten blijken welke ontwerpcriteria er zijn voor een risicomanagement benadering.

Deelvraag 3: Hoe kan een risicomanagement benadering worden ontworpen voor de KMar?

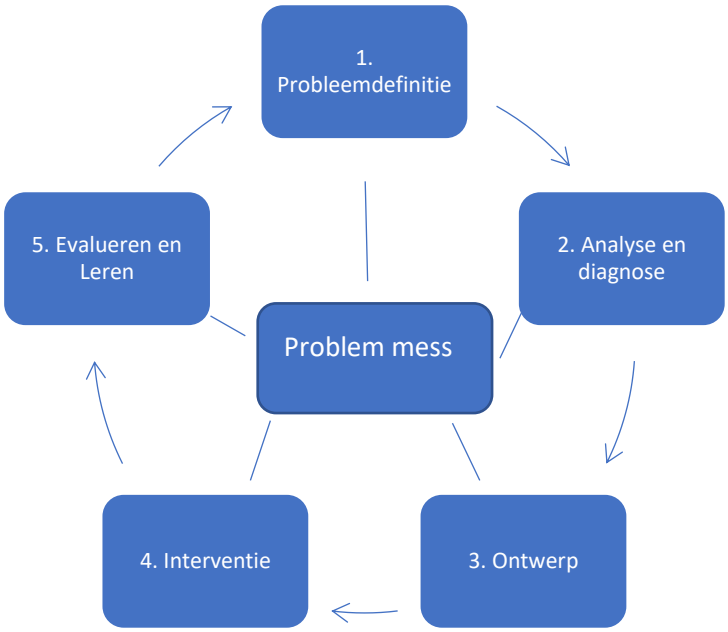
Toelichting: Deze deelvraag betreft een ontwerpvraag, op basis van de selectie van risicomanagement benaderingen en de drie sets ontwerpcriteria zal er een cyber security risicomanagement benadering voor de KMar worden ontworpen.

1.6 Methodologie

Voor de beantwoording van de verschillende onderzoeksvragen zijn uiteenlopende onderzoeksmethoden gebruikt, in deze paragraaf is de onderzoeksstrategie uiteengezet. Volgens Verschuren en Doorewaard (2021) bestaat de onderzoeksstrategie uit het geheel van met elkaar samenhangende beslissingen over de manier waarop het onderzoek wordt uitgevoerd, hierna zijn deze beslissingen uitgewerkt. Voor eenduidig overzicht is gekozen om na een algemene inleiding de onderzoeksstrategie per deelvraag uit te werken in een tabel.

Er is gekozen voor kwalitatief en praktijkgericht ontwerponderzoek, de aard van het probleem is leidend. Omdat is gestreefd naar een risicomanagement benadering die aansluit op de behoeften van de organisatie waarbinnen dit onderzoek wordt uitgevoerd en het ontwerp geïntegreerd dient te worden in de dagelijkse praktijk heeft dit onderzoek een exploratief en inductief karakter.

Hierbij is gebruik gemaakt van de *problem solving cycle* als beschreven door van Aken en Berends (2018). Dit cyclische proces bestaat uit 5 stappen welke in volgordelijkheid doorlopen dienen te worden. Er kan pas aangevangen worden met een volgende stap wanneer de voorgaande stap is voltooid.



Figuur 2: *problem solving cycle*, (Aken & Berends, 2018)

In de paragraven 1.1 en 1.2 is het probleem gedefinieerd. Omdat in deze fase van het onderzoek het probleem, na vooronderzoek, beperkt is beschreven, is verdere analyse en diagnose noodzakelijk. In stap 2 van de cyclus, die overeenkomt met deelvraag 2, zijn de context en mogelijke oorzaken van het probleem onderzocht.

Om deze stap gedegen uit te voeren is een theoretisch kader vastgesteld, in hoofdstuk 2 van dit rapport is dit kader uiteengezet. Door eerst een theoretische basis te leggen en enkele kernbegrippen uit te werken kan vervolgens in de praktijk een analyse van het probleem worden uitgevoerd.

In stap 3 van de cyclus, die overeenkomt met deelvraag 3, wordt aan de hand van de criteria uit stap 2 inductief naar oplossingsrichtingen gezocht. Bestaande raamwerken, standaarden en modellen (hierna 'benaderingen') zijn beoordeeld op relevantie en gebruikt om te komen tot een definitieve risicomanagement benadering voor de KMar.

Stap 4 en 5 betreffen achtereenvolgens de interventie en evaluatie van het ontwerp. Dit onderzoek richt zich op de eerste drie stappen van de cyclus, in het laatste hoofdstuk worden wel enkele aanbevelingen gedaan waarmee stap 4 en 5 kunnen worden ingezet.

Onderzoeksstrategie			
Onderzoeksvraag	Onderzoeksmethode	Bijdrage aan onderzoek	Stap cyclus
Wat is de stand van de wetenschappelijke- en vakinhoudelijke literatuur over risicomanagement ten aanzien van cybersecurity?	Literatuuronderzoek, document analyse interne stukken.	Kwalitatieve data waarmee theoretisch- en begrippen-kader wordt gevormd, ontwerpcriteria worden vastgesteld vanuit literatuur.	Stap 1
Op welke wijze wordt risicomanagement ten aanzien van cybersecurity toegepast binnen de Koninklijke Marechaussee?	documentonderzoek, semigestructureerde interviews.	Vanuit de literatuur naar context en organisatie specifieke ontwerpcriteria.	Stap 2
Hoe kan een risicomanagement benadering worden ontworpen voor de KMar?	ontwerponderzoek, semigestructureerde interviews.	Synthese van ontwerpcritieria uit literatuur, documentanalyse en interviews.	Stap 3

Tabel 1: onderzoeksstrategie

2. De Theorie: literatuur onderzoek

In dit hoofdstuk is het uitgevoerde literatuuronderzoek beschreven en zal deelvraag 1 beantwoord worden. Het hoofdstuk start met een beschrijving van de in dit onderzoek gebruikte kernbegrippen (2.1). Daarna zal er een beschrijving worden gegeven van cyber security risico (2.2), en vervolgens van cyber security risicomanagement (2.3). In paragraaf 2.4 worden relevante risicomanagement benaderingen uiteengezet, in de laatste paragraaf (2.5) wordt de eerste set ontwerpcriteria vanuit de wetenschappelijke literatuur gepresenteerd.

De in dit onderzoek voorkomende kernbegrippen en daar aan relevante synoniemen zijn hierna beschreven. Vanuit de probleemstelling, de doelstelling en de onderzoeksvragen zijn vijf kernbegrippen vastgesteld, het betreft een subjectieve selectie, met behulp van een thesaurus zijn vervolgens synoniemen bepaald. Er is tijdens het zoeken naar wetenschappelijke literatuur zowel in het Engels als in het Nederlands gezocht.

Kernbergrip	Synoniem
Cybersecurity	Informationsecurity
Cyberrisk	Cyberhazard, cyberthreat
Cyberresilience	Cybercontinuity
Riskmanagement	Riskmitigation
Framework	Model, architecture, design, method, approach

Tabel 2 Kernbegrippen en synoniemen.

Er is gebruik gemaakt van de volgende wetenschappelijke databases

- Scopus
- Web of Science
- Google Scholar

Tevens zijn er interne bedrijfsdocumenten, standaarden van internationale organisaties voor standaardisering, beleidsstukken, rapportages, implementatieplannen, wetgeving, presentaties, onderzoeksrapporten en kamerstukken geanalyseerd. Een volledig overzicht van alle geraadpleegde literatuur is opgenomen als bijlage bij dit rapport.

De volgende zoekstring is gebruikt bij het raadplegen van bovengenoemde databases:

(cybersecurity OR informationsecurity) AND (cyberrisk OR riskmanagement OR riskmitigation OR cyberresilience) AND (framework OR model OR architecture OR design OR method OR approach)

Scopus	Web of Science	Google Scholar
104	80	570

De zoekopdracht leverde het bovenstaande resultaat op. Hierbij is gezocht op titel, abstract, onderwerp en kernwoorden binnen de publicaties. Vervolgens is een aanvullend selectieproces toegepast waarbij duplicaten uit de drie databases zijn verwijderd, er zijn alleen artikelen in de Engelse en Nederlandse taal geselecteerd. Daarna is op basis van de titels van de publicaties geselecteerd op relevantie in relatie tot de onderzoeksvragen. Zo zijn artikelen die de betrekking hebben op andere niet cyber- gerelateerde domeinen zoals de zorg of het onderwijs verwijderd.

2.1 Kernbegrippen in dit onderzoek

Het Ministerie van Defensie (MinDef) definieert **risico** als "Het effect van onzekerheid op (het behalen van) doelstellingen." Een gebeurtenis, incident of kwestie met - als het zich voordoet - een impact op doelstellingen. Tevens wordt hierbij verondersteld dat het effect zowel positief als negatief kan zijn, kansen of bedreigingen kan aanpakken, creëren, of daarin kan resulteren (Ministerie Van Defensie, 2017). Deze definitie is door MinDef ontleend uit de NEN-ISO 31000 (ISO, 2018). Hierbij dient te worden opgemerkt dat risico's in relatie tot veiligheid doorgaans geen positief effect hebben op doelstellingen.

Over het concept risico bestaat veel discussie, zo schrijft Aven (2012) *"there is no agreed definition of the concept of risk".* Risico wordt gezien als verwacht verlies (Willis, 2007), of als kans op een nadelige uitkomst (Graham & Weiner, 1995). Van Staveren (2015) beschrijft vier verschillende betekenissen van risico die vaak onbewust door elkaar worden gebruikt.

(1) Risico als kans op een ongewenste gebeurtenis;
(2) Risico als gevolg van een dergelijke gebeurtenis;
(3) Risico als ongewenste gebeurtenis zelf;
(4) Risico als oorzaak van die gebeurtenis.

Ook het begrip **onzekerheid** komt veelvuldig naar voren in de literatuur. Van Staveren (2015) gaat hierop in en definieert twee vormen van onzekerheid; ontologische of aleatorische onzekerheid en epistemologische onzekerheid. De eerste vorm heeft de betrekking op onvermijdelijke variatie in eigenschappen en de tweede vorm gaat over een gebrek aan kennis en vaardigheden, beide vormen van onzekerheid zijn relevant in de context van dit onderzoek.

Een andere, ook binnen het Ministerie van Defensie veelvuldig gebruikte benadering van risico is die van kans x effect, soms aangevuld met de factor detectie (Hopkin, 2018). Deze benadering van risico heeft het voordeel praktisch in gebruik te zijn maar laat de factor onzekerheid grotendeels buiten beschouwing (Aven & Renn, 2009). Binnen het Ministerie van Defensie wordt deze benadering gebruikt in combinatie met een risicomatrix (Ministerie Van Defensie, 2019; Geraets, 2018), dit levert een getalsmatige waarde op waar mitigerende maatregelen aan gekoppeld kunnen worden. In de literatuur bestaat veel discussie over deze vorm van het kwantificeren van risico, bijvoorbeeld door Aven (2009) die stelt dat voorzichtigheid betracht dient te worden met het veronderstellen dat risico een meetbaar object is. Daarnaast levert een hoge kans en een laag effect dezelfde waarde op als een lage kans en een hoog effect, dit maakt deze methode onderwerp van discussie.

Samengevat; Ook binnen het Ministerie van Defensie worden diverse definities van het begrip risico gehanteerd. Door de Koninklijke Marechaussee wordt het begrip risico als volgt gedefinieerd: *Het effect van onzekerheid op (het behalen van) de vooraf bepaalde doelstelling(en) gerelateerd aan de (kern)waarden van de organisatie. Een risico wordt uitgedrukt in termen van risicobronnen, mogelijke gebeurtenissen, alsmede de gevolgen en de waarschijnlijkheid ervan. Risico's kunnen worden onderkend van uit zowel operationeel, strategisch en/of veranderperspectief, waarbij de afgestemde risicobereidheid (risk appetite) bij aanvang van integrale risicobeoordeling en –behandeling bepalend is"* (Ministerie van Defensie, 2023).

Onder risicomanagement wordt verstaan: *Het omvat de gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's. Het doel van risicomanagement is het creëren en beschermen van waarde. Het ondersteunt het realiseren van continuïteit, proces & compliance-, performance/verbeter- of vernieuwingsdoelstellingen"* (Ministerie van Defensie, 2023).

Risicobereidheid; een derde en laatste in dit onderzoek belangrijk begrip is risicobereidheid, vaak *risk-appetite* genoemd. Van Staveren (2015) omschrijft dit als "de figuurlijke trek in risico's die een persoon of organisatie heeft." De *International Organisation for Standardization* (ISO) beschrijft in de ISO 31000 en ISO 27000 standaarden een vrijwel gelijke definitie en vult aan met de opmerking dat het top management

meermaals per jaar de risicobereidheid dient vast te stellen. Risicobereidheid varieert van organisatie tot organisatie en kent zelfs binnen organisaties veel differentiatie. Zo kan de KMar ten aanzien van een kritiek primair proces een lage risicobereidheid hebben en de bereidheid hoger zijn in een meer ondersteunend proces.

Nu is vastgesteld dat er geen gangbare definitie is voor risico binnen de wetenschap op basis van het uitgevoerde literatuur onderzoek is er gekozen om de hiervoor beschreven definities van risico en risicomanagement te hanteren binnen de context van dit onderzoek. De risicobereidheid is organisatie en context afhankelijk maar kent in de wetenschap meer eenduidigheid.

Binnen het cyberdomein krijgt het concept ***cybersecurity risico*** steeds meer aandacht. Ter illustratie, een zoekslag op Scopus laat een beperkt maar toenemend aantal papers over dit onderwerp zien; 3 in 2008, 18 in 2013, 60 in 2017, 116 in 2021. In een literatuur review uitgevoerd door Strupczewski (2021) wordt gesteld dat er, gelijk aan het kernbegrip risico, ook geen eenduidige definitie van cyber(security)risico bestaat. Böhme (2010) beschrijft twee eigenschappen die cyberrisico onderscheiden van conventioneel risico, dit behoeft enige toelichting.

In het inleidende hoofdstuk van dit onderzoek is uiteengezet wat wordt verstaan onder het begrip cyberspace; "*cyberspace is a collection of interconnected computerized networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit*" (Refsdal et al., 2015). Het geheel van deze elementen samen creëert de waarde van een netwerk, de afzonderlijke elementen kunnen niet los van elkaar worden gezien. Dit geldt ook voor het risico en het te verwachten verlies bij een gebeurtenis, incident of kwestie. Ten tweede dienen de elementen van waaruit cyberspace is opgebouwd het doel waarde toe te voegen aan het proces van een organisatie. Wanneer een systeem of netwerk faalt manifesteert een risico en treedt potentieel verlies op. Wanneer er een succesvolle cyberaanval plaatsvindt op één van de elementen vormt het individuele element de bedreiging voor een organisatie. Een netwerk creëert in normale omstandigheden dus waarde maar is bij een incident juist het object dat zorgt voor het waarde verlies (Böhme, 2010).

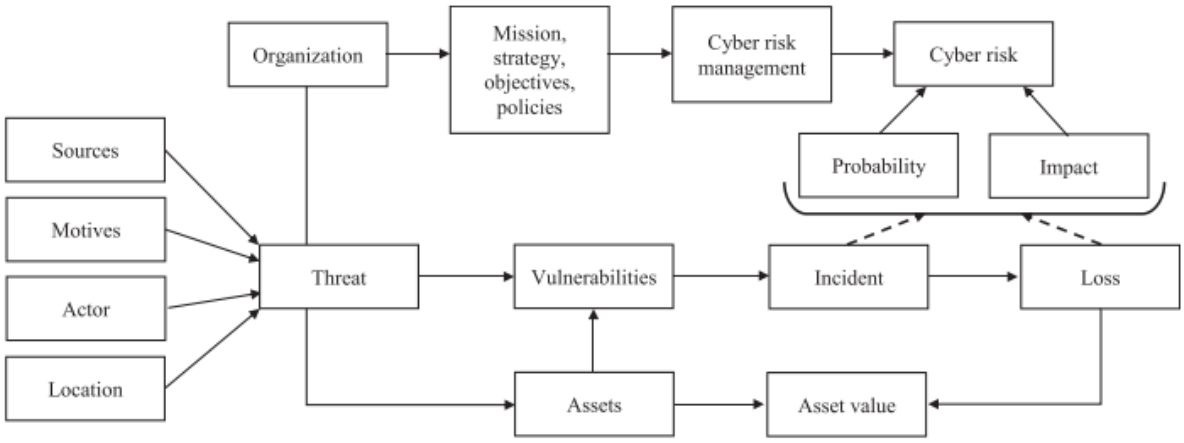
2.2 Cyber security risico

In deze paragraaf wordt ingegaan op de definitie van cybersecurity risico aan de hand van de huidige stand van de wetenschap.

Refsdal et al., (2015) beschrijven dat cybersecurity risico bestaat uit drie elementen; (1) een cyber securityrisico is een risico dat voortkomt uit een cyberdreiging, (2) een cyberdreiging is een dreiging die betrekking heeft op een netwerk in cyberspace en (3) cyberspace is een verzameling aan elkaar verbonden

netwerken. Cebula et al., (2014) gaan verder en beschrijven cybersecurity risico als een operationeel risico dat de betrekking heeft op; beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Hiervoor wordt steun gevonden in papers van Lloyds (2015a) en CRO forum (2014). Diverse auteurs beschrijven de financiële schade aan een organisatie als belangrijk element van cybersecurity risico, zie: Mukhopadhyay et al., (2013), Swiss Re (2014) en Institute of Risk Management (2014). Dit element is gezien de context van dit onderzoek nadrukkelijk buiten beschouwing gelaten. De risicogebieden binnen dit onderzoek staan beschreven in H3.2.1 figuur 10. Veel van de genoemde onderzoekers concentreren zich op de negatieve consequenties van risico en het potentiële verlies. Een aantal onderzoekers beschrijft cyberrisico vanuit een sterk organisatie specifieke context, bijvoorbeeld de zorg, weer anderen hebben alleen een focus op cybercrime.

In figuur 3, ontleent uit Strupczewski (2021), is weergegeven welke relaties er bestaan tussen de verschillende concepten, begrippen en factoren ten aanzien van cyber securityrisico.



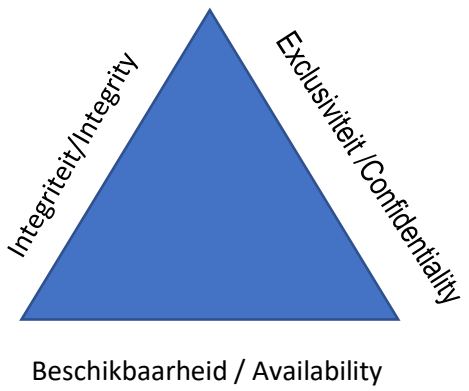
Figuur 3. Model cyber risico (Strupczewski, 2021)

In het model is zichtbaar dat cyberrisico het resultaat is van kans en impact, waarbij kans iets zegt over de waarschijnlijkheid van optreden van het risico gebaseerd op data van incidenten en gebeurtenissen uit het verleden, ook impact wordt gebaseerd op eerder geleden verlies. De cyberdreiging *(threat*) wordt beschreven aan de hand van vier parameters; bron van de dreiging, het motief, de actor en de locatie waar de dreiging vandaan komt. Deze vier parameters zijn aan continue verandering onderhevig en verder uiteen te rafelen, zo kan de bron van de dreiging een technisch mankement zijn, ongeoorloofde toegang tot een systeem of plaats of het breken van de genomen beveiligingsmaatregelen. Het Ministerie van Defensie gebruikt gerubriceerde daderprofielen (Ministerie van Defensie, 2021a), dit document beschrijft dadertyperingen, potentiële daders tegen Defensie en de gebruikte aanvalsmiddelen door deze potentiële daders. Het daderprofiel is een weerspiegeling van de actuele kennis omtrent mogelijke bedreigingen en wordt jaarlijks

geactualiseerd. Het motief kan voortkomen uit een bewuste of onbewuste actie, of het gevolg zijn van incompetentie. De bron van de dreiging kan zich intern of extern van de organisatie bevinden.
De kwetsbaarheid (*vulnerabilitiy*) komt voort uit zwakheden binnen het netwerk van een organisatie, een zwakke plek kan leiden tot een incident dat verlies (*loss*) tot gevolg heeft. Hierbij dient te worden opgemerkt dat de menselijke factor een grote rol speelt in relatie tot kwetsbaarheid (Eling et al., 2016).
In figuur 3 is goed zichtbaar dat de begrippen dreiging (*threat*), kwetsbaarheid (*vulnerability*) en risico (*risk*) drie verschillende elementen zijn in de context van cyber. Uit het empirisch onderzoek blijkt dat deze begrippen in de praktijk veelvuldig door elkaar gebruikt worden.

Samengevat stelt Strupczewski (2021) de volgende definitie voor:
"Cyber security risk is an operational risk associated with performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term 'cyber security risk' also includes physical threats to the ICT resources within organisation."
Deze definitie is overgenomen en wordt gebruikt binnen dit onderzoek.

Tot slot zijn de BIE criteria (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2012) in de context van dit onderzoek relevant. Deze criteria zijn afgeleid van de *'CIA Triad'* (Fenrich, 2008). De driehoek is in de Verenigde Staten ontworpen om organisaties in staat te stellen beveiligingsmaatregelen te nemen en gevoelige data te beschermen. De driehoek is weergegeven in figuur 4 met daarbij de vertaling in gebruik binnen de Nederlandse overheid. Een andere veelgebruikte vertaling van Exclusiviteit is Vertrouwelijkheid, dit levert de BIV criteria op.



Figuur 4: BIE of BIV driehoek / CIA Triad

Beschrijving driehoek	
Beschikbaarheid	Een informatie-kenmerk waardoor informatie toegankelijk en bruikbaar is voor een geautoriseerd individu of entiteit.
Integriteit	Een informatie-kenmerk waardoor informatie niet opzettelijk of onbewust kan worden veranderd of vernietigd.
Vertrouwelijkheid / Exclusiviteit	Een informatie-kenmerk waardoor alleen gemachtigde personen, entiteiten of processen toegang hebben tot bepaalde data.

Tabel 3: Beschrijving driehoek

2.3 Cybersecurity risicomanagement

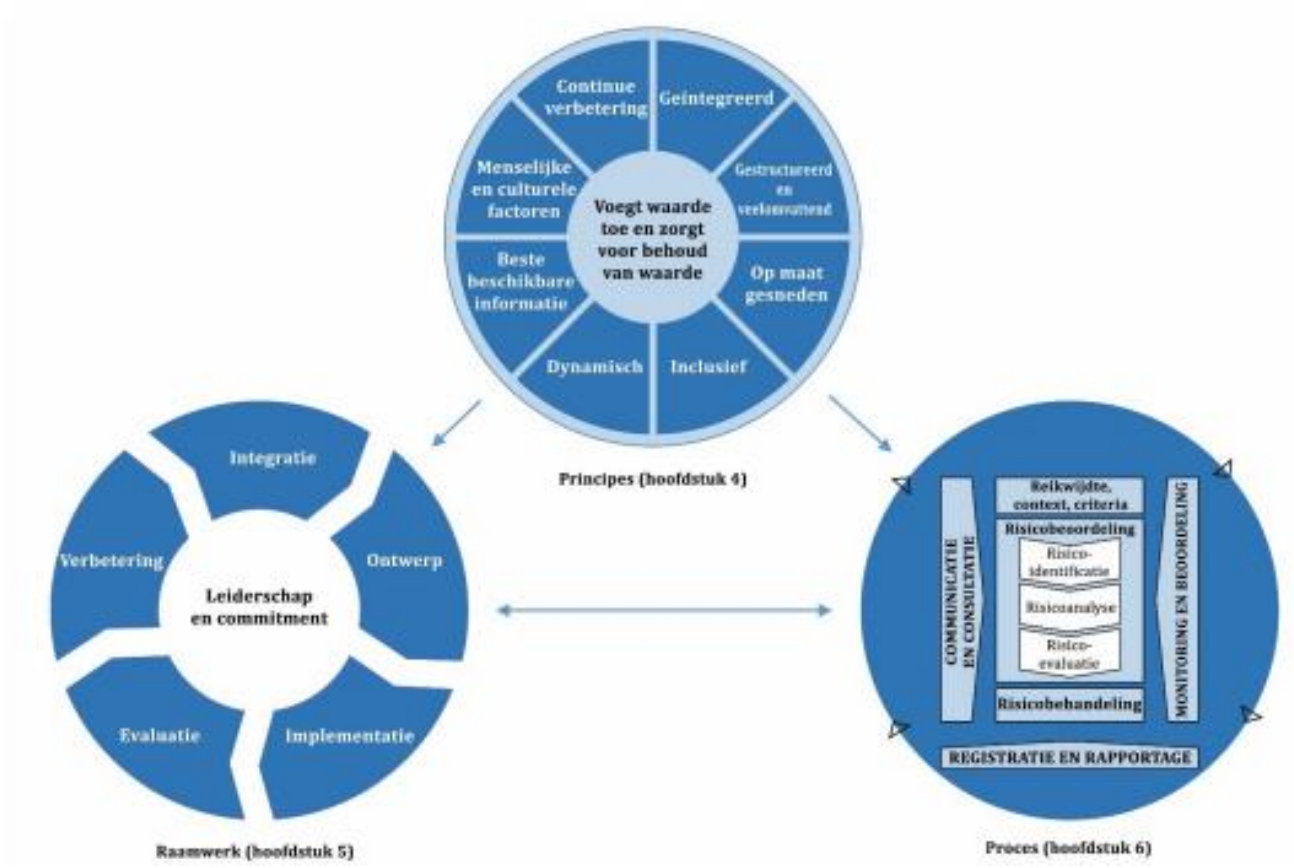
In deze paragraaf wordt nader ingegaan op risicomanagement binnen het domein cybersecurity, het begrip risico is in paragraaf 2.1 reeds beschreven.

Risicomanagement is volgens Van Staveren (2015) het; "doelgericht, expliciet, gestructureerd, communicerend en continu omgaan met risico's". Het Ministerie van Defensie gebruikt de volgende definitie: "*Risicomanagement omvat de gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's. Het doel van risicomanagement is het creëren en beschermen van waarde. Het ondersteunt het realiseren van continuïteit, proces & compliance-, performance/verbeter- of vernieuwingsdoelstellingen"* (Ministerie van Defensie, 2023). Risicomanagement is in ontwikkeling, de toenemende mate van complexiteit en onzekerheid in de samenleving maakt risico minder tastbaar. Door de steeds maar toenemende digitalisering kunnen kleine oorzaken leiden tot grote gevolgen, talloze voorbeelden van cyberaanvallen die hebben geleidt tot maatschappelijke ontwrichting vormen daar het bewijs voor. Zo schrijft het Nationaal Cyber Security Centrum in het Cyber Security Beeld Nederland 2022: *Een samenhangend en geïntegreerd risicomanagement binnen en tussen de niveaus van organisaties, sectoren en nationaal, staat nog in de kinderschoenen"* (Minsterie van Justitie en Veiligheid, 2022).

Er zijn verschillende manieren om risicomanagement toe te passen. ENISA's *Compendium of Risk Management Frameworks* (Lambrinoudakis et al., 2022) schetst verschillende benaderingen voor risicomanagement. Twee veelgebruikte standaarden zijn ISO 27005, met een focus op informatie, en de bredere ISO 31000, met een focus op bedrijfsvoering. Voor veel risicomanagement benaderingen geldt dat risicobeoordeling ofwel risico-identificatie een belangrijk deel van het motorblok vormt van een gedegen aanpak (Ministerie van Justitie en Veiligheid, 2022).

Er is gekozen om in het deel hierna de handleiding van de ISO 31000 standaard te gebruiken voor de beschrijving van de proces stappen van risicomanagement. Uit Van Staveren (2015 p. 70) blijkt dat benaderingen als COSO-ERM, ISO31000, risicogestuurd werken en RISMAN vrijwel identieke stappen bevatten waarbij soms andere benamingen gebruikt worden en stappen in volgorde kunnen verschillen.

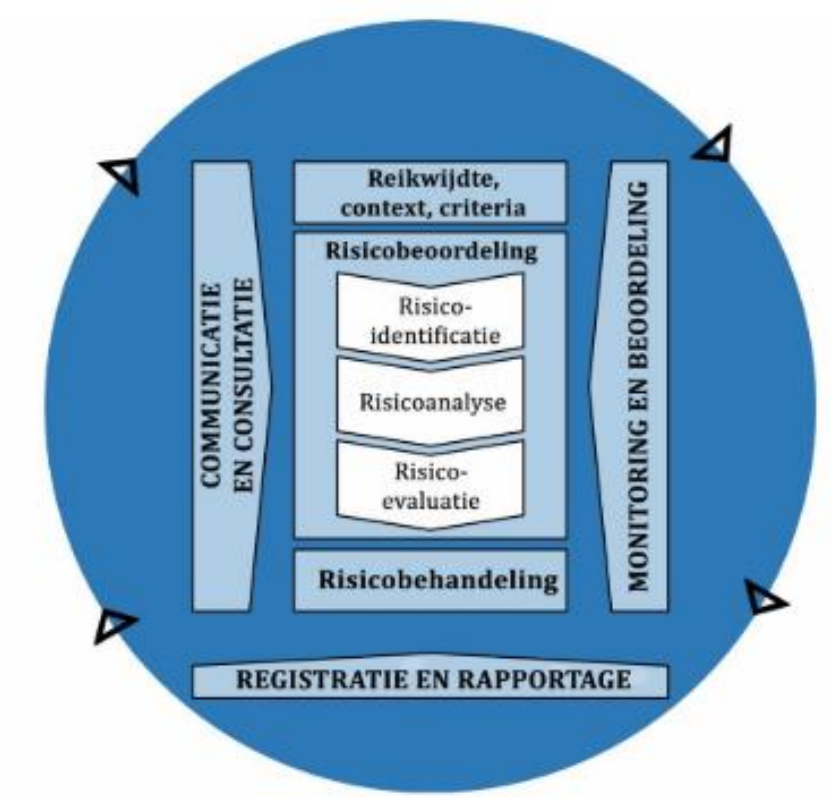
De *International Organisation for Standadization* (ISO) beschrijft risicomanagement in de publicatie ISO:31000:2018 als volgt: 'Risicomanagement bestaat uit een drietal elementen; risicomanagement principes, een raamwerk en een proces.'



Figuur 5 Elementen risicomanagement ISO standaard (ISO, 2018)

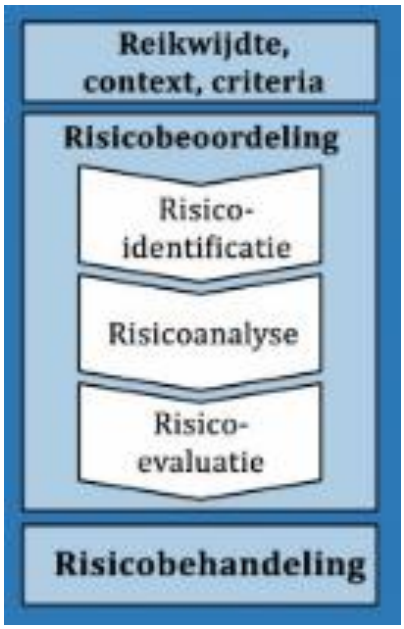
Om effectief risicomanagement toe te passen is het noodzakelijk om een raamwerk als basis te gebruiken. Een dergelijk raamwerk dient te voldoen aan een aantal basis principes van risicomanagement, in de ISO31000 standaard zijn elf principes beschreven. Het raamwerk dient in lijn te zijn met het risicomanagement proces dat een organisatie uitvoert en dient regelmatig te worden geëvalueerd aan de hand van resultaten uit het proces. De drie elementen tezamen maken het mogelijk om risicomanagement als proces integraal onderdeel uit te laten maken van het werk.

Hierna worden het risicomanagement proces en het risicomanagement raamwerk nader toegelicht. Het risicomanagement proces behelst de systematische toepassing van beleid, procedures en werkwijzen op de activiteiten van communicatie en consultatie, het vaststellen van de context en het beoordelen, behandelen, monitoren en herbeoordelen, registreren en rapporteren van risico (ISO, 2018).



Figuur 6 Risicomanagement proces ISO 31000 (ISO, 2018).

Communicatie en consultatie heeft als doel informatie te verkrijgen, verstrekken en te delen met de bij het risico betrokken *stakeholders.* Het dient als informatiebron voor de risicobeoordeling/risico-inschatting en vormt de basis voor besluitvorming over de te nemen maatregelen (Hopkin, 2018). De risicobeoordeling/risico-inschatting betreft het systematische proces waarmee risicobronnen worden geïdentificeerd, dreiging, gevaar en kansen worden onderkend; het begrijpen hoe deze kunnen optreden en wat de consequenties kunnen zijn is van belang (Aven, 2020). Het resultaat van de risicobeoordeling/risico-inschatting dient als basis voor besluitvorming over te nemen maatregelen.



Figuur 7 risicoprocesstappen uit ISO 31000 (ISO, 2018)

In figuur 7 zijn de risicoprocesstappen weergegeven volgens de ISO 31000 norm. De stappen zijn hierna beknopt beschreven:

1. Bepalen van de context, reikwijdte en criteria. In deze stap wordt de context bepaald, op welk niveau en op welke systemen of entiteiten is de risico-inschatting van toepassing. Tevens worden relevante stakeholders geïdentificeerd en risicocriteria bepaald.
2. Risico-identificatie is de stap waarin dreiging, kwetsbaarheid en de zaak waarop het risico van toepassing is in kaart worden gebracht. Belangrijk om te vermelden is dat deze drie elementen noodzakelijk zijn om over een risico te kunnen spreken, zonder zaak is er niets om te raken, zonder dreiging is er geen oorzaak en zonder kwetsbaarheid is er geen mogelijkheid om schade te doen (Refsdal et al., 2015), het is daarom essentieel om de drie genoemde elementen met elkaar in relatie te beschouwen.
3. De derde stap is de risicoanalyse, het is relevant om te benoemen dat het uitvoeren van een risicoanalyse een veelomvattend proces is, voor dit onderzoek is kennis genomen van het boek *"The Science of the Risk Analysis"* geschreven door Terje Aven (2020). Met een risicoanalyse worden alle activiteiten bedoelt waarmee een inschatting wordt gemaakt van de hoeveelheid risico, vaak in termen van waarschijnlijkheid en gevolg (Aven, 2020; Refsdal et al., 2015). Een ander belangrijk begrip is severity in het Nederlands vertaalt naar ernst. De ernst kan alleen worden bepaald in samenhang met de in stap 1 bepaalde context, de uitval van informatiesysteem A kan zorgen voor grote schade aan een organisatie terwijl de uitval van informatiesysteem B slechts beperkte gevolgen heeft.

4. De vierde stap is de risico-evaluatie, tijdens deze stap worden de hiervoor in kaart gebrachte risico's gewogen en geclassificeerd. Dit heeft besluitvorming over al dan niet te nemen maatregelen als doel.
5. Risico-behandeling betreft de uitvoering van mitigerende maatregelen om de in kaart gebrachte risico's te behandelen. Niet elk risico is van gelijke aard en behoeft mitigerende maatregelen.

Het is voor een organisatie belangrijk om het risicomanagement proces aan te passen naar de behoeften van de organisatie. Hiermee kan de organisatie de waarde van risicomanagement verbeteren (Aven, 2019). In het resultaten hoofdstuk van dit rapport is beschreven op welke wijze delen van risicomanagement benaderingen met elkaar gecombineerd kunnen worden. Na deze vijf stappen is het proces niet voltooid, het is noodzakelijk om te monitoren en te evalueren. Niet alleen het proces maar ook de gebruikte benadering en risicoprocesstappen dienen te worden geëvalueerd. De evaluatie dient niet te worden verward met de hiervoor beschreven processtap risico-evaluatie.

2.4 Risicomanagement benaderingen

In deze paragraaf wordt een selectie van relevante risicomanagement raamwerken, methoden en standaarden beschreven. Een raamwerk (Engels: framework) is een beschrijving van verantwoordelijkheden, taken, beleid en de wijze waarop risicomanagement is geïntegreerd in de werkprocessen van een organisatie. Een methode is meer specifiek en beschrijft vaak een stap voor stap werkproces waarmee een specifiek risico kan worden beheerst. Een standaard is een Internationaal geaccepteerde werkwijze, een relevant voorbeeld is de ISO 31000 standaard voor risicomanagement. Om de leesbaarheid te vergroten wordt in dit rapport de term 'benadering' gebruikt als overkoepelend begrip voor raamwerken, standaarden en methoden.
De selectie is gebaseerd op basis van uitgebreid literatuuronderzoek en documentanalyse maar is enigszins arbitrair. Er is tijdens de analyse van een aantal review-artikelen een voorselectie gemaakt op basis van de volgende criteria:

- De RM-benadering moet gangbaar zijn in Nederland. [3]
- De RM-benadering moet toepasbaar zijn binnen een publieke organisatie[4]
- De RM-benadering moet toepasbaar zijn binnen het cybersecurity domein[5].

[3] De gangbaarheid is bepaald aan de hand van een in 2009 en 2014 uitgevoerd onderzoek naar risicomanagement in Nederland (PWC, 2014). De top 3 benaderingen zijn geselecteerd.
[4] RM-benaderingen met een specifieke domeintoepassing zoals de financiële sector, de bouw sector, de medische sector of de maritieme sector zijn op voorhand buiten beschouwing gelaten. Een volledig overzicht van alle onderzochte RM-benaderingen is beschikbaar.
[5] Met toepasbaarheid is de context van de RM benadering onderzocht en beoordeeld. Bijvoorbeeld kwantitatieve methoden zijn buiten beschouwing gelaten.

In 2009 en 2014 is door de Nederlandse Beroepsorganisatie voor Accountants, Nyenrode, PwC en de Rijksuniversiteit Groningen (PWC, 2014) onderzoek gedaan naar risicomanagement in Nederland. In dit onderzoek zijn 727 bedrijven, zowel publiek als privaat, onderzocht op het gebruik van risicomanagement benaderingen. De top 3 benaderingen binnen de publieke sector en dus in lijn met de context van dit onderzoek is:

Top 3 risicomanagement benaderingen	
INK/EFQM model	31,5%
COSO	20,3%
ISO31000	12,0%
Overige (N=7)	36,2%

Tabel 4 Top 3 risicomanagement benaderingen (PWC, 2014)

Uit literatuuronderzoek (ENISA, 2022; Kure et al., 2022; Lambrinoudakis et al., 2022; Teymourlouei & Harris, 2019) specifiek gericht op cybersecurity risicomanagement is vervolgens de top drie benaderingen onderzocht die domein specifiek toegepast worden in cybersecurity. De bekendheid van deze benaderingen is gevalideerd in de interviews.

Top 3 cybersecurity risicomanagement benaderingen	
ISO/IEX 27005	Information security riskmanagement
NIST framework 800-39	Managing Information Security Risk This document developed by NIST provides guidance for an integrated, organisation- wide programme for managing information security risk to organisational operations.
BSI Germany Standard 200-3	Risk analysis based on IT-Grundschutz This methodology developed by the German Federal Office for Information Security demonstrates how the threats listed in the IT-Grundschutz Catalogues can be used to carry out a simplified analysis of risks for information processing

Tabel 5: Benaderingen cyber security risicomanagement (ENISA, 2022; Kure et al., 2022; Lambrinoudakis et al., 2022; Teymourlouei & Harris, 2019)

Tot slot zijn uit documentanalyse diverse binnen Defensie in gebruik zijnde benaderingen naar voren gekomen, deze benaderingen zijn in tabel 6 weergegeven. Deze tabel betreft een zo volledig mogelijk overzicht en heeft in deze fase van het onderzoek het toepassingsbereik cybersecurity nog buiten beschouwing gelaten.

Risicomanagement benaderingen binnen Defensie
Risico Inschatting en Evaluatie (RI&E)
Risico Analyse Operationeel (RAO)
Operationeel Risico Management
Taak Risico Analyse
Data Protectie Impact Analyse

Tabel 6 Risicomanagement benaderingen Defensie

Alle risicomanagement benaderingen worden hierna beknopt besproken en in hoofdstuk 3 onderling met elkaar vergeleken en beoordeeld.

2.4.1 INK EFQM model

Het Instituut Nederlandse Kwaliteit (INK) en de European Foundation for Quality Management (EFQM) hebben het INK kwaliteitsmanagement model gepubliceerd. Het model heeft vijf organisatiegebieden en vier resultaatgebieden. Verbeteren en vernieuwen vormt een overkoepelend aandachtsgebied binnen het model. Het model is gestoeld op (1) leiderschap, (2) vertrouwen, (3) samenwerking, (4) resultaatgerichtheid, (5) doorlopend verbeteren en vernieuwen (INK, 2023).

Figuur 8 Het INK management model (INK, 2023)

De sterkte punten van het model liggen in de relatie met de organisatie, het beleid en de strategie. Externe invloeden zoals waardering door klanten, medewerkers en maatschappij zijn belangrijke factoren. Een Zwak punt van dit model is dat het geen meetbare normen gebruikt. Het is met gebruikmaking van het INK model niet mogelijk de werkelijke situatie en de gewenste situatie te vergelijken. Tevens kent het model een breed toepassingsbereik waardoor de implementatie een veelomvattend proces is (van den Heuvel & Wondergem, 2005).

2.4.2 COSO

Het Committee of Sponsoring Organizations of the Treadway Commission (2017) heeft in 2004 het COSO-ERM ontwikkeld. COSO-ERM is een framework waarmee organisaties Enterprise Risk Management kunnen toepassen en is ontwikkeld in de financiële wereld . Het laatste framework dateert uit 2017 en heeft een focus op Governance, Culture, Strategy and Objective-Setting, Performance, Review and Revision, and Information, Communication and Reporting. Het framework is sterk intern gericht op beheersing. Het bestaat uit twintig principes, hierna zijn de principes die betrekking hebben op risicomanagement weergegeven:

Principles strategy & objective setting:

1. Analyze Business Context
2. Define Risk Appetite
3. Evaluate Alternative Strategies
4. Formulate Business Objectives

principles risk performance:

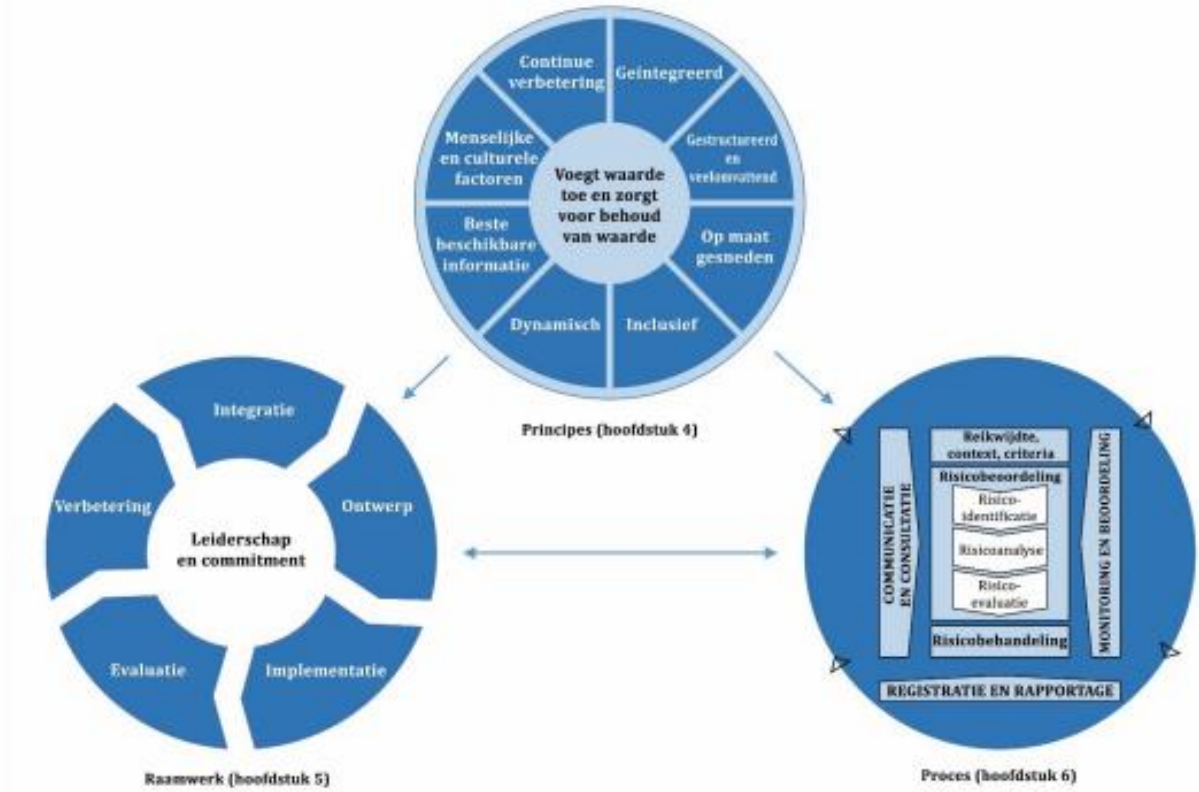
1. Identify Risk
2. Assess Severity of Risk
3. Prioritize Risk
4. Implement Risk Responses
5. Develop Portfolio View

Figuur 9: COSO-ERM framework (Committee of Sponsoring Organizations of the Treadway Commission, 2017)

COSO ERM is een risicomanagement benadering die gericht is op gebruik door het strategisch niveau van een organisatie, de laatste versie heeft aandacht voor cyber security risico's. Het framework beschrijft de impact van een cyber security verstoring op de doelstellingen van de organisatie. In de publicatie *managing cyber risk in a digital age* (COSO, 2019) wordt beschreven wat het belang van cybersecurity is voor organisaties en wordt in detail ingegaan op hoe het COSO ERM framework toepasbaar is voor cyber security risk management.

2.4.3 ISO 31000

De *International Organisation of Standardisation* (ISO) heeft in 2009 de eerste versie van de ISO 31000:2009 uitgebracht. Deze standaard bestaat uit de drie elementen (1) principes, (2) framework en (3) proces. ISO kan door ieder type organisatie gebruikt worden en verhoogd de waarschijnlijkheid van het behalen van organisatiedoelstellingen, identificatie van kansen en bedreigingen en effectiviteit.



Figuur 10: ISO 31000 standaard (ISO, 2018)

Een voordeel van de standaard is dat er in de implementatie veel ruimte is voor verder uitwerking binnen de context van een organisatie, de ISO 31000 standaard is daarmee breed toepasbaar. Voor veel organisaties is dit een groot voordeel omdat risicomanagement geïntegreerd moet worden in alle werkprocessen.

De standaard wordt beschouwd als de ‘moeder standaard’ voor risicomanagement binnen de ISO en kent een aantal context specifieke uitwerkingen. In relatie tot cyber security risicomanagement is de ISO 27005 de verbijzondering van de ISO 31000.

2.4.4 ISO 27000 series

De ISO 27000 serie van standaarden bestaat uit de ISO27001, deze standaard beschrijft de principes van cyber security en is geschreven om organisaties te helpen de basis te leggen voor het beleid. De ISO27002 beschrijft de implementatie van het cyber security beleid en is binnen de Nederlandse overheid de basis voor de Baseline Informatiebeveiliging Overheid (BIO) waarover eerder in dit rapport geschreven is. De ISO 27005 gaat dieper in op cyber security risicomanagement. De standaarden zijn breed toepasbaar in zowel publieke als private organisaties. De ISO 27005 cyber security risicomanagement heeft als doel risico’s te beheersen die compromitatie van informatie als gevolg heeft. De volgende stappen vormen de kern van deze standaard;

- Context vaststellen
- Inschatting van het risico
- Nemen van maatregelen
- Accepteren van (rest) risico
- Communicatie
- Monitoring en evaluatie.

De standaard is gebaseerd op de ISO 31000 en kent veel overeenkomsten. De ISO 27005 is een verbijzondering van de meer algemene ISO 31000 standaard en heeft informatiebeveiliging als belangrijkste toepassingsbereik (Everett, 2011). Een groot voordeel van de ISO 27005 ten opzichte van de ISO 31000 is dat de standaard helpt met het identificeren van het IT landschap binnen de organisatie, cyberdreiging, kwetsbaarheden en oorzaken, gevolg en waarschijnlijkheid in kaart brengt (Everett, 2011; Ferreira, 2020; Kosutic, 2022). Door deze specificatie stelt de standaard organisaties in staat om doeltreffend cyber security risico’s in kaart te brengen.

2.4.5 NIST series

Het Amerikaanse National Institute of Standards and Technology (NIST) heeft een aantal benaderingen uitgebracht waarvan er twee worden besproken, het NIST Cyber Security Framework (NIST CSF) en de NIST 800-39.

Het NIST CSF is een risicomanagement proces waarmee organisaties de basis te leggen voor cyber security risicomanagement en bestaat uit de elementen *core, tiers* en *profiles*. De *core*, ofwel kern van de benadering kent 5 opvolgende stappen:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

De benadering richting zich in relatie tot cybersecurity op interne en externe invloeden van organisaties en kent overeenkomsten met de ISO 27000 serie. De toepassing van het NIST CSF is technisch van aard en de benadering beschrijft concrete maatregelen voor een organisatie. De stap *identify* kent bijvoorbeeld de subcategorie *asset management* die voorschrijft dat het gehele IT landschap van de organisatie in kaart gebracht dient te worden (Roy, 2020).

NIST 800-39 beschrijft het pad naar een integraal en organisatie breed programma voor cyber security risicomanagement en is geschikt om in samenhang met andere NIST en/of ISO standaarden te gebruiken. Het NIST CSF is zelfstandig te implementeren door organisaties, het vereist (beperkte) technische kennis. De standaard is, gelijk aan de ISO standaarden, eenvoudig aan te passen aan de behoefte en context van de organisatie (NIST, 2011).

Ten tijden van schrijven is het NIST de tweede versie van het CSF aan het ontwikkelen, omdat deze nog niet formeel gepubliceerd is wordt versie 1.1 gebruikt in dit onderzoek.

2.4.6 BSI Germany Standard

De BSI STANDARD 200-1, 200-2 en 200-3 zijn drie standaarden voor het management van informatiebeveiliging die in te richten zijn naar de specifieke context van een organisatie. De 200-1 is gebaseerd op de ISO 27001, de 200-2 op de ISO27002 en de 200-3 kent overeenkomst met de ISO27005. De standaard bevat drie elementen; *'Standard Protection', 'Base Protection,* en *'Core Protection'* (Bundesambt fur Sicherheit in der Informationstechnik, 2017).

Het belangrijkste verschil met de ISO standaarden en in mindere mate met de NIST series is dat de BSI een zeer uitgebreid en modulair framework is. Waar de ISO standaarden bestaan uit enkele tientallen pagina's met algemeen geformuleerde instructies, gaat NIST verder met een paar honderd pagina's. Het BSI kent meer dan duizend pagina's met gedetailleerde beschrijvingen van maatregelen (Bundesambt fur Sicherheit in der Informationstechnik, 2017). Een groot voordeel is dat de BSI minder ruimte laat voor eigen interpretatie van cyber security maatregelen (Mahmoud et al., 2020). Organisaties kiezen de gewenste modules en kunnen van start. Het is organisatie afhankelijk of de mate van detail in het BSI toepasbaar is, voor sommige organisaties is flexibiliteit en eigen inrichting wellicht gewenst

2.4.7 Benaderingen in gebruik binnen Defensie

Bij het Ministerie van Defensie zijn een aantal risicomanagement benaderingen in gebruik. Deze zijn weergegeven in tabel 7. voorzien van een toelichting en het toepassingsbereik.

Risicomanagement benaderingen binnen Defensie	
Risico Inschatting en Evaluatie (RI&E) (Ministerie van Defensie, 2023)	Identificeren, analyseren en treffen van maatregelen tav veiligheidsrisico's.
Risico Analyse Operationeel (RAO)(Ministerie van Defensie, 2021b)	Gericht op veiligheid onder operationele omstandigheden, bijvoorbeeld tijdens missies.
Operationeel Risico Management (Kunstt, 2020)	Voorkómen van ongevallen en incidenten door proactief risico's te identificeren, te beoordelen en te beheersen.
Taak Risico Analyse (Ministerie Van Defensie, 2019)	Analyse gericht op gevaren voortkomend uit risicovolle werkzaamheden, gericht op veiligheid en gezondheid van medewerkers.
Data Protectie Impact Analyse (Autoriteit Persoonsgegevens, 2017)	Risicoanalyse voor privacymanagement aan de hand van AVG wetgeving.

Tabel 7 Risicomanagement benaderingen binnen Defensie met toelichting en toepassing.

2.5 Criteria voor risicomanagement uit de literatuur

Het doel in dit onderzoek is het ontwikkelen van een risicomanagement benadering waarmee de Koninklijke Marechaussee in staat wordt gesteld om op een effectieve wijze cybersecurity risico's te beheersen. Om tot een ontwerpbenadering te komen is van belang criteria vast te stellen waaraan het ontwerp dient te voldoen. In deze paragraaf is het literatuuronderzoek uiteengezet dat leidt tot een initiële set aan ontwerpcriteria. In het volgende hoofdstuk worden hier twee sets aan criteria vanuit de praktijk aan toegevoegd.

Van Staveren (2009) heeft voor zijn proefschrift onderzoek gedaan naar de implementatie van risicomanagement in organisaties en beschrijft dat het implementeren van risicomanagement 'het uitvoeren van alle activiteiten die het routinematig toepassen van risicomanagement mogelijk maken' (Van Staveren, 2009). Hij beschrijft een conceptueel model bestaande uit drie dimensies: (1) risicomanagement methodologieën, (2) risico management gebruikers en (3) sociale systemen.
De dimensie risicomanagement methodologieën is in de context van dit onderzoek relevant en beschrijft 8 kenmerken en daaruit afgeleid 18 criteria waaraan een risicomanagement benadering dient te voldoen. Het onderzoek toont aan dat het erkennen van deze kenmerken en criteria essentieel is voor het genereren van de noodzakelijke motivatie en toewijding bij de gebruikers van de benadering (Van Staveren, 2009).
De gebruikers dimensie bestaat uit vijf groepen risicomanagement gebruikers gedefinieerd naar Rogers (2003), te weten; innovators, early adopters, early majority, late majority en laggards.
De dimensie sociale systemen bestaat uit 22 condities voor de realisatie van de noodzakelijke criteria en sub-criteria waaraan het sociale systeem van een organisatie dient te voldoen. Het erkennen van het belang van het sociale systeem wordt geregeld onderschat of zelfs genegeerd binnen organisaties.

Dit onderzoek is gericht op de eerste dimensie, de risicomanagement methodologieën. De andere twee dimensies zijn van belang voor de uiteindelijke implementatie van risicomanagement binnen een organisaties maar vallen buiten de scope van dit onderzoek.

In tabel 8 zijn de criteria, sub-criteria en kernvoorwaarden voor risicomanagement methodologieën weergegeven.

Kenmerk	Sub-kenmerk	Kernvoorwaarden voor risicomanagement methoden
Relatief voordeel	Economisch	RM is kosteneffectief
	Sociale status	RM geeft sociale status
	Over-adoptie	RM vermijdt instrument focus
	Preventief	RM genereert preventie
	Beloning	RM wordt beloond
	Mandaat	Top management ondersteunt RM
Compatibilieit	Overtuigingen	RM sluit aam bij overtuigingen
	Werkprocessen	RM past in bestaande werkprocessen
	Behoeften	RM vervult behoeften
	Bijeffecten	RM versterkt innovativiteit
	Naam	RM heeft een positief imago
Complexiteit		RM is eenvoudig uitvoerbaar
Oefenbaarheid		RM is eenvoudig te proberen
Zichtbaarheid		Effecten van RM zijn meetbaar
		Voorbeelden demonstreren RM succes
Netwerkeffecten		Externe partijen ondersteunen RM
Prijs		RM kosten zijn acceptabel
Relatief nut		RM verhoogt de betrouwbaarheid van de organisatie

Tabel 8 de criteria, sub-criteria en kernvoorwaarden uit Risk, Innovation en Change (Van Staveren, 2009)

Een literatuurstudie uitgevoerd door Oliveira et al (2019) brengt 10 criteria naar voren, deze criteria zijn weergegeven in tabel 9. De criteria uit de tabellen 8 en 9 samen vormen een relevante en actuele wetenschappelijke basis waarmee het empirisch onderzoek is vormgegeven en uitgevoerd.

Criteria voor risicomanagement uit Oliveira et al (2019).
Toewijding top management
Vaststellen risicobereidheid is essentieel voor succes
Risicomanangement creëert kansen
Aanwezigheid van risicomanagers
Bewustwording van risico's
Beschikbaarheid van middelen voor uitvoering risicomanagement
Een werkproces voor de uitvoering van de risicoprocesstappen
Monitoren en evalueren van risicomanagement
Risicocommunicatie
In lijn met interne regelgeving, procedures en wetgeving.

Tabel 9 criteria voor risicomanagement (Oliveira et al., 2019)

Vanuit de praktijk zijn aan de hand van zowel interviews als interne bedrijfsdocumentatie twee aanvullende sets aan criteria vastgesteld. Deze worden in samenhang beschouwd en zullen resulteren in een definitieve set criteria waar de cybersecurity risicomanagement benadering aan dient te voldoen.

2.6 Samenvatting en deelconclusie

Dit hoofdstuk afsluitend kan deelvraag 1 worden beantwoord:

Deelvraag 1: Wat is de stand van de huidige wetenschappelijke- en vakliteratuur over risicomanagement in relatie tot cybersecurity?

Samengevat kan worden vastgesteld dat cybersecurity bestaat uit een aantal met elkaar in samenhang zijnde elementen (figuur 3). Hierbij zijn de elementen risico, kwetsbaarheid, impact en dreiging in relatie tot risicomanagement het meest relevant. Het is belangrijk deze begrippen in de juiste context te gebruiken.

Binnen MinDef wordt zeer beperkt cybersecurity risicomanagement toegepast, verschillende aanwijzingen en instructies vormen het Defensie Beveiligingsbeleid waarmee de organisatie beoogd de Beschikbaarheid, Exclusiviteit en Integriteit van haar data te beschermen. Deze bescherming is schaalbaar en verdeeld in 4 categorieën van Te Beschermen Belangen.

In dit hoofdstuk is deelvraag 1 beantwoord en is uiteengezet welke begrippen in de context van dit onderzoek relevant zijn, hoe deze zich tot elkaar verhouden en is beknopt ingegaan op hoe MinDef haar beleid heeft geformuleerd ten aanzien van cyber security en risicomanagement. Vervolgens is op basis van Van Staveren (2009) en Oliveira et al (2019) een eerste set aan criteria vastgesteld voor het ontwerp. In het volgende hoofdstuk zal worden beschouwd hoe het risicomanagement in de praktijk uitgevoerd wordt. Daarna zal worden geanalyseerd wat de criteria zijn voor het ontwerp van een risicomanagement benadering.

3. De praktijk: Risicomanagement binnen de Koninklijke Marechaussee

In dit derde hoofdstuk wordt het praktijk deel van dit onderzoek beschreven, dit hoofdstuk vormt stap 2 van de *problem solving cycle*; de analyse en diagnose.

Dit hoofdstuk bestaat uit drie delen, in paragraaf 3.1 wordt in aanvulling op de methodologie uit hoofdstuk 1 beschreven hoe het empirisch onderzoek is uitgevoerd. In paragraaf 3.2 wordt de theorie beschreven vanuit interne documentatie zoals beleidstukken, aanwijzingen, nota's en presentaties.

Daarna zullen in paragraaf 3.3 de resultaten van de interviews worden uitgewerkt. Paragraven 3.2 en 3.3 worden beiden afgesloten met een set aan ontwerpcriteria.

Hoofdstuk 3 wordt afgesloten met een samenvatting en tussenconclusie waarin de definitieve set aan criteria voor het ontwerp zal worden geselecteerd, tot slot zal deelvraag 2 worden beantwoord.

3.1 Methodologie praktijkonderzoek

Er is gekozen voor een casestudy omdat dit de mogelijkheid biedt aan de hand van een praktijkprobleem medewerkers uit de organisatie te interviewen en hierbij de diepte in te gaan in plaats van de breedte. Er is gekozen voor medewerkers uit verschillende delen van de organisatie maar allen werkzaam binnen eenzelfde context. Deze medewerkers zijn allen op strategisch niveau op enigerlei wijze betrokken bij cybersecurity. De medewerkers zijn verdeeld in twee categorieën.

- Medewerkers werkzaam binnen JIVC, de IT organisatie van MinDef.
- Medewerkers werkzaam binnen de KMar en Bestuursstaf

Er is gekozen voor deze selectie omdat uit het theorie onderzoek is gebleken dat deze twee categorieën medewerkers een verschillende rol hebben in de governance van cybersecurity binnen de KMar. Binnen de context van dit onderzoek is het waardevol te onderzoeken of dit verschil leidt tot overeenkomsten of verschillen in zienswijze ten aanzien van risicomanagement. Een overzicht van de respondenten met bijbehorende functie is vanwege herleidbaarheid niet opgenomen als bijlage maar separaat beschikbaar.

3.1.1 Empirisch onderzoek / Interviews

In dit onderzoek wordt de *problem solving cycle* van Aken en Berends (2018) gebruikt waarbij specifiek de stappen 1, 2 en 3 worden doorlopen. Omdat uit het vooronderzoek is gebleken dat de probleemstelling het ontbreken van inzicht in cybersecurity risico's luidt, en er geen raamwerk, standaard of methode voor risicomanagement in gebruik is, is er gekozen voor een inductief onderzoek. Hierbij wordt er vanuit de empirie gezocht naar generaliseerbare inzichten (Aken en Berends, 2018). Inductief redeneren is goed toepasbaar in dit onderzoek omdat er in deze context geen theorie is die getoetst kan worden.

Er is in dit onderzoek gebruik gemaakt van de *'grounded theory'* benadering, onder andere beschreven in Glaser & Strauss (1967) en meer recent door Boeije & Bleijenbergh (2019)
De *'grounded theory'* ofwel de gefundeerde theoriebenadering is een kwalitatieve methode gericht op theorievorming. De theorie ontstaat langzaam maar zeker tijdens het onderzoek. Er wordt op een inductieve wijze van het bijzondere (de feiten) naar het algemene (de theorie) geredeneerd. Tijdens het onderzoek wordt opgedane informatie uit interviews voortdurend met elkaar vergeleken om op deze wijze te zoeken naar overeenkomsten en verschillen. Aan de hand daarvan ontstaan zogenoemde *sensitizing concepts* (Baarda, 2013; Verschuren & Doorewaard, 2021). Dit zijn richtinggevende begrippen die in het begin van het onderzoek nog wat vaag en betekenisloos zijn, gaandeweg het onderzoek krijgen deze begrippen meer inhoud en kunnen geoperationaliseerd worden waarmee ze een algemener karakter krijgen en bruikbaar zijn voor theorievorming, in de context van dit onderzoek dienen deze begrippen het doel te komen tot ontwerpcriteria voor de risicomanagement benadering.

De interviews zijn semigestructureerd vormgegeven aan de hand van 4 vragen. Een voordeel van deze vorm van interviewen is dat er door de open structuur ruimte is om tijdens het gesprek door te vragen en relevante nieuwe kennis op te doen. De vragenlijst is opgesteld aan de hand van het vooronderzoek (probleemstelling en doelstelling) en het theoretisch kader uit hoofdstuk 2. Er is bewust gekozen voor een beperkte hoeveelheid vragen om voldoende ruimte te laten voor doorvragen om diepte te creëren in de antwoorden in plaats van breedte.

De volgende vragen zijn gesteld, het interviewprotocol is toegevoegd als bijlage 1.

- Met welke risico's heeft de KMar te maken ten aanzien van cyber security?
- Hoe is risicomanagement ten aanzien van cybersecurity momenteel ingericht?
- Wat zijn belangrijke verbeterpunten ten aanzien van cybersecurity risicomanagement?
- Wat zijn belangrijke aandachtspunten bij de implementatie van verbeteringen in de wijze waarop risicomanagement wordt uitgevoerd?

3.1.2 Analyse en verwerking van data

Alle interviews zijn uitgewerkt tot een samenvatting, deze is ter validatie aangeboden aan de respondenten waarbij in sommige gevallen aanvullingen of aanpassingen zijn toegevoegd. Na goedkeuring van de resultaten door de respondenten zijn deze verwerkt in een resultatenmatrix.

Om de in dit onderzoek verzamelde data te kunnen analyseren is gebruik gemaakt een resultaten matrix (Baarda, 2013; Verschuren & Doorewaard, 2021). In de matrix is per interviewvraag en per respondent de kern van het gegeven antwoord weergegeven, dit wordt verdichting van de data genoemd (Verschuren &

Doorewaard, 2021). Aan de hand van de informatie in de matrix is inzichtelijk gemaakt welke aanknopingspunten er zijn voor ontwerpcriteria ten behoeve van de risicomanagement benadering.

3.2 Risicomanagement binnen de KMar, het beleid vanuit documentanalyse

Het cyberdomein binnen de Koninklijke Marechaussee is diffuus en complex, de organisatie heeft diverse taken, rollen en verantwoordelijkheden in relatie tot cyber. Zo heeft de KMar een rechts-handhavende taak waarbinnen activiteiten worden uitgevoerd die erop gericht zijn om controle of toezicht uit te voeren krachtens de Politiewet 2012 of de Vreemdelingenwet 2002. Een opsporende taak, hieronder wordt verstaan; het verzamelen, registeren en verwerken van gegevens of informatie door de KMar over (de voorbereiding van) crimineel handelen en criminele organisaties om te komen tot vervolging, voorkoming of beëdiging van dit handelen of deze organisaties (Koninklijke Marechaussee, 2022).
Een inlichtingen taak, hieronder wordt verstaan; het verzamelen, verwerken en interpreteren van gegevens voor het nemen van gefundeerde beslissingen. Naast genoemde cyberactiviteiten binnen de taakvelden van de KMar is veiligheid van de eigen IT systemen van cruciaal belang (Koninklijke Marechaussee, 2022). Alle operationele en ondersteunende processen van de organisatie zijn gedigitaliseerd. Cybersecurity richt zich, als reeds benoemd in het eerste hoofdstuk van dit onderzoek, op het voorkomen van schade aan, de bescherming van, en in voorkomend geval het herstel van het brede scala aan IT systemen van de organisatie.

Risicomanagement vormt een besturingsprincipe binnen het Besturingsmodel Defensie (BBD) (Ministerie van Defensie, 2012). Dit betekent dat de KMar risico's integraal inzichtelijk maakt, zodat deze op adequate wijze beoordeeld en beheerst kunnen worden. In de afgelopen jaren werden binnen de KMar risico's vaak gefragmenteerd – binnen functionele domeinen – geïnventariseerd en beheerst (Koninklijke Marechaussee, 2023).

Het ultieme doel van risicomanagement binnen Defensie is om bij te dragen aan het vergroten van de inzet van militair vermogen. Doordat er in de aanloop naar inzet door het beheersen van risico's minder materieel en personeel uitvalt, is er meer militair vermogen beschikbaar voor die inzet. Dit wordt gerealiseerd door Defensie om te vormen naar een meer risicovolwassen organisatie. Op die manier wordt de Defensie organisatie wendbaarder.

Het vergroten van militair vermogen geschiedt door aan de voorkant, proactief, risico's te detecteren, mogelijke verliezen te mitigeren of te voorkomen en anderzijds de potentiële opbrengsten te verbeteren of te optimaliseren. Daarbij dient acceptatie van (rest)risico's op het juiste niveau in de organisatie plaats te vinden. De SG-Aanwijzing 002, Besturen bij Defensie (Ministerie van Defensie, 2012) beschrijft

risicomanagement als: ‘een middel om het militair vermogen te vergroten, om doelstellingen te realiseren met het oog voor belangen vanuit verschillende perspectieven, en om compliant te zijn met wet- en regelgeving’.

Dat de KMar risicomanagement nog niet zo lang als zodanig benoemd in (strategische) beleidsdocumenten betekent niet dat er in zijn geheel nog geen risicomanagement toegepast wordt. Het ontbreekt nog aan een samenhangend stelsel van risico identificatie en beheersing. Risicomanagement wordt binnen verschillende risicogebieden/domeinen in meer of mindere mate toegepast, maar niet of nauwelijks beredeneerd vanuit (strategische) doelstellingen. Risico’s worden daar gefragmenteerd – binnen domeinen – geïnventariseerd en beheerst. Zoals eerder genoemd vooral prominent binnen het domein (fysieke) veiligheid maar ook op het gebied van integriteit en integrale beveiliging vindt er risicomanagement plaats.

Risicomanagement is niet nieuw voor Defensie, maar het beheersen van risico’s op een integrale manier is nog geen onderdeel van de dagelijkse bedrijfsvoering, noch zijn er KPI’s voor risicomanagement op inhoudelijk gebied, noch procesindicatoren waarmee Defensie de vorderingen van risicomanagement kan volgen.

3.3 Criteria vanuit het beleid

Uit de analyse van de interne documentatie zijn een aantal criteria naar voren gekomen, deze zullen in tabel 9 worden weergegeven een vormen samen met de eerder in de literatuur gevonden criteria en de criteria uit de interviews de definitieve ontwerpcriteria. De in tabel 9 beschreven criteria zijn afgeleid uit een rapport van het Nederlands Lucht- en Ruimtevaartcentrum dat in 2021 een onderzoek naar risicomanagement binnen Defensie heeft uitgevoerd (NLR, 2021). De SG aanwijzing 007 Risicomanagement (Ministerie van Defensie, 2023), het implementatieplan KMar (Koninklijke Marechaussee, 2023), het VMS Defensie (Ministerie Van Defensie, 2019) en een in 2020 geschreven masterthesis naar risicomanagement binnen een operationele brigade van de KMar (Kunstt, 2020).

Ontwerpcriteria uit interne documentatie
Risicomanagement is een verantwoordelijkheid van de lijn
Risicomanagement heeft een zo beperkt mogelijke extra belasting van bestaande capaciteit, structuren en processen
Risicomanagement sluit zo goed mogelijk aan bij bestaande processen
Het top management is betrokken en heeft de juiste “tone at te top”
Eerstelijns rollen[1] zijn betrokken en beschikken over kennis en motivatie om leiding en sturing te geven[i]
Tweedelijns rollen beschikken over inhoudelijke expertise, capaciteit en betrokkenheid
Risicomanagement wordt ondersteund met leiderschap en voorbeeldgedrag
Risicomanagement wordt onderworpen aan interne auditing
Risicomanagement dient een ondersteunend ICT systeem te gebruiken.
Risicomanagement dient uitgevoerd te worden aan de hand van uniforme producten en een eenduidige begrippenkader
Duidelijkheid in taken, verantwoordelijkheden en bevoegdheden.
Zorg voor zichtbare resultaten om draagvlak en motivatie te verhogen

Tabel 10: Ontwerpcriteria uit interne documentatie.

[1] Three Lines Model, Murdock (2018)

3.4 Risicomanagement binnen de KMar, de interviews

In deze paragraaf worden de resultaten van de 8 afgenomen interviews gepresenteerd. Nadat de respondenten de interviews hebben gevalideerd zijn alle resultaten verwerkt in een resultatenmatrix. Met behulp van de matrix is het mogelijk om per onderwerp uit het interview de antwoorden overzichtelijk weer te geven. In deze paragraaf zijn de resultaten per interview vraag uitgeschreven, soms voorzien van relevante quotes. Daarna is per onderwerp een beknopte samenvatting gegeven. Deze paragraaf sluit af met de criteria vanuit de interviews.

3.4. Criteria uit interviews

De uitwerking van de interviews is in de publieke versie van dit onderzoek niet opgenomen. De resultaten van de interviews zijn in de onderstaande tabellen weergegeven.

Ontwerpcriteria cybersecurity risicomanagement uit interviews (1)
Het verhoogd kennis over risicomanagement
Het creëren van rolduidelijkheid en structuur
Het vergroten van het inzicht in cybersecurity risico's
Het bepalen van de risicobereidheid binnen organisatie
Het vergroten van de kennis over cyber security risico management
Het gebruik van een risicomanagement benadering

Tabel 11: Ontwerpcriteria cybersecurity risicomanagement.

De belangrijkste aandachtspunten bij de implementatie van verbeteringen in de wijze waarop risicomanagement wordt uitgevoerd zijn:

Ontwerpcriteria voor implementatie van cybersecurity risicomanagement uit interviews (2)
Het vergroten van de noodzakelijke kennis in risicomanagement.
Het creëren van draagvlak voor-, een heldere doelstelling van- en een duidelijke output van de risicomanagement benadering.
De benadering dient aan te sluiten bij bestaande werkprocessen.
De samenwerking tussen JIVC en de KMar dient te worden verstrekt, waarbij aandacht is voor wederzijdse communicatie.
De personele capaciteit voor de implementatie en uitvoering van risicomanagement dient te worden vergroot.
De implementatie dient zorgvuldig plaats te vinden waarbij er niet louter op laaghangend fruit gestuurd wordt.

Tabel 12: Ontwerpcriteria voor implementatie.

3.5 Conclusie hoofdstuk 3

Aan de hand van documentanalyse en interviews is in dit hoofdstuk gezocht naar criteria voor een cybersecurity risicomanagement benadering die in het volgende hoofdstuk van dit onderzoek zal worden ontworpen. Eerder zijn de criteria vastgesteld vanuit literatuuronderzoek, tevens is deelvraag 2 nu beantwoord.

Deelvraag 2: Op welke wijze wordt risicomanagement ten aanzien van cybersecurity toegepast binnen de Koninklijke Marechaussee?

Het is nu mogelijk de criteria uit het literatuuronderzoek (hoofdstuk 2), de documentanalyse (hoofdstuk 3.1) en de interviews (hoofdstuk 3.3) samen te voegen en hoofdstuk 3 af te sluiten met een matrix waarin de ontwerpcriteria worden gepresenteerd.

Ontwerpcriteria		
Literatuuronderzoek	**Documentanalyse**	**Interviews**
RM is kosteneffectief		
RM geeft sociale status		
RM vermijdt intrument bias	RM dient een ondersteunend ICT systeem te gebruiken	
RM genereert preventie		RM zorgt voor vroegtijdige risico identificatie
RM wordt beloond	RM zorgt voor zichtbare resultaten om motivatie en draagvlak te vergroten	RM dient waarde toe te voegen
Top management ondersteunt RM	RM is verantwoordelijkheid van de lijn	RM dient opgedragen te worden
	Top management is betrokken en heeft juiste 'tone at the top'	Juiste tone at the top is belangrijk
RM sluit aan bij overtuigingen		
RM past in bestaande werkprocessen	RM sluit zo goed mogelijk aan bij bestaande processen	RM sluit aan bij bestaande processen
RM vervult de behoeften	RM zorgt voor duidelijkheid in taken, verantwoordelijkheden en bevoegdheden	RM moet waarde toevoegen, geen losstaand proces zijn.
RM verstrekt innovativiteit		
RM heeft een positief imago	Top is betrokken en gemotiveerd en geeft leiding en sturing	Top down opdragen met duidelijke boodschap
RM is eenvoudig uitvoerbaar	RM dient te worden uitgevoerd aan de hand van uniforme producten / eenduidig begrippenkader	RM uitvoeren aan de hand van eenduidig kader
RM is eenvoudig te proberen		
Effecten van RM zijn meetbaar	RM zorgt voor zichtbare resultaten	RM creert zichtbare output
Voorbeelden demonstreren RM succes		
Externe partijen ondersteunen RM		
RM kosten zijn acceptabel	RM heeft zo beperkt mogelijke extra belasting van capaciteit	Voor RM dient aanvullende capaciteit te worden vrijgemaakt
RM verhoogd betrouwbaarheid organisatie		
		RM creert rolduidelijkheid en structuur
		RM verhoogd de risicovolwassenheid
	RM wordt onderworpen aan interne auditting	
	RM wordt ondersteund met leiderschap en voorbeeldgedrag	
		RM vergroot kennis

Figuur 11: Ontwerpcriteria, 3 sets

4. Het ontwerp

In dit hoofdstuk wordt het ontwerp van de cybersecurity risicomanagement benadering beschreven.

4.1 Inleiding ontwerp

Nu de ontwerpcriteria zijn vastgesteld is het mogelijk om een benadering te ontwerpen voor cyber security risicomanagement. In dit onderzoek wordt gebruik gemaakt van de *problem solving cycle* van Aken & Berends (2018). In hoofdstuk 1.3 is het onderzoeksmodel gepresenteerd, stap 2 van het onderzoeksmodel beschrijft de vergelijking van de ontwerpcriteria met bestaande risicomanagement benaderingen en stap 3 het uiteindelijke ontwerp, dit hoofdstuk beschrijft stap 2 en 3.

Een ontwerp dient volgens Wijnen en Storm (2007) te voldoen aan vier eisen:

1. Functionele eisen
2. Operationele eisen
3. Randvoorwaarden
4. Ontwerpbeperkingen

Functionele eisen beschrijven wat een ontwerp moet kunnen, ofwel de behoefte van de opdrachtgever. Operationele eisen zijn kenmerken van het ontwerp, de behoeften van de gebruikers. Randvoorwaarden beschrijven normen of wetgeving waaraan een ontwerp dient te voldoen. Ontwerpbeperkingen zijn eisen die gaan over het onderzoek zelf.

In de volgende paragraaf zal de definitieve selectie van ontwerpcriteria worden weergegeven, deze selectie is tot stand gekomen vanuit de analyse van de drie sets aan ontwerpcriteria weergegeven in figuur 11. Er is gezocht naar overeenkomsten en verschillen tussen de criteria uit de literatuur, de documentanalyse en de interviews. Dit levert 6 ontwerpcriteria op, dit betreffen zowel functionele als operationele ontwerpeisen.
In dit onderzoek zijn geen randvoorwaarden of ontwerpbeperkingen naar voren gekomen.

4.2 Definitieve selectie ontwerpcriteria

In figuur 11 zijn de ontwerpcriteria met elkaar in verband gebracht, er zijn overeenkomsten en verschillen gevonden binnen de sets. De onderstaande tabel geeft de definitieve selectie weer.

Ontwerpcriteria
1. RM creëert zichtbare vooruitgang.
2. RM sluit aan bij bestaande werkprocessen.
3. RM voldoet aan behoefte.
4. RM is eenvoudig toe te passen met structuur.
5. RM zorgt voor zichtbaar resultaat.
6. De personele capaciteit benodigd voor de toepassing van risicomanagement is in verhouding met het gewenste resultaat.

Tabel 13 Definitieve selectie

Toelichting op de definitieve selectie:

1. RM creëert zichtbare vooruitgang, de toepassing van risicomanagement dient de organisatie te helpen met het creëren van vooruitgang binnen het cyberdomein van de organisatie. Het creëert overzicht in het IT-landschap, inzicht in cybersecurity risico's en maakt effectieve en efficiënte beheersing van risico's mogelijk.
2. Risicomanagement past binnen en sluit aan op bestaande werkprocessen en maakt daarmee *'risicogestuurd werken'* (Staveren, 2015) mogelijk.
3. Risicomanagement vervult de behoeften van de organisatie, duidelijkheid in taken, rollen en verantwoordelijkheden.
4. Risicomanagement is met gebruikmaking van een duidelijke structuur eenvoudig toe te passen.
5. Risicomanagement zorgt voor zichtbare en meetbare resultaten. De effecten van genomen maatregelen worden zichtbaar, zowel intern in alle lagen van de organisatie als extern bij ketenpartners. Het aantal cybersecurity incidenten wordt minder.
6. De personele capaciteit benodigd voor de toepassing van risicomanagement is in verhouding met het gewenste resultaat.

Naast de ontwerpcriteria zijn er twee criteria bepaald die beiden van belang zijn voor de implementatie van het ontwerp maar geen directe selectiecriteria vormen waarop de bestaande risicomanagement benaderingen kunnen worden gescoord, deze criteria zijn daarom niet meegewogen in het ontwerp maar vormen wel input voor de aanbevelingen voor implementatie later in dit rapport.

1. Risicomanagement is een verantwoordelijkheid van de lijn en dient top down opgedragen te worden, de juiste *'tone at the top'* is essentieel.
2. De voordelen van risicomanagement worden positief uitgedragen, hierbij is de top van de organisatie betrokken, gemotiveerd en geeft zij leiding en sturing aan de implementatie.

Aan de hand van de 6 definitieve criteria zullen in de volgende paragraaf de in hoofdstuk 2.4 geselecteerde risicomanagement benaderingen worden gescoord.

4.3 Score bestaande benaderingen

In tabel 13 worden uitsluitend benaderingen vergeleken die in hoofdstuk 2.4 zijn beschreven. Domein specifieke benaderingen, benaderingen die niet toepasbaar zijn binnen de publieke sector en benaderingen die niet gangbaar zijn in Nederland zijn buiten beschouwing gelaten. Daarnaast zijn de benaderingen die specifiek binnen MinDef in gebruik zijn (zie tabel 6) buiten beschouwing gelaten omdat deze allen fysieke veiligheid, arbo veiligheid of operationele veiligheid als toepassingsbereik hebben. Dit maakt deze benaderingen op voorhand ongeschikt voor de uitvoering van cyber security risico management.

De scores zijn bepaald aan de hand van de handleidingen, voorschriften, artikelen en bronteksten van de 6 benaderingen. Er is gebruik gemaakt van een multicriteria-analyse (Mendoza et al., 1999). Deze wetenschappelijke methode is zeer geschikt om keuzes te rationaliseren. In de context van dit onderzoek dient de analysemethode tevens om op een transparante en navolgbare wijze te laten zien hoe het ontwerp tot stand is gekomen zonder daarbij alle benaderingen gedetailleerd op te nemen in dit rapport. Alle gebruikte literatuur is opgenomen in de bibliografie van dit rapport. Er is gebruik gemaakt van een ordinaire schaal waarbij score 2 inhoudt dat de benadering geheel voldoet aan het criterium, bij score 1 voldoet deze niet volledig/deels, bij score 0 voldoet de benadering niet aan het criterium.

	INK/EFQM	COSO-ERM	ISO31000	ISO27005	NIST CSF	BSI 200
RM creëert vooruitgang	1	2	2	2	2	2
RM sluit aan bij bestaande werkprocessen	0	0	2	2	1	0
RM voldoet aan behoefte/governance	0	1	2	2	2	2
RM is eenvoudig toe te passen met structuur	1	0	2	2	2	1
RM zorgt voor zichtbaar resultaat	2	2	1	2	2	2
Capaciteit voor RM in verhouding met resultaat	1	0	2	2	2	0
Totaal score	**5**	**5**	**11**	**12**	**11**	**8**

Tabel 14: Scores risicomanagement benaderingen

Een conclusie op basis van de tabel is dat de ISO 27005 standaard het hoogst scoort en op alle criteria de maximale score behaald. De ISO 31000 en het NIST Cyber Security Framework (NIST CSF) volgen daarna. NIST CSF scoort alleen op het criterium; risicomanagement sluit aan bij bestaande werkprocessen een lagere score omdat de documentanalyse en de interviews aantonen dat het NIST CSF binnen sommige onderdelen van MinDef in gebruik is maar geen basis kent binnen het beleid zoals de ISO standaarden dit wel kennen in bijvoorbeeld de aanwijzing risicomanagement A007 (Ministerie van Defensie, 2023).

De BSI standaard scoort laag op de criteria; risicomanagement sluit aan bij bestaande werkprocessen en capaciteit voor risicomanagement staat in verhouding met het resultaat. Oorzaak is het uitgebreide implementatieplan waarin zeer beperkt ruimte is voor aanpassing naar de specifieke context van de KMar organisatie. Daarnaast zal implementatie veel capaciteit kosten omdat het risicomanagement naar de BSI standaard zeer technisch van aard is.

4.4 Keuze definitief ontwerp

Nu duidelijk is dat de ISO 27005 en ISO 31000 standaarden en het NIST Cyber Security Framework de hoogste scores behalen wordt in deze paragraaf een definitief ontwerp gemaakt voor een cyber security risicomanagement benadering voor de KMar. De analyse die nu volgt beschrijft vanuit het beleid tot aan uitvoering hoe de KMar haar cyber security risicomanagement zou kunnen inrichten.
Er zal worden verwezen naar eerdere delen van dit rapport om herhaling van theorie te voorkomen.
Tevens wordt de derde en laatste deelvraag beantwoord:

> Deelvraag 3: Hoe kan een risicomanagement benadering worden ontworpen voor de KMar?

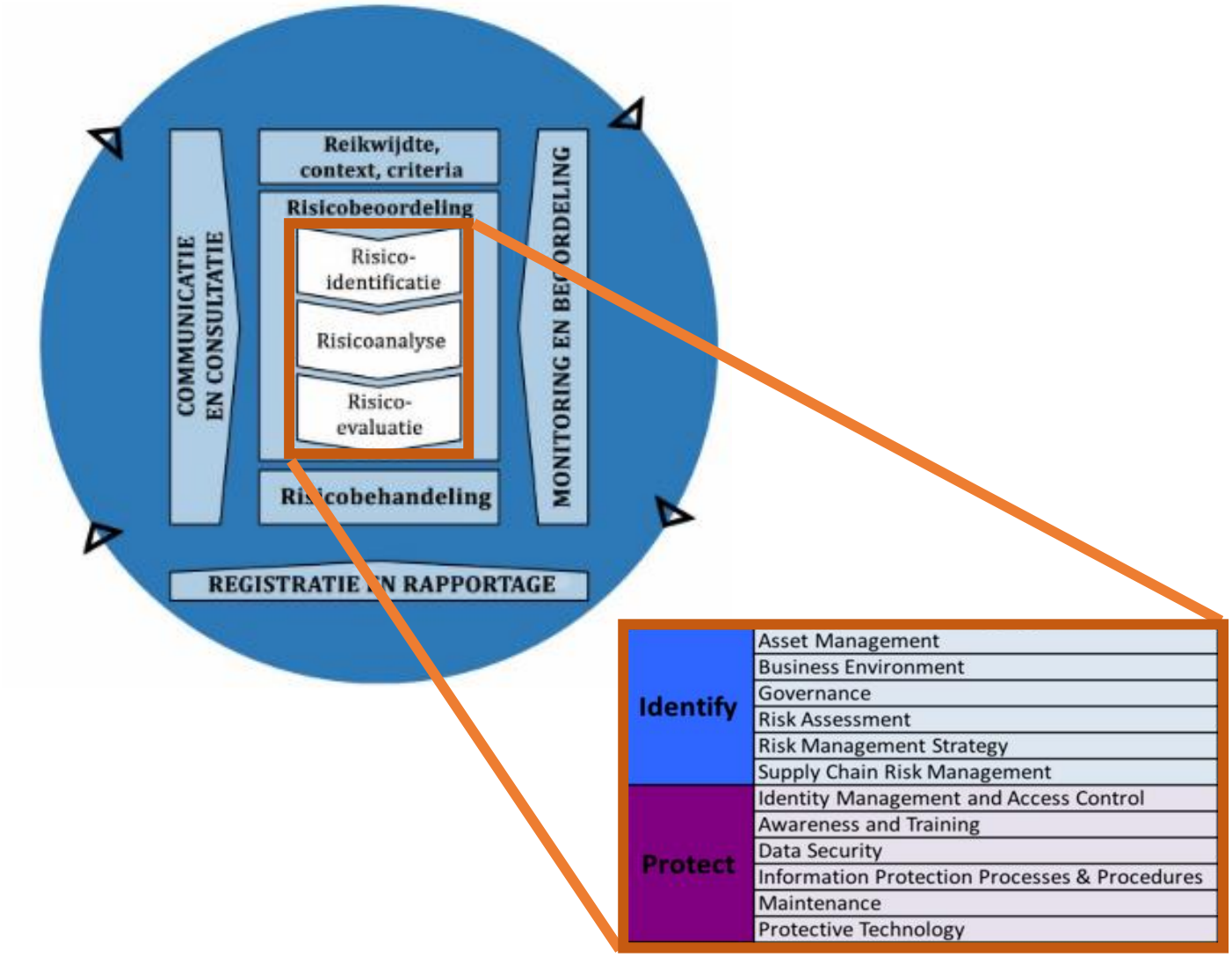
In paragraaf 3.2 is het beleid ten aanzien van risicomanagement binnen MinDef en de KMar uiteengezet en beschreven dat de 'SG-aanwijzing 007: risicomanagement' de ISO 31000 standaard als basis gebruikt. Het beleid volgende en in samenhang met de onderzoeksresultaten beschouwd kan worden geconcludeerd dat het definitieve ontwerp gebaseerd dient te zijn op de ISO 31000 standaard. De ISO 27005 standaard gebruikt, als beschreven in paragraaf 2.4.4, een gelijk raamwerk, principes en proces.
MinDef streeft naar de implementatie van risicomanagement binnen alle domeinen van de organisatie, er is daarom gekozen voor het gebruik van de ISO 31000 standaard om dit streven te benaderen. Vanwege de vele overeenkomsten tussen beide standaarden is besloten de ISO 31000 standaard te gebruiken voor het ontwerp, de ISO 27005 blijft onverminderd van toepassing binnen dit onderzoek.
In 2023 wordt er een programma gestart waarin de focus ligt op de implementatie van risicomanagement vanaf het jaar 2025 en verder (Ministerie van Defensie, 2023).
Onder de naam Integraal Risicomanagement (IRM) wordt gestreefd naar *"IRM als integraal onderdeel van alle activiteiten en de besluitvorming bij Defensie, worden risico's uit verschillende domeinen in samenhang behandeld, hetgeen leidt tot effectievere risicobeheersing* (Ministerie van Defensie, 2023).
De ontwerpvoorwaarde luidt; het definitieve ontwerp dient in lijn te zijn met ISO 31000.

De ISO 27005 beschrijft, zoals in paragraaf 2.4.4 uiteengezet in meer detail dan de ISO 31000 hoe risicomanagement kan worden toegepast ten aanzien van cybersecurity. Net als in de ISO 31000 standaard bestaat de deze uit drie elementen; principes, een raamwerk en een proces (zie paragraaf 2.3). Hoewel de ISO standaarden lijdend zijn in de risicomanagement gemeenschap is een beperking van beiden dat er geen specifieke methode of proces wordt voorgeschreven waarmee cybersecurity risico's kunnen worden geïdentificeerd. Uit de resultaten van de interviews blijkt meermaals dat de KMar de behoefte heeft aan een gestructureerde aanpak die inzicht biedt in de verschillende risico's.

Het NIST Cyber Security Framework (NIST CSF) is beschreven in paragraaf 2.4.6 en scoort de op één na hoogste score in de multicriteria analyse. Het NIST CSF bevat concrete beschrijvingen van werkprocessen en is daarom eenvoudig te implementeren (Roy, 2020).

In de aanleiding en probleemstelling van dit onderzoek is beschreven dat de KMar beperkt inzicht heeft in haar cybersecurity risico's, daarna is uit documentanalyse gebleken dat de kennis over risicomanagement binnen de organisatie laag is en bevestigen de interviews dit beeld. De drie hoogst scorende risicomanagement benaderingen in beschouwing nemende ligt een combinatie van ISO 31000 en NIST CSF het meest voor de hand. Zoals beschreven worden de ISO 27005 en ISO 31000 vanwege de vele overeenkomsten als gelijkwaardig beschouwd en prevaleert de ISO 31000 om een integrale aanpak voor risicomanagement binnen MinDef te waarborgen.

Dit leidt tot de volgende keuze voor een definitieve ontwerpbenadering: Het is aan te bevelen de principes en het raamwerk van de ISO 31000 standaard te gebruiken en het proces van risicobeoordeling uit te voeren middels de eerste twee stappen van het NIST CSF. Dit is in figuur 12 eerst visueel weergegeven en daarna toegelicht. Het belangrijkste voordeel is dat de stappen *Identify* en *Protect* van het NIST CSF concreet beschreven zijn in het NIST handboek, lijden tot meetbare resultaten en de organisatie aanzetten tot het nemen van actie in de stap *protect*. Ten opzichte van de risicobeoordeling zoals deze is beschreven in de ISO 31000 standaard biedt de voorgestelde wijze de KMar meer structuur, meetbare resultaten en lijdt het tot een beter inzicht in cyber security risico's.



Figuur 12: Ontwerpbenadering cyber security risicomanagement KMar.

5. Conclusie en aanbevelingen

In dit laatste hoofdstuk zal antwoord worden gegeven op de hoofdvraag van dit onderzoek en worden er enkele aanbevelingen gedaan voor de organisatie. Tevens is de wetenschappelijke en praktische relevantie uiteengezet en zijn de betrouwbaarheid en validiteit beschreven.

5.1 Conclusie en beantwoording hoofdvraag

Om de hoofdvraag te kunnen beantwoorden is in hoofdstuk 2 literatuuronderzoek uitgevoerd waarmee een wetenschappelijke basis is gelegd onder begrippen als risico, cyber security en risicomanagement. Tevens is een eerste set aan ontwerpcriteria vastgesteld en is deelvraag 1 beantwoord. Vervolgens is in hoofdstuk 3 empirisch onderzocht op welke wijze de Koninklijke Marechaussee risicomanagement uitvoert ten aanzien van cyber security risico's. Aan de hand van zowel documentanalyse als interviews zijn twee aanvullende sets aan ontwerpcriteria vastgesteld en de tweede en derde deelvraag beantwoord.
In hoofdstuk 4 is een cyber security risicomanagement benadering ontworpen aan de hand van de drie sets aan ontwerpcriteria en is het ontwerp en de wijze waarop dit tot stand gekomen is beschreven en verantwoord.

Dit leidt tot de beantwoording van de hoofdvraag van dit onderzoek:
Hoe kunnen cybersecurity risico's van de Koninklijke Marechaussee doeltreffend worden beheerst?

De taken van de Koninklijke Marechaussee zijn breed en veelomvattend, de organisatie voert haar taken uit in een complexe omgeving en in een tijd waarin de veiligheid van onze samenleving belangrijker is dan ooit. Ontwikkelingen als *Artificial Intelligence,* steeds snellere digitalisering en daaraan verwante afhankelijkheid van IT maken de KMar kwetsbaar voor cyber verstoringen. De afhankelijkheid ten aanzien van IT is anno 2023 groot, onontkoombaar en vraagt om doeltreffend risicomanagement. Ondanks dat dit door de KMar wordt onderkent en er diverse initiatieven zijn ontplooid ontbreekt het de KMar aan een risicomanagement benadering om cybersecurity risico's te identificeren en beheersen.
De in dit onderzoek ontworpen benadering stelt de KMar in staat de noodzakelijke stappen te zetten in de richting van integraal risicomanagement in het cyberdomein. Binnen het onderzoek is voortdurend aandacht besteed aan de behoeften van de organisatie en is getracht het ontwerp zoveel als mogelijk aan te laten sluiten op bestaand beleid en werkprocessen.

Het definitieve ontwerp is een synthese van de ISO 31000 en ISO 27005 standaarden waaraan het NIST Cyber Security Framework (NIST CSF) is toegevoegd. Deze verrijking dient de KMar in staat te stellen diepgang in het gewenste overzicht in het IT landschap en de daarbij behorende risico's ten aanzien van

het primaire proces te identificeren. Het NIST CSF is een breed toegepaste cyber security risicomanagement benadering en geschikt voor organisaties als de KMar waarin de risicovolwassenheid laag is.

De validatie van het ontwerp valt buiten de scope van dit onderzoek, hoewel dit in eerste instantie wel onderdeel was van de doelstelling is er tijdens de uitvoering van het onderzoek voor gekozen om geen empirische validatie uit te voeren. Hoofdzakelijk gedreven door het feit dat de kennis over risicomanagement laag is en gestructureerd en integraal risicomanagement binnen de KMar nog niet is geïmplementeerd. De organisatie staat ten tijden van schrijven van dit rapport voor de opgave een strategische keuze te maken over de visie op risicomanagement. Het is daardoor te vroeg om een validatieonderzoek uit te voeren. Dit onderzoek dient de KMar te helpen bij het maken van de keuze en geeft mogelijk in een later stadium een aanzet tot validatie, bijvoorbeeld door middel van een pilot.
Tot slot de implementatie, hoewel dit geen doelstelling in dit onderzoek is volgen er wel enkele aanbevelingen voor de implementatie.

5.2 Aanbevelingen en vervolgonderzoek

In deze paragraaf volgen enkele aanbevelingen voor de Koninklijke Marechaussee, steeds is beschreven op welk niveau binnen de organisatie het mandaat ligt om een aanbeveling over te nemen. Deze paragraaf sluit af met enkele suggesties voor vervolgonderzoek.

Maak op **strategisch niveau de keuze voor risicomanagement** binnen alle domeinen van de KMar waaronder het cyberdomein en bepaal het beleid. Hierbij is het van belang te zorgen voor het uitdragen van een visie op risicomanagement en het creëren van de benodigde randvoorwaarden, voornamelijk in personele capaciteit. Het aanstellen van één of meerdere accenthouders risicomanagement ofwel risicomanagers is op basis van de bevindingen uit dit onderzoek een aan te bevelen startvoorwaarde.

Maak gebruik van de **principes uit de ISO 31000 standaard**, stel een risicomanagement benadering vast en werk een werkproces uit. Draag zorg voor **adaptiviteit en flexibiliteit** bij het ontwerp om aansluiting op de werkprocessen te vergemakkelijken. Deze aanbeveling kan worden uitgevoerd op strategisch niveau door nog aan te wijzen risicomanagers.

Om risicomanagement te kunnen implementeren en uit te kunnen voeren en de **kennis over risicomanagement te verhogen** is het van belang de benodigde kennis en vaardigheden te creëren. Het is daarom van belang zorg te dragen voor het opleiden en trainen van medewerkers in risicomanagement zowel

op strategisch, tactisch als operationeel niveau. Op strategisch niveau dient een opleidingsbehoefte te worden vastgesteld en verkend te worden welke opleidingsinstantie deze behoefte kan vervullen.

Zorg voor inrichten van **governance, risk & compliance** (GRC) waarmee rolduidelijkheid in taken en verantwoordelijkheden en verbetering van de gehele IT governance kan worden bereikt. In dit rapport worden diverse voorbeelden beschreven waaruit blijkt dat de afhankelijkheid van de KMar in JIVC als leverancier groot is maar de samenwerking beperkt. Het valt op dat respondenten binnen zowel de KMar als JIVC de huidige beperkte manier van samenwerking opmerken. Het is daarnaast voor de KMar van belang haar **rol** ten aanzien van **cyber security** en daarmee gepaard gaande **verantwoordelijkheden** te erkennen en hier een **visie op te ontwikkelen**. Met de vorming van het CIO-office en het aanstellen van een Chief Information Security Officer (CISO) worden hier de eerste goede stappen in gezet.

Bepaal in nauwe samenwerking met de operatie van de KMar welke **systemen kritiek** zijn voor de uitvoering van het operationele proces, breng prioritering aan en pas risicomanagement als eerst toe op deze systemen. Het is belangrijk om vanuit het primaire proces te redeneren en risico's te beoordelen aan de hand van de doelstellingen van de organisatie. Stel de **risicobereidheid of *risk-appetite*** vast. Deze aanbeveling dient op tactisch en operationeel niveau te worden overgenomen op het niveau van (plaatsvervangend) brigadecommandanten.

Beschouw ten aanzien van cyber security risico de gehele keten (zie figuur 3) en beperk de focus niet louter op continuïteit bij niet beschikbaarheid van IT-toepassingen. Zorg voor actuele informatie over cyberdreiging en zorg dat dit bij belanghebbenden onder de aandacht wordt gebracht. Het strategisch niveau van de KMar en JIVC dienen beleid te ontwikkelen met inachtneming van deze aanbeveling.

Oefen en train met de gehele bij cybersecurity betrokken keten, hierbij dienen zowel JIVC als verantwoordelijken op strategisch, tactisch en operationeel niveau te worden betrokken. een **Table top of *'serious gaming'*** zou hierbij een gewenste vorm kunnen zijn.

Besteed aandacht aan communicatie over risico's, risicomanagement en relevante casuïstiek, nodig alle lagen van de organisatie uit met risico's en relevante praktijkvoorbeelden te komen. De Koninklijke Luchtmacht maakt gebruik van het Safety Rapportage Systeem (SRS), hoewel dit sterk geënt is op vliegveiligheid is een dergelijk systeem goed toepasbaar voor de Koninklijke Marechaussee ten aanzien van (cyber-) risico's.

5.3 Aanbevelingen voor vervolgonderzoek

Dit onderzoek is gericht op het ontwerpen van een cyber security risicomanagement benadering, met gebruikmaking van de *problem solving cycle* (Aken & Berends, 2018) zijn de eerste drie stappen doorlopen, de eerst volgende stap betreft de interventie. Het is aan te bevelen onderzoek te doen naar de implementatie van risicomanagement binnen de organisatie. Hoewel er in dit onderzoek enkele succesfactoren voor implementatie worden beschreven is het van belang nader te onderzoeken hoe de KMar kan streven naar de toepassing van integraal risicomanagement. Dit onderzoek dient zich te richten op zowel harde factoren als beleid, *tooling* en evaluatie, als op zachte factoren als de mens en organisatiecultuur. Een voor te stellen eerste stap is het uitvoeren van een pilot waarin het ontwerp uit dit onderzoek kan worden gevalideerd.

Tevens is het aan te bevelen onderzoek te doen naar de gewenste risicobereidheid of *risk-appetite* binnen de organisatie en daarbij behorende mandaten voor (rest)risico acceptatie. Uit zowel de documentanalyse als de interviews is gebleken dat de risicobereidheid onvoldoende in kaart is gebracht. Dit leidt frequent tot discussie of escalatie van risico's naar een naast-hoger niveau.

5.4 Wetenschappelijke en praktische relevantie

Dit onderzoek beoogt een bijdrage te leveren aan zowel de wetenschap als de praktijk binnen Koninklijke Marechaussee. Daarbij zijn het ontwerp en de aanbevelingen voor andere (semi-) overheidsorganisaties relevant en toepasbaar. De bijdrage aan de wetenschap wordt gevormd door wetenschappelijke criteria voor risicomanagement benaderingen uit diverse literatuurbronnen in samenhang te beschouwen met empirisch verkregen onderzoeksresultaten. Het definitieve ontwerp is een integratie van twee gangbare risicomanagement benaderingen. Hoewel er meerdere onderzoeken zijn verricht naar het combineren van risicomanagement benaderingen, zie bijvoorbeeld (Ferreira, 2020; Kosutic, 2022), is een combinatie van het NIST raamwerk met een ISO standaard zoals in dit onderzoek ontworpen slechts zeer beperkt onderzocht.

Voor de Koninklijke Marechaussee en andere (semi-) overheidsorganisaties biedt het ontwerp de mogelijkheid te streven naar een integrale aanpak voor risicomanagement binnen alle domeinen van de organisatie. Het gebruik van de ISO 31000 standaard creëert voldoende ruimte voor het inrichten van risicomanagement zodat dit aansluit op bestaande werkprocessen en de doelstellingen van de organisatie. De toevoeging van het NIST raamwerk zorgt voor een gestructureerde en eenvoudig toe te passen methode om inzicht in- en effectieve beheersing van- cyberrisico's mogelijk te maken.

5.5 Betrouwbaarheid en Validiteit

De kwaliteit van een onderzoek kent twee belangrijke criteria, betrouwbaarheid en validiteit. Beide begrippen worden hierna toegelicht.

Onderzoeksgegevens zijn betrouwbaar te noemen wanneer ze minder van incidentele toevalligheden afhangen (Baarda, 2013). In dit onderzoek met een inductief karakter levert dit een aantal aandachtspunten op. Omdat in het onderzoek een open manier van interviewen is gebruikt en binnen het cyberdomein begrippen niet altijd eenduidig zijn, is het nemen van maatregelen vooraf en tijdens de interviews van belang. Om de betrouwbaarheid van dit onderzoek te garanderen en tot generaliseerbare resultaten te komen zijn de volgende betrouwbaarheid verhogende maatregelen genomen:

- Er is gekozen voor respondenten uit verschillende domeinen van de organisatie;
- Interviews worden afgenomen in een besloten ruimte;
- Er is gekozen voor het opnemen van interviews waarbij is benoemd dat de opname alleen dient voor de schriftelijke uitwerking van het interview;
- Voorafgaand aan het interview is benoemd dat de naam en functiegegevens van de respondent niet in het openbare verslag worden opgenomen en de gegevens vertrouwelijk en geanonimiseerd worden verwerkt;
- Het interviewprotocol inclusief gebruikt begrippenkader is voorafgaand aan het gesprek gedeeld met de respondent;
- Na afloop van het interview is een verslag uitgewerkt dat ter validatie is verzonden naar de respondent;

Op basis van bovenstaande kan worden aangetoond dat dit onderzoek betrouwbaar is.

Het tweede criterium is de validiteit ofwel de geldigheid van het onderzoek. Dit criterium geeft, in navolging op de betrouwbaarheid, weer of de verzamelde data een geldige weergave is van de werkelijke situatie. Deze keuze brengt risico's met zich mee ten aanzien van de interne validiteit. Om de validiteit te kunnen waarborgen maar ook voldoende ruimte te houden voor de toepassing van de gefundeerde theoriebenadering is het interview protocol ontworpen na het eerste literatuuronderzoek (Hoofdstuk 2). Er is getracht aan de hand van wetenschappelijke artikelen in combinatie met interne bedrijfsdocumentatie te komen tot eenduidige begripsbepalingen. Dit om te voorkomen dat er tijdens de interviews sprake is van (spraak)verwarring. De interview verslagen zijn door de respondenten gevalideerd. Tot slot is de hoeveelheid interviews niet vooraf bepaald en is doorgegaan tot er theoretische saturatie optrad (Baarda, 2013).

6. Bijlagen

6.1 Bibliografie

Aken, J. van, & Berends, H. (2018). *Problem Solving in Organisations*.; Cambridge University Press.

Aven, T. (2012). The risk concept-historical and recent development trends. *Reliability Engineering and System Safety*, *99*(0951), 33–44. https://doi.org/10.1016/j.ress.2011.11.006

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, *12*(1), 1–11. https://doi.org/10.1080/13669870802488883

Baarda, B. (2013). *Basisboek Kwalitatief Onderzoek*.; Noordhoff Uitgevers Groningen/Houten.

Boeije, H., & Bleijenbergh, I. (2019). *Analyseren in kwalitatief onderzoek: Denken en doen*.; Boom Uitgeverij.

Böhme, R., Laube, S., & Riek, M. (2019). A Fundamental Approach to Cyber Risk Analysis. *Variance. Advancing the Science of Risk*, *12*(2), 161–185.

Bundesambt fur Sicherheit in der Informationstechnik. (2017). *BSI-Standard 200-2 IT-Grundschutz MethodologyVersion 1.0,*.

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). A Taxonomy of Operational Cyber Security Risks Version 2. *Carnegie-Mellon Univ Software Engineering Inst*, *May*, 1–47. http://www.sei.cmu.edu

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *COSO - ERM framework*. https://www.house-of-control.nl/coso-erm.html

CRO Forum. (2014). *Cyber resilience The cyber risk challenge and the role of insurance*. https://www.scor.com/sites/default/files/cro_forum_cyberrisk_paper_0.pdf

Eling, M., Schnell, W., & Sommerrock, F. (2016). Ten key questions on cyber risk and cyber risk insurance. *The Geneva Association*, *November*, 92–93.

ENISA. (2022). *Risk Management Standards* (Issue March). https://doi.org/10.2824/001991

ENISA. (2021). METHODOLOGY FOR SECTORAL CYBERSECURITY ASSESSMENTS. EU Cybersecurity Certification Framework. In *Enisa* (Issue September). https://doi.org/10.2824/490490

Everett, C. (2011). FEATURE A risky business : ISO 31000 and 27005 unwrapped. *Computer Fraud & Security Bulletin*, *2011*(2), 5–7. https://doi.org/10.1016/S1361-3723(11)70015-X

Fenrich, K. (2008). Securing your control system. *Power Engineering (Barrington, Illinois)*, 44–51.

Ferreira, G. (2020). *Comparing ISO 31000 and ISO 27005*. The Risk Academy. https://theriskacademy.org/is0-31000-iso-27005/

Geraets, R. (2018). Veiligheid; Security Risk Management. Interne uitgave bibliotheek Koninklijke Marechaussee.

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. In *European Commission JRC (Joint Research Center) Technical notes.* https://doi.org/10.2788/22260

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory; strategies for qualitative research; Journal of Nursing Studies.*

Graham, J.D.; Wiener, J. B. (1995). Risk vs. risk tradeoffs in protecting public health and the environment. *Cambridge*, *Harvard University Press*.

Grandry, E., Feltus, C., & Dubois, E. (2013). Conceptual Integration of enterprise architecture management and security risk management. *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC*, 114–123. https://doi.org/10.1109/EDOCW.2013.19

Hansen, S. F., & Tickner, J. A. (2008). Putting risk-risk tradeoffs in perspective: A response to Graham and Wiener. *Journal of Risk Research*, *11*(4), 475–483. https://doi.org/10.1080/13669870802124413

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Research 1. *Design Science in IS Research MIS Quarterly*, *28*(1), 75.

Hopkin, P. (2018). *Fundamentals of Risk Management* (5th ed.); Kogan Page, New York.

INK, *INK management model*. (26 april 2023), https://www.ink.nl/modellen/ink-managementmodel/

International Organisation for Standardization. (2022). *Nen-iso/iec 27005*. (2 november 2022), https://www.nen.nl

International Organisation for Standardization. (2018). *Nen-iso 31000+c11*. *(2 november 2022)*, https://www.nen.nl

Koninklijke Marechaussee. (2021). *Fiche kabinetsformatie Rutte IV*.

Koninklijke Marechaussee. (2017). *Ontwikkelagenda 2017-2022*.

Koninklijke Marechaussee. (2020). *Cyber Doctrine*.

Kosutic, D. (2022). *ISO 31000 and ISO 27001 How are they related?* https://advisera.com/27001academy/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/

Kosutic, D. (2023). *ISO 27001 implementation checklist*. https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/

Kunstt, D. (2020) *Van "Make it happen" naar ORM : een onderzoek naar risicomanagement binnen de brigade Brabant Zuid van de Koninklijke Marechaussee.*

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. In *Neural Computing and Applications* (Vol. 34, Issue 18). Springer London. https://doi.org/10.1007/s00521-022-06959-2

Lambrinoudakis, C., Gritzalis, S., Xenakis, C., Katsikas, S., Karyda, M., Tsochou, A., Papadatos, K., Rantos, K., Pavlosoglou, Y., Gasparinatos, S., Pantazis, A., Zacharis, A., & European Union Agency for Cybersecurity. (2022). *Compendium of risk management frameworks with potential interoperability : supplement to the interoperable EU risk management framework report.* (Issue January). https://doi.org/10.2824/75906

Lempinen, H., Rossi, M., & Tuunainen, V. K. (2012). Design principles for inter-organizational systems development - Case Hansel. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 7286 LNCS*. https://doi.org/10.1007/978-3-642-29863-9_5

Lloyds. (2015). *A quick guide to cyber risk*. https://www.lloyds.com/news-and-insights/news/a-quick-guide-to-cyber-risk

Mahmoud, A., Schmidt, F., & Siebert, G. (2020). *ISO/IEC 27001 and IT baseline protection (IT-Grundschutz)*. https://www.bsi.bund.de/

Mendoza, G. (1999). Guidelines for applying multi-criteria analysis to the assessment of criteria and indicators. In *Guidelines for applying multi-criteria analysis to the assessment of criteria and indicators*. https://doi.org/10.17528/cifor/000769

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2018). *Baseline informatiebeveiliging Rijksoverheid*. 1–80.

Ministerie van Defensie. (2021). *Risicomanagement A006*. 1–36.

Ministerie van Defensie. (2021). *Instructie Defensie Beveiligingsbeleid D302*. 1–20.

Ministerie Van Defensie. (2019). *Veiligheidsmanagementsysteem Defensie*. 1–2.

Ministerie van Defensie. (2023). *Implementatieplan risicomanagement*.

Ministerie van Defensie. (2021). *Instructie Defensie Beveiligingsbeleid Deelgebied Beveiliging Algemeen & Organisatie A/003: Algemeen Daderprofiel Defensie*.

Ministerie van Defensie. (2018). *Instructie Defensie Beveiligingsbepalingen Deelgebied Beveiliging Algemeen & Organisatie A / 004 : Beveiligingsincidenten.*

Ministerie van Defensie. (2020). *Instructie Defensie Beveiligingsbeleid Deelgebied Informatiebeveiliging D102 Cybersecurity-onderzoek van informatiesystemen.*.

Ministerie van Defensie. (2006). *Algemene Beveiligingseisen voor Defensieopdrachten 2006*. https://www.defensie.nl/binaries/defensie/documenten/beleidsnota-s/2006/08/13/abdo-2006/abdo-2006.pdf

Ministerie van Defensie. (2021). *Instructie Defensie Beveiligingsbeleid Deelgebied Beveiliging Algemeen & Organisatie A / 005 : Te Beschermen Belangen*. 1–38.

Ministerie van Defensie. (2021). *Instructie Defensie Beveiligingsbeleid Deelgebied Informatiebeveiliging Beveiligen van informatiesystemen D300*. 1–11.

Ministerie van Defensie. (2018). *Instructie Defensie Beveiligingsbeleid Deelgebied Informatiebeveiliging D101 Betrouwbaarheid van informatiesystemen*. 1–16.

Ministerie van Defensie. (2012). *Introductiebundel Besturen Bij Defensie uitgave 2012.*

Molen, I. Van Der. (2015). *Bewust naar risico-gestuurd in een politiek-bestuurlijke omgeving*. Onderzoek naar risicomanagement bij het Directoraat-Generaal Politie, Ministerie van Veiligheid en Justitie.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). *Cyber-risk decision models : To insure IT or not ?.*

Murdock, H. (2018). Three Lines of Defense. *Auditor Essentials*, 427–430. https://doi.org/10.1201/9781315178141-95

NCTV. (2021). Cybersecuritybeeld Nederland 2021. *Csbn*, 1–76. https://www.thehaguesecuritydelta.com/media/com_hsd/report/237/document/CSBN2019-online-tcm31-392768.pdf

NCTV. (2022). *Cybersecuritybeeld Nederland 2022*., https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

NIST. (2011). *Managing Information Security Risk*. Organization, Mission, and Information System View. NIST publication 800-39. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NLR. (2021). *Adviesrapport over inrichting Integraal Risicomanagement bij Defensie*.

Oliveira, K., Méxas, M., Meiriño, M., & Drumond, G. (2019). Critical success factors associated with the implementation of enterprise risk management. *Journal of Risk Research*, *22*(8), 1004–1019. https://doi.org/10.1080/13669877.2018.1437061

Paper, W., Böhme, R., & Schwartz, G. (2010). *Modeling Cyber-Insurance: Towards A Unifying Framework*. *June*, 1–36.

Paredes, G. (2018). Institutional Repository - Research Portal Dépôt Institutionnel - Portail de la Recherche Modeling enterprise risk management and security with the ArchiMate language Modeling Enterprise Risk Management and Security with the ArchiMate ® Language A White P. *The Open Group*, 12–15.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

PWC. (2014). *Hoeveel zijn we opgeschoten na de crisis ? Tweede Nationaal Onderzoek Risicomanagement in Nederland*.

Ramesh, S. (2022). *Data Governance for Sustainability , Security , and Business Intelligence in the Transport , Logistics , and Supply Chain Industry Data Governance for Sustainability , Security and Business Intelligence in the Transport , Logistics and Supply Chain Industry*.

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management*. http://www.springer.com/series/10028

Rogers, E. M. (2003). *Diffusion of Innovations* (5th edn.). Free Press, New York.

Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020*, *53*, 27001–27003. https://doi.org/10.1109/NCETSTEA48365.2020.9119914

Starodubtsev, Y. I., Balenko, E. G., Vershennik, E. V., & Fedorov, V. H. (2020). Cyberspace: Terminology, Properties, Problems of Operation. *2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon* 2020–2022. https://doi.org/10.1109/FarEastCon50210.2020.9271282

Staveren, M.Th. Van. (2009). *RISK , INNOVATION & CHANGE Design Propositions for Implementing Risk Management in Organizations*. Proefschrift: Universiteit Twente.

Staveren, M.Th. Van. (2015). *Risicogestuurd werken in de praktijk*. Vakmedianet Uitgeverij, Deventer.

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). Integrating Cybersecurity and Enterprise Risk Management (ERM). *National Institute of Standards and Technology*, 76. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286-draft.pdf%0Ahttps://doi.org/10.6028/NIST.IR.8286-draft2

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *(*October 2020), 105143. https://doi.org/10.1016/j.ssci.2020.105143

Swiss. (2014). *Working together with clients to find cyber risk solutions*. https://www.swissre.com/reinsurance/property-and-casualty/solutions/cyber-solutions/cyber-product-suite-sme.html

Tušer, I., & Hošková-Mayerová, Š. (2022). *Trends and Future Directions in Security and Emergency Management*.

van den Heuvel, R. J. H. ., & Wondergem, B. C. . (2005). *Integratie van risicomanagement leidt tot betere prestaties*.

Verschuren, P., & Doorewaard, H. (2021). *Het ontwerpen van een onderzoek* (6th ed.) Boom Uitgevers Amsterdam.

Visitatiecommissie Defensie en Veiligheid (2021). *Eindrapport 2021*. https://www.defensie.nl/binaries/defensie/documenten/rapporten/2021/06/21/jaarrapport-2021-visitatiecommissie-defensie-en-veiligheid/2021+06+21+Jaarrapport+2021+-+Ruimte+voor+Veiligheid_web.pdf

Visitatiecommissie Defensie en Veiligheid (2020). Jaarrapport 2020. https://www.defensie.nl/binaries/defensie/documenten/rapporten/2020/06/15/jaarrapport-visitatiecommissie-2020/20200615+Jaarrapport+2020+Visitatiecommissie+DEF.pdf

vom Brocke, J., Hevner, A., & Maedche, A. (2020). *Introduction to Design Science Research*. *September*, 1–13. https://doi.org/10.1007/978-3-030-46781-4_1

vom Brocke, J., & Maedche, A. (2019). The DSR grid: six core dimensions for effectively planning and communicating design science research projects. *Electronic Markets*, *29*(3), 379–385. https://doi.org/10.1007/s12525-019-00358-7

Wagner, D., & Disparte, D. (2016). Cyber Risk. *Global Risk Agility and Decision Making*, 199–220. https://doi.org/10.1057/978-1-349-94860-4_9

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology*, *54*(12), 1317–1339. https://doi.org/10.1016/j.infsof.2012.07.007

Wijnen, G., & Storm, P. (2007). *Projectmatig werken*. Unieboek uitgeverij Het Spectrum, Amsterdam.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis*, *27*(3), 597–606. https://doi.org/10.1111/j.1539-6924.2007.00909.x

Bijlage 1: Interviewprotocol

Het interviewprotocol is niet opgenomen in de publieke versie van dit rapport.

Bijlage 2: Overzicht figuren en tabellen

Figuur	
1	Onderzoeksmodel
2	Problem Solving Cycle
3	Model Cyber Risico
4	BIE driehoek / CIA triad
5	Elementen risicomanagement ISO standaard
6	Proces risicomanagement ISO standaard
7	Risico proces stappen
8	INK Model
9	COSO-ERM Framework
10	Risicogebieden Koninklijke Marechaussee *niet opgenomen in de publieke versie
11	Ontwerpcriteria, 3 sets
12	Ontwerpbenadering cybersecurity risicomanagement KMar

Tabel	
1	Onderzoeksstrategie
2	Kernbegrippen en synoniemen
3	Beschrijving driehoek
4	Top 3 risicomanagement benaderingen
5	Top 3 cybersecurity risicomanagement benaderingen
6	Risicomanagement benaderingen Defensie
7	Risicomanagement benaderingen Defensie met toelichting en toepassing
8	Ontwerpcriteria uit Van Staveren (2009)
9	Ontwerpcriteria uit Oliveira et al (2019)
10	Ontwerpcriteria uit interne documentatie
11	Ontwerpcriteria cyber security risicomanagement
12	Ontwerpcriteria voor implementatie
13	Definitieve selectie ontwerpcriteria
14	Scores risicomanagement benaderingen