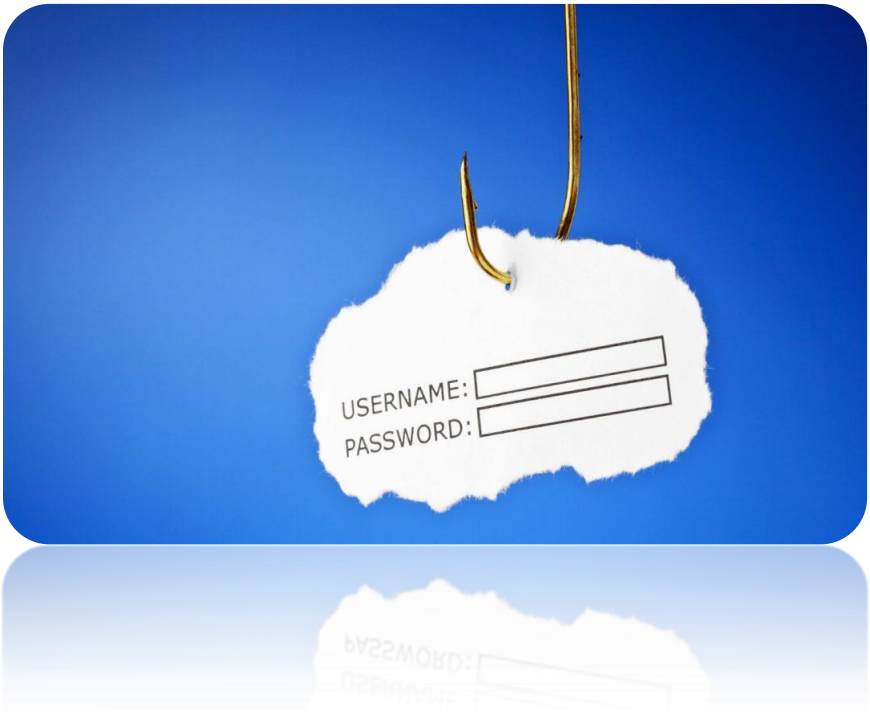
Ministerie van Justitie en Veiligheid

Plan van Aanpak 'hoofdlijnen verbetering centrale sturing en beheersing informatiebeveiliging van het ministerie van Justitie en Veiligheid'

Versie 1.64

Datum	24 okt 2018
Status	Definitief



Colofon

Afzendgegevens **Directie Informatievoorzienig en Inkoop**
I-control en Security

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon S. Cammeraat

Projectnaam Verbetering centrale sturing en beheersing IB MinJenV

Auteurs Henk Jan van der Molen en Richard van der Kroft

Versie historie

Versie	Belangrijkste wijzingen	Datum
0.1	Initiële versie	7 juli 2018
0.2	Bijwerkingen op basis van commentaar en voortschrijdend inzicht	14 juli 2018
1.0	Aangeleverd commentaar verwerkt	5 aug 2018
1.1	Aanvullend commentaar in deze definitieve versie	22 aug 2018
1.2	Commentaar pSG verwerkt	12 sept 2018
1.3	Laatste commentaren verwerkt	26 sept 2018
1.4	Review dDI&I	28 sept 2018
1.5	Commentaar pSG verwerkt	3 okt 2018
1.6	Commentaar CIO’s en CISO’s verwerkt	23 okt 2018

Samenvatting

Bij het ministerie van JenV zijn de primaire processen sterk afhankelijk van ICT en zijn veel van de verwerkte gegevens gevoelig van aard. Bovendien is het belang van een adequate informatiebeveiliging (IB) voor JenV als hoeder van de rechtsstaat groot, omdat de digitale dreiging wereldwijd steeds toeneemt. Het is essentieel dat de IB van JenV op orde is en blijft, daarom zal JenV de komende jaren blijven investeren in de beveiliging van haar processen.

Dit plan richt zich op de verbetering van de centrale sturing en beheersing van de IB van de JenV organisatie. De scope richt zich daarbij niet direct op de taakorganisaties en *sui generis* organisaties van het ministerie, al worden de activiteiten zoveel mogelijk gezamenlijk opgepakt.

Het plan van aanpak IB werkt voor de periode 2018-2022 de volgende drie speerpunten uit:

- Het verbeteren van de governance,
- Het versterken van het risicomanagement, en
- Het verbeteren van incidentmanagement.

Deze speerpunten zijn vertaald in technische-, organisatorische- en personele maatregelen, gebaseerd op het volwassenheidsmodel van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA). De ADR gebruikt ditzelfde NBA model bij het jaarlijks meten van de volwassenheid van de IB van alle departementen. Tevens biedt het plan ruimte aan interdepartementale ontwikkelingen.

Het plan beschrijft op hoofdlijnen de huidige situatie, de gewenste verbeteringen en het meerjarige groeipad naar de realisatie van deze resultaten. JenV werkt de gewenste verbeteringen uit in projectplannen. Voldoende capaciteit van deskundig personeel vormt daarbij een kritische succesfactor.

Inhoud

1 Inleiding

1.1 Achtergrond

Het recht raakt ons dagelijks leven. Wetten beschermen onze vrijheid en veiligheid. Zo bieden ze de regels waardoor mensen kunnen samenleven en bedrijven kunnen floreren. Het ministerie van Justitie en Veiligheid (hierna: JenV) staat voor:

- een goed werkende rechtsstaat
- een veiliger Nederland
- een rechtvaardig migratiebeleid

Een goed werkende rechtsstaat geeft mensen zekerheid. De zekerheid in vrijheid te leven en dat de meeste mensen hun verplichtingen nakomen. En de zekerheid van een eerlijke behandeling door de overheid, die staat voor de gelijkheid van iedereen. In een samenleving die verandert en internationaliseert, blijft de rechtsstaat een fundament van de welvaart. Daarom spelen we in op de steeds sneller gaande veranderingen. Door deze veerkracht biedt de rechtsstaat ook in de toekomst rechtvaardige uitkomsten.

De afgelopen jaren is Nederland veiliger geworden. Steeds minder mensen kregen te maken met gewelds- of vermogenscriminaliteit of een inbraak. Tegelijkertijd zien we nieuwe vormen van criminaliteit. Ook de omvang en ernst van de digitale dreiging in Nederland zijn reeds aanzienlijk en blijven zich ontwikkelen, zodat er sprake is van een continue digitale dreiging voor de nationale veiligheid. De Nederlandse maatschappij en economie zijn bijna volledig afhankelijk geworden van digitale middelen. De gevolgen van aanvallen en uitval kunnen groot en zelfs maatschappij ontwrichtend zijn. Dat blijkt onder andere uit het Cybersecuritybeeld Nederland 2018 (CSBN 2018) van de NCTV.

<u>Belang van Informatiebeveiliging voor JenV</u>
Ook het ministerie van Justitie en Veiligheid is een “high target”. Ze is dus niet alleen de hoeder van een goed werkende rechtsstaat, maar kan potentieel ook zelf het slachtoffer worden van de bovenstaande digitale dreiging op een schaal die voorheen – in de fysieke wereld – niet aan de orde was. Hierdoor is het van absoluut belang dat de interne informatiebeveiliging van JenV op orde is.

Informatiebeveiliging (IB) is essentieel voor de betrouwbaarheid en continuïteit van JenV. JenV is in de huidige 24-uurs informatiemaatschappij niet (meer) effectief te besturen zonder adequate informatie die juist, volledig en tijdig beschikbaar is voor de gebruiker. Daarnaast stellen we steeds hogere eisen aan de beveiliging van bedrijfs- en persoonsinformatie. Informatie is hiermee een belangrijke productiefactor geworden, waarvan de beschikbaarheid, exclusiviteit en integriteit moet worden gegarandeerd. Bovendien dient JenV het goede voorbeeld te geven.

Het op orde brengen en houden van IB is geen eenvoudige opgave. Het beeld verslechterd jaarlijks, zoals te zien is aan: kwetsbaarheden in software; toename van malware; het tekort aan goed opgeleid IT/IB personeel; het beperkt implementeren van informatiebeveiliging bij nieuwe producten; het (nog) beperkt aanwezig zijn van informatiebeveiliging in de ‘cultuur’ van JenV en eindgebruikers die onvoldoende in staat zijn om de juiste beslissingen te nemen met betrekking tot de digitale dreigingen waarmee ze geconfronteerd worden (risicobewustzijn). Tegelijkertijd neemt de afhankelijkheid van informatie en ICT steeds verder toe, waardoor de impact van verstoringen groter wordt. Dit vraagt om een continue en meerjarige aanpak.

1.2 Aanleiding en scope

In het verantwoordingsdebat van 13 juni 2018 heeft de Kamer gesproken over het rapport Verantwoordingsonderzoek 2017 van de Algemene Rekenkamer(ARK). De ARK heeft geconstateerd dat op het gebied van informatiebeveiliging door het ministerie stappen zijn gezet en dat de centrale sturing en beheersing zijn verstevigd, maar dat er nog verbeteracties mogelijk zijn. Met name op het gebied van risico- en incidentmanagement waren de verbeteringen nog onvoldoende gevorderd om de onvolkomenheid voor informatiebeveiliging (IB) op te heffen. De ARK heeft de onvolkomenheid gebaseerd op het onderzoek van de Auditdienst Rijk (ADR) naar de volwassenheid van de centrale beheersing van de informatiebeveiliging.

Het voorliggende plan richt zich op de verbetering van de *centrale sturing en beheersing* van de informatiebeveiliging van JenV en beschrijft op hoofdlijnen de huidige situatie, de gewenste situatie en de weg daar naar toe. De beschrijving van de uitvoering van de decentrale activiteiten (van de taakorganisaties en sui generis organisaties van het ministerie) is daarmee, in dit plan van aanpak, niet in scope. Dit is de verantwoordelijkheid van de organisaties zelf. Ze dienen uiteraard wel in samenhang te worden bezien.

1.3 Rijksbrede ontwikkelingen

De samenleving is in hoge mate afhankelijk van diensten van de Rijksoverheid. Die diensten zijn en worden in toenemende mate digitaal georganiseerd. Over de ambitie van het kabinet ten aanzien van de digitalisering van onze samenleving en van de overheid heeft het kabinet de Kamer onlangs de Nederlandse Digitaliseringsstrategie[1] en de Agenda Digitale Overheid[2] gestuurd.
Het kabinet is van mening dat wij in het licht van de digitale ontwikkelingen in de samenleving en de overheid onze inzet op alle fronten moeten versterken. Voor digitalisering binnen de Rijksoverheid vertaalt dit zich, in het verlengde van de Agenda Digitale Overheid, naar scherpere en meer eenduidige sturing op het gebied van informatie beveiliging.

Ook het ministerie van BZK[3] constateert dat de Rijksoverheid net als alle andere organisaties en individuen, kwetsbaarder wordt voor de snel toenemende hoeveelheid cyberaanvallen. Met name ten aanzien van de bescherming van gegevens van burgers en bedrijven mag van de Rijksoverheid een adequate beveiliging worden verwacht en is afgestemd op het belang van de bedrijfsprocessen en een actueel risicobeeld. De wettelijke plichten die zij oplegt aan burgers en bedrijven (zoals beschreven in de AVG) onderstreept de voorbeeldfunctie van de overheid. De maatregelen die door BZK worden genoemd - waar JenV ook invulling aan zal geven of al geeft - zijn de volgende:

- *Implementatie centrale voorziening: vulnerability scanning*
- *Opstellen van een lijst van vereiste beveiligingsmaatregelen*
- *Ontwikkelen van gezamenlijk kader voor een voorziening voor staatsgeheime toepassingen*
- *Uitbouw van het Nationaal Detectie Netwerk[4] (NDN) bij de Rijksdienst*

[1] Nederlandse Digitaliseringsstrategie, Nederland Digitaal, bijlage bij Kamerstukken II 2017/18, 26643, 541

[2] NL Digibeter, Agenda Digitale Overheid, bijlage bij Kamerstukken II 2017/18, 26643, 549

[3] Brief aan de kamer: "Sturing informatiebeveiliging en ICT binnen de Rijksdienst"

[4] Het Nationaal Detectie Netwerk is een door het Nationaal Cyber Security Centrum gestart initiatief om, samen met de inlichtingen- en veiligheidsdiensten, aanvallen van buitenaf sneller te detecteren en informatie over deze en andere dreigingen sneller te delen binnen de Rijksoverheid (Threat Intel Platform).

Ook is in de Agenda Digitale Overheid 'NL DIGIbeter' toegezegd de Tweede Kamer in het najaar te voorzien van een nadere uitwerking van maatregelen die worden getroffen om de informatieveiligheid bij de overheid te verhogen. Het ministerie van BZK heeft dit verder uitgewerkt in het kamerstuk "Verhogen informatieveiligheid bij de overheid[5]". Dit zijn bijvoorbeeld punten als het vaststellen van de Baseline Informatiebeveiliging Overheid (BIO), het organiseren van overheidsbrede crisissimulatie-oefening en het verplichten open informatieveiligheidsstandaard HTTPS (veilige overheidswebsites). Deze en de overige punten staan benoemd in hoofdstuk 3.2.

JenV zal de komende jaren invulling geven aan de rijksbrede ambities binnen de rijksbrede kaders en heeft deze in dit plan van aanpak in haar meerjarige activiteitenreeks waar nodig opgenomen. Deze worden in paragraaf 3.1 (JenV ambitie) en paragraaf 4.2 (uitvoering) nader toegelicht.

[5] Kamerstuk "Verhogen informatieveiligheid bij de overheid" met als kenmerk 2018-0000791223

2 Vertrekpunt; waar staan we nu

2.1 ADR en ARK bevindingen

In 2017 heeft de ADR de IB volwassenheid van JenV van de *centrale beheersing en sturing* gemeten op basis van het NBA[6] model, dat de ARK vervolgens ook heeft gebruikt voor haar bevindingen. Het model gaat uit van verschillende domeinen van centrale beheersing en sturing van IB waaronder het bv. hebben van een IB strategie, IB kaders, een toereikende organisatie en aanwezigheid van service level management in relatie tot leveranciers.

Het volwassenheidsmodel bevat naast de 5 onderzochte aandachtsgebieden ten aanzien van centrale sturing en beheersing van de informatiebeveiliging nog 10 andere aandachtsgebieden. De 10 andere aandachtsgebieden zijn meer vakinhoudelijk van aard en binnen JenV grotendeels decentraal georganiseerd of bij de Shared Service / IT Organisaties (SSO's) belegd. Sturing op dergelijke aandachtsgebieden geschiedt onder andere via het aandachtsgebied 'supply chain management'. Via Service level management worden centraal eisen gesteld aan de dienstverlening van derden en dientengevolge worden de overig aandachtsgebieden daarmee van een afspraken en kaders voorzien. Het aandachtsgebied 'HRM' wordt echter wél tevens tot de invloedssfeer van centrale beheersing en sturing gerekend.

Voor de 10 overige aandachtgebieden heeft de ADR (nog) geen volwassenheidsniveau bepaald. Binnen deze aandachtgebieden worden uiteraard wel plannen en projecten gerealiseerd. Hieronder wordt het volledige overzicht van aandachtsgebieden gepresenteerd:

	Gebied	**Betreft o.a.**
1	Governance	Strategie, beleid, architectuur
2	Organisatie	Rollen, verantwoordelijkheden
3	Risico management	Framework, assessment, planning
4	HR	Training, risicobewustzijn
5	Configuratie management	Beheer apparatuur
6	Incident management	Incident, escalatie en respons
7	Change management	Security testen, impact analyse
8	Systeem ontwikkeling	Secure software development
9	Data Management	Classificatie, opslag, dataverkeer
10	Identity en Access mgt.	Logische toegang, rechten, controle
11	Security Management	Baseline, mobiel, logging, monitoring, cryptografie
12	Fysieke beveiliging	Fysieke toegangsbeveiliging gebouwen
13	Computer Operations	Backup
14	BCM	BC planning, recovery
15	Supply Chain management	Service level mgt., leveranciersmgt.

In scope ADR onderzoek (centrale beheersing IB)

2.2 Analyse huidige situatie

Het ministerie heeft in 2017 ten aanzien van de 5 onderzochte aandachtgebieden op onderstaande vijfpuntsschaal uit het NBA-model een *gemiddeld* volwassenheidsniveau van 2.9 gescoord. De betekenis van de scores staan hieronder in tabel 1 uitgelegd.

[6] De handreiking bij het NBA model is te vinden op de NBAsite: https://www.nba.nl

	Naam	Omschrijving	Criteria
1	Initieel	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd • Niet of ad-hoc uitgevoerd • Niet/deels gedocumenteerd • Wijze van uitvoering afhankelijk van individu
2	Herhaalbaar	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd	• Control is geïmplementeerd • Uitvoering is consistent en standaard • Informeel en grotendeels gedocumenteerd
3	Gedefinieerd	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar.	• Control gedefinieerd o.b.v. risico assessment • Gedocumenteerd en geformaliseerd • Verantwoordelijkheden en taken eenduidig toegewezen • Opzet, bestaan en effectieve werking aantoonbaar
4	Beheerst en meetbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd en kwalitatief gecontroleerd.	• Periodieke (control) evaluatie en opvolging vindt plaats • Rapportage management vindt plaats
5	Continu verbeteren	Een ECO systeem is verankerd en draagt zorg voor een continue en effectieve controle en risicobeheersing	• Self-assessment, gap en root cause analyses • Real time monitoring • Inzet automated tooling

Tabel 1: Volwassenheidsniveau

Een gemiddelde score van 2.9 bij een initiële meting ten aanzien van centrale sturing en beheersing stemt tot enige tevredenheid. Echter, gezien het feit dat de context van de organisatie continu verandert en IB trends geen reden zijn voor optimisme, werkt JenV constant aan verbetering. Om een niveau omhoog te gaan in volwassenheid kost een complexe organisatie (als JenV) zeker een aantal jaren. En hoe hoger het niveau volwassenheid, des te hoger zijn ook de (jaarlijkse) kosten om dat niveau in stand te houden.

Uit het onderzoek van de ADR blijkt dat de belangrijkste sterktes en zwaktes van JenV als volgt kunnen worden getypeerd:[7]

[7] Het ADR 'onderzoeksrapport rijksbrede rapportage beheersing IB 2017' bevat een uitvoerige analyses van sterktes en zwaktes.

Sterktes	**Zwaktes**
• IB wordt in verschillende lagen gemanaged, zowel centraal als decentraal is kennis en expertise beschikbaar • Beleid en regelingen worden proactief en centraal gecoördineerd opgezet en actief kenbaar gemaakt • Er wordt centraal actief gestuurd op service levels	• Er zijn vele rijkskaders en regelingen, maar de samenhang in de veelheid ontbreekt • Er is geen centraal inzicht in de planning en uitkomsten van decentrale audits en pentesten • Bevindingen uit onderzoeken blijven soms lang liggen
Kansen	**Bedreigingen**
• Versterken van I(B) control door meten en sturen op basis van de juiste KPI's, waardoor betere sturing mogelijk is • Verbeteren van risico- en incidentmanagement, o.a. oefenen en herzien escalatieproces, vernieuwen incidentenregeling; betere en frequentere trendanalyses	• Uitwerking IB strategie en visie op lange termijn, staat door beperkte capaciteit en sturing op centrale beheersing onder druk, waardoor niet adequaat kan worden geanticipeerd op trends en ontwikkelingen (ad hoc karakter) • De ambitie en werklast is groter dan de beschikbare capaciteit voor IB, zowel centraal als decentraal en externe expertise is schaars

De ADR analyse geeft een heldere richting voor het plan van aanpak om tot betere centrale beheersing en sturing te komen. De verbeteringen de komende jaren zullen dan ook gericht zijn op het wegnemen van de zwaktes (centraal inzicht vergroten op stand van zaken bevindingen en onderzoeken) en benutten van de kansen (door ontwikkelen van de juiste KPI's en verbeteren van processen). De aandacht zal daarnaast moeten worden gericht op het complementeren van de PDCA cyclus, het hebben van inzicht en bevindingen op centraal niveau is niet voldoende ook de check op de daadwerkelijke activiteiten en het effect ervan creëert een continue verbetercyclus. Het is dan ook een groeimodel. Capaciteit en deskundig personeel zijn daarvoor een voorwaarde, waarbij we momenteel zien dat zowel rijks breed als in de markt de capaciteit schaars is.

2.3 De inrichting van IB

Informatiebeveiliging is binnen JenV op meerdere niveaus ingericht en georganiseerd, zowel centraal als decentraal. Tevens is er nog een separate verbeterplancyclus ingericht voor de eventuele bevindingen van de Auditdienst Rijk en de Algemene Rekenkamer. De verantwoordelijkheid voor beheersing van de IB is formeel belegd in de lijn. Hieronder wordt kort de governance ten aanzien van IB alsook de control nader toegelicht.

De organisatie van *IB governance* is binnen het ministerie op de hieronder genoemde manier vormgegeven.

CIO Raad en CIO stelsel
Het ministerie werkt met een CIO-stelsel waarbinnen alle taakorganisaties opereren met uitzondering van de twee sui generis organisaties[8] welke een uitzonderingspositie hierin vervullen. Het CIO-stelsel van JenV bestaat uit de departementale CIO en de CIO's van de afzonderlijke JenV taakorganisaties. Binnen het CIO-stelsel komt het beleid ten aanzien van informatievoorziening tot stand en wordt de uitvoering daarvan, waar nodig, gefaciliteerd en gemonitord. De CIO JenV

[8] De Politie en de Rechtspraak hebben binnen de organisatie van IB een speciale positie met eigen verantwoordelijkheden en rapportagelijnen. Dit in verband met de speciale positie (onafhankelijke, *sui generis*) die deze taakorganisaties innemen binnen het ministerie van JenV.

heeft zitting in de Bestuursraad JenV waardoor informatievoorziening en dientengevolge het onderwerp IB ook op het hoogste bestuurlijke niveau binnen JenV is geborgd. De CIO's van de taakorganisaties hebben een verantwoordingsplicht naar de departementale CIO ten aanzien van de departementale en rijksbrede Informatievoorziening (IV) kaders zo ook ten aanzien van informatiebeveiliging. Het op orde houden van de informatievoorziening en -systemen van de taakorganisaties is een verantwoordelijkheid van de taakorganisaties zelf. Immers op dit punt hoort de dagelijkse verantwoordelijkheid daar te liggen, waar deze het meest effectief is invloed uit te oefenen op de verbeteringen. Op centraal niveau ligt de verantwoordelijkheid voor:

1. Heldere kaders (o.a. BIR, etc.);
2. Beoordelen periodieke verantwoording door taakorganisaties;
3. Opvragen en toetsen van de "in control" verklaringen.

CISO board: security community
Alle grote JenV taakorganisaties hebben een eigen 'chief information security officer' (CISO) die rapporteert aan de CIO van het onderdeel. JenV heeft sinds april 2013 een 'CISO board' waar ook de sui generis organisaties in participeren en dat fungeert als voorportaal van de CIO Raad JenV. De rol van de security officers (CISO's) is op 29 augustus 2013 vastgesteld in de CIO Raad en omvat onder meer: ontwikkelen IB visie, strategie en beleid, toezicht op verbeterplannen en naleving IB kaders binnen het eigen organisatieonderdeel en de monitoring daarvan, gevraagd en ongevraagd adviseren van het lijnmanagement ten aanzien van vraagstukken op het gebied van informatiebeveiliging.

Security Operations Center (SOC JenV)
JenV heeft sinds 2016 een eigen 'Security Operations Center' (SOC). Het SOC JenV beschermt proactief de JenV brede IT-omgeving en mitigeert reactief alle dreigingen voor de IT-dienstverlening. Hiertoe biedt het SOC informatie, advies en ondersteuning aan de gebruikersorganisaties en beheerorganisaties bij de implementatie van:

- Proactieve IB-maatregelen om de kans op IB-incidenten te verkleinen, en
- Detectieve en repressieve IB-maatregelen om snel en adequaat te kunnen reageren op dergelijke incidenten, wanneer die zich voordoen[9].

Het belangrijkste doel van het SOC is het op tijd detecteren van en reageren op cyberdreigingen. Het SOC werkt hiervoor samen met de aangesloten taakorganisaties van JenV. Het SOC bewaakt de JenV-omgeving door te controleren op afwijkend gedrag in dataverkeer of in processen; het SOC signaleert kwetsbaarheden en risico's op het ICT-vlak; en adviseert de beheerorganisaties en verantwoordelijken over de oplossing daarvan. In 2018 is de capaciteit van het SOC verder uitgebreid.

Bureau BVA: toezicht op integrale veiligheid
Het Bureau BVA (beveiligingsautoriteit) is toezichthouder voor integrale veiligheid van het Ministerie. De BVA werkt onder andere samen met de beveiligingscoördinatoren van de JenV onderdelen om significante beveiligingsincidenten te signaleren en af te handelen. Binnen het Bureau BVA is ook de Functionaris Gegevensbescherming (FG) ondergebracht, die toezicht houdt op de verwerkingen van privacygevoelige gegevens.

IB-Control in het tweelaags besturingsmodel
De organisatie van *IB control* is op de volgende manier vorm gegeven.

[9] Gebaseerd op het adviesrapport Het Virtuele Rijks Security Operations Centre (SOC) dd. 7 maart 2014

Sinds 2017 is de aansturing van JenV aangepast van een drielaags naar een tweelaags model. Hierbij is tevens het werken met een eigenaar, opdrachtnemer en opdrachtgever ingevoerd. De control op IB is sinds 2017 ondergebracht in het planning en control proces. De deelnemers aan het CIO-stelsel zijn verantwoordingsplichtig aan de departementale CIO ten aanzien van de departementale en rijksbrede Informatievoorziening (IV) kaders en daarmee ook de IB kaders. De taakorganisaties rapporteren per tertaal de stand van zaken op basis van in de jaaraanschrijving uitgewerkte doelen. Deze worden eens per tertaal besproken in de accountgesprekken tussen eigenaar, opdrachtgever en opdrachtnemer. Daarnaast leggen alle JenV taakorganisaties jaarlijks verantwoording af over de informatiebeveiliging van het eigen onderdeel (in control verklaring ICV-IB). De deelverklaringen worden centraal gewogen en vertaald naar een ICV–IB voor heel JenV. De onderdeel overstijgende risico's worden opgenomen in de ICV-IB die JenV verstrekt aan het ministerie van BZK. Overige gesignaleerde risico's komen in de risicolog van Concern I-Control, die tijdens elke tertaal rapportage de opvolging met risico beperkende maatregelen monitort. Op deze wijze wordt erop toegezien dat IB in control is bij de J&V taakorganisaties en wordt op basis van de rapportages de behoefte aan beleid vastgesteld. Planning, uitvoering, controle en sturing vindt plaats op basis van een stelsel van wettelijke kaders (zoals AVG en de EU-richtlijn 'opsporing en vervolging') en rijksbrede kaders (zoals VIR, VIR-BI en BIR2017[10]).

Voor bevindingen van de Auditdienst Rijk en de Algemene Rekenkamer[11] is een separate verbeterplancyclus ingericht. De voortgang hiervan wordt op maandbasis gemonitord. Voor 2018 is de monitoring gericht op de geconstateerde onvolkomenheid inzake informatiebeveiliging. Voorts heeft JenV een Audit Committee ingesteld dat tot taak heeft het departementale management te adviseren op onder andere de volgende terreinen:

- het borgen van de kwaliteit van de bedrijfsvoering en de financiële verslaggeving;
- de regie op het auditbeleid;
- het risicomanagementbeleid en de uitkomsten daarvan.

[10] Besluit Voorschrift Informatiebeveiliging Rijksdienst[11] Het ADR 'onderzoeksrapport rijksbrede rapportage beheersing IB 2017'

[11] Het ADR 'onderzoeksrapport rijksbrede rapportage beheersing IB 2017'

3 Gewenste niveau; ambitie

3.1 Ambitie centrale beheersing van IB

De ADR heeft de departementen en het CIO-beraad van het Rijk geadviseerd om het *gewenste* volwassenheidsniveau (conform het NBA model voor de beheersing van IB) meerjarig te bepalen. Het verschil tussen het huidige niveau van volwassenheid en die ambitie kan worden gebruikt om zicht te krijgen op het groeitraject in de beheersing van informatiebeveiliging. Dit plan van aanpak IB is een uitwerking van dat advies. De ADR benadrukt daarbij dat niet naar een maximaal volwassenheidsniveau moet worden gestreefd, maar naar een optimaal niveau, rekening houdend met de risicobereidheid en karakteristieken van het betreffende aandachtsgebied op het departement.

Zoals ook in paragraaf 2.1 beschreven, wil JenV de centrale beheersing en sturing van IB verbeteren door het ontwikkelen van de juiste KPI's, het verbeteren van processen en het verder vergroten van centraal inzicht op stand van zaken op basis van uitgevoerde onderzoeken.

JenV streeft naar een *gemiddeld* volwassenheidsniveau over 5 aandachtsgebieden en 14 subgebieden in ca. 4 jaar van 2,9 in 2017 naar 4,0 in 2021. De ambities voor het groeien in volwassenheid zijn in de onderstaande tabel samengevat. De cijfers in 2017 zijn toegekend door de ADR.

NBA ID	Aandachtsgebied \ score	2017	2018	2019	2020	2021	2022+
GO	Governance (4 subgebieden)	3,0	3,0	3,3	3,6	3,9	4,0
OR	Organisatie (1 subgebied)	4,0	4,0	4,0	4,0	4,0	4,0
RM	Risicomanagement (3 subgebieden)	2,3	2,7	3,0	3,3	3,8	4,0
IM	Incidentmanagement (2 subgebieden)	2,0	2,5	3,0	3,3	3,5	4,0
SC	Supply management (4 subgebieden)	3,5	3,5	3,8	3,8	3,9	4,0
Gemiddelde score (over 14 subgebieden)		**2,9**	**3,1**	**3,3**	**3,6**	**3,8**	**4,0**

Tabel 2: De ambities voor het groeien in volwassenheid

De grootste groei wordt voorzien in de aandachtsgebieden risicomanagement en incident management alsook een versterking in de governance. Dezelfde aandachtsgebieden heeft de Algemene Rekenkamer ook expliciet genoemd in het Verantwoordingsonderzoek 2017. De mate van groei is afhankelijk van (beschikbare) mensen, middelen, technische en organisatorische haalbaarheid. Aangezien de aandachtsgebieden Organisatie en Supply Chain Management respectievelijk score 4 en 5 hebben, zal de focus in de verbeteringen de komende jaren zich hier richten op het vasthouden van het huidige niveau. De hoge score op het gebied van supply chain management staat voor het op orde hebben van het centrale deel inzake service level management van de gemeenschappelijke voorzieningen van JenV en het toezicht op derden inzake IB.

Met een groei naar het volwassenheidsniveau met de score 4 op de bovenstaande vijf aandachtsgebieden uit het NBA model ziet JenV dit als het niveau waarop de effectiviteit van de maatregelen (op een continue basis) periodiek wordt geëvalueerd en kwalitatief gecontroleerd. Alsdan zijn we in staat om:

- JenV breed (nog meer) richting, sturing en ondersteuning te geven aan informatiebeveiliging en effectieve naleving van de van toepassing zijnde

wet- en regelgeving waarbij ook nagedacht is over de risicobereidheid van het ministerie en haar taakorganisaties inzake IB;
- Beveiligingsincidenten zoveel mogelijk te voorkomen en, indien opgetreden, van een lagere impact en/of hogere hersteltijd te voorzien;
- De informatiesystemen veilig en betrouwbaar te houden door o.a. "security by design" beveiligingsmaatregelen te treffen;
- Onze informatie te beveiligen door actief onze netwerken en informatiesystemen te bewaken;
- De organisatie en haar medewerkers weerbaarder te maken door het kennisniveau omtrent IB te verhogen en periodiek te monitoren of de boodschap goed is afgestemd op de doelgroepen en de weerbaarheid daadwerkelijk verbetert.

Dit betekent dat de ***speerpunten*** c.q. aandachtsgebieden en bijbehorende doelstellingen voor de komende jaren als volgt zijn bepaald:

1 Het verbeteren van de governance van IB

- Activiteiten zijn gericht om het NBA model de komende jaren JenV breed in te voeren. Tevens worden KPI's omtrent IB gedefinieerd. Enerzijds wordt hiermee tegemoet gekomen aan de opmerkingen van de ARK om het centrale inzicht en sturing te verbeteren, anderzijds wordt hiermee nog verder invulling gegeven aan het verbinden van JenV doelstellingen inzake IB met de uitvoering in de taakorganisaties.

2 Versterken van risicomanagement

- Met het inrichten van een integraal register voor risico's die centraal én decentraal zijn gesignaleerd (risicolog) inclusief IB risico's heeft JenV de risico´s goed in beeld (due dilligence) en kan ze hierop sturen en ondersteunen (due care);
- Op basis van collectief inzicht en het besef dat samenwerking in de aanpak de snelheid en effectiviteit van oplossingen inzake risicomanagement kan vergroten, speelt het bestuursdepartement een coördinerende en faciliterende rol bij het ontwikkelen van methodiek en aanpak;
- Het risicobewustzijn van medewerkers wordt verhoogd. Bij beveiligingsincidenten is het onbewust handelen van de mens een belangrijke oorzaak. Om die reden wordt in kennis en kunde van medewerkers met betrekking tot informatiebewust handelen geïnvesteerd. Uit vorenstaande volgt ook dat medewerkers hierover in gesprek gaan met hun leidinggevende om de weerbaarheid in de het omgaan met waardevolle data te verhogen;
- Er ontstaat inzicht in de risico's omtrent dataverwerking in de ketens van JenV. Hierbij wordt een gezamenlijke aanpak en methodiek ontwikkeld om beveiligingsrisico's in de informatievoorzieningsketens van JenV te beheersen;
- Het SOC JenV wordt organisatorisch en instrumenteel in staat gesteld kwetsbaarheden en risico's beter te detecteren. Primaire processen van JenV worden gecontroleerd aangesloten op de monitoringsfunctie van het SOC.

3 Verbeteren van incidentmanagement

- Incidenten- en escalatieprocedures worden periodiek geëvalueerd;
- JenV heeft centraal breed zicht op de verschillende incidenten en datalekken in samenwerking met de BVA en de FG. Op basis van nieuwe inzichten wordt het beleid continu aangescherpt en geëvalueerd;
- De tijdige en effectieve afhandeling van beveiligingsincidenten wordt bewaakt en zo nodig bijgestuurd.

3.2 Aansluiten bij de ambitie van de Rijksoverheid

Naast de individuele elementen stelt de Rijksoverheid ook een aantal gezamenlijke maatregelen voor waar JenV waar relevant ook aan mee zal doen of al doet. Dit zijn bv de IB maatregelen uit de Nederlandse Digitaliseringsstrategie[12], Agenda Digitale Overheid[13] en de Agenda Digitale Overheid 'NL DIGIbeter' (ADO). In hoofdstuk 1.2 zijn deze elementen beschreven, in de onderstaande tabel staat de JenV invulling aan de rijksbrede ambities gespecificeerd en zijn deze waar mogelijk gekoppeld aan de speerpunten zoals hierboven beschreven.

Rijksbrede ambitie	**Bron**	**JenV invulling**
Implementatie centrale voorziening: vulnerability scanning	BZK	Aansluiting op SOC JenV *Speerpunt risicomanagement*
Opstellen vereiste beveiligingsmaatregelen	BZK	Bijdrage aan de uitwerking
Ontwikkelen van gezamenlijk kader voor een staatsgeheime werkplek	BZK	Bijdrage aan de uitwerking
Uitbouw Nationaal Detectie Netwerk (NDN) bij Rijksdienst	BZK	J&V is met het SOC aangesloten op het NDN. Nadere uitbouw wordt rijksbreed onderzocht
Vaststellen Baseline informatiebeveiliging overheid (BIO)	ADO	J&V stuurt aan op het per 1-1-2019 voldoen aan de BIR2017. De BIO is hier in zijn geheel op gebaseerd. *Speerpunt governance*
Onderzoek welke aanvullende maatregelen bij inkoop ter bevordering van de digitale veiligheid van hard- en software (DVHS) nodig en gewenst zijn	ADO	Bijdrage aan de uitwerking
Implementatie en doorontwikkeling Eenduidige Normatiek Single Information Audit (ENSIA) bij gemeenten	ADO	Geen, is BZK domein
i-Bewustzijn Overheid: Alertheid, kennis en vaardigheden van bestuurders, managers en medewerkers vergroten door middel van een overheidsbrede campagne	ADO	JenV heeft een awareness project Cybersecurity in 2018 opgezet. Nadat de strategie in 2018 is bepaald wordt hier in 2019 en 2020 verdere invulling aan gegeven. *Speerpunt risicomanagement*
Organiseren van overheidsbrede incident response capaciteit met het NCSC en CERTs (Computer Emergency Response Teams)	ADO	Bijdrage aan de uitwerking *Speerpunt incidentmanagement*
Opnemen categorie digitale overheid als	ADO	Geen, is BZK domein

[12] Nederlandse Digitaliseringsstrategie, Nederland Digitaal, bijlage bij Kamerstukken II 2017/18, 26643, 541

[13] NL Digibeter, Agenda Digitale Overheid, bijlage bij Kamerstukken 2017/18, 26643 nr. 549

Rijksbrede ambitie	**Bron**	**JenV invulling**
vitale infrastructuur, onderdeel van de Wet beveiliging netwerk- en informatiesystemen (Wbni)		
Versleuteling basisregistraties: Onderzoek naar afdoende bescherming tegen mogelijke beveiligingsrisico's	ADO	Geen, is BZK domein
Verhogen adoptie informatieveiligheidsstandaarden: • Onderzoek naar de stand van zaken implementatie van informatieveiligheidsstandaarden • Onderzoek of meer harde verplichtingen opportuun zijn op het gebied van de implementatie van informatieveiligheids-standaarden • Beschikbaar stellen meet-tool voor bulkmetingen t.a.v. de implementatie van informatie-veiligheidsstandaarden	ADO	Onderzoek eigen adoptie *Speerpunt governance*
Veilige overheidswebsites: Verplichten open informatieveiligheidsstandaard HTTPS	ADO	Onderzoek eigen sites *Speerpunt risicomanagement*
Herkenbaarheid overheidswebsites en e-mail: Onderzoek naar wenselijkheid om te komen tot één domeinnaam -extensie voor de overheid	ADO	Onderzoek eigen sites en e-mail *Speerpunt risicomanagement*
Verankering in wet- en regelgeving: Onderzoek of en hoe meer generiek informatieveiligheidsbeleid een plaats krijgt in de volgende tranche van de Wet Digitale Overheid	ADO	Bijdrage aan de uitwerking

Tabel 3: JenV invulling en betrokkenheid bij rijksbrede ambities

4 Hoe gaan we het doen; hoofdlijnen van activiteiten en roadmap

4.1 Projectmatige aanpak

Om aan de speerpunten die in dit plan van aanpak zijn genoemd invulling te geven, zal er waar nodig worden gekozen voor een projectmatige aanpak. Door deze manier van werken proberen we een goede balans te vinden tussen de verschillende aspecten van effectiviteit, efficiëntie, flexibiliteit en commitment.

Bij voorkeur werken we met een stuurgroep, projectleider, pilot en een project-planning. Aan de hand van een planning met mijlpalen wordt de oplossing door het projectteam uitgewerkt, getest en naar beheer overgedragen. Flexibiliteit, creativiteit en snelheid zijn hierbij belangrijk. Daar waar nodig zetten we ook nieuwe werkmethoden in zoals het actief ondersteunen van taakorganisaties van JenV met kleine teams die een bijdrage kunnen leveren bij vraagstukken. Samenwerking is van essentieel belang. Via de CISO community wordt deze zogenaamde "Vliegende Brigade" onderzoeksmethodiek ingevoerd, die eerder is toegepast als methodiek voor de Privacy Impact Assessments en ondersteuning van taakorganisaties bij de implementatie van AVG. Waar nodig werken we tevens kortcyclisch en flexibel (agile) aan onze doelstellingen.

4.2 Geplande activiteiten

Het behalen van niveau 4 voor de vijf aandachtsgebieden van de NBA-model inclusief de bovengenoemde speerpunten kost capaciteit en zal niet in alle gevallen op hetzelfde moment kunnen worden ingezet. Daarnaast is er een natuurlijke volgorde van activiteiten, zoals de afronding van de migratie naar de BIR2017 om vervolgens het volledig inrichten van risicomanagement op basis van KPI's. Tevens wordt bijgedragen aan de rijksbrede ambitie uit de genoemde stukken. J&V werkt daarom met een gefaseerde aanpak en roadmap waarin de verschillende activiteiten zijn opgenomen. Alhoewel de scope is gericht op het verder verbeteren van de centrale sturing en beheersing van IB wordt door de activiteiten ook een grote impuls gegeven aan IB op decentraal niveau.

Hieronder volgt per speerpunt op hoofdlijnen een beschrijving van activiteiten die JenV de komende jaren zal gaan uitvoeren. Deze activiteiten kunnen in de komende maanden en jaren nog worden aangescherpt of bijgesteld.

Verbeteren Governance IB:

Om ook in de toekomst een sterke centrale sturing te borgen is het van belang dat er ook op het gebied van de centrale governance en toezicht stappen worden gemaakt. Naast de vier eerder genoemde speerpunten worden op dit gebied op hoofdlijnen de volgende activiteiten ontplooit, zoals:

- De centrale IB visie, IB strategie het IB beleid vormen aantoonbaar de basis voor alle IB acties en metingen en zijn uitgewerkt in IB plannen, standaarden, procedures, maatregelen en instructies. Er worden KPI's voor IB op centraal en decentraal niveau gedefinieerd.
- Gelet op decentrale verantwoordelijkheid van de taakorganisaties is het de ambitie van J&V om het NBA model breder toe te passen in de JenV organisatie. Op deze wijze kan het ministerie J&V op IB gebied mogelijk naar een hoger level worden getild. In 2018 en 2019 starten daarvoor de eerste pilot projecten bij de JenV taakorganisaties. In 2020 en 2021 kan het NBA-model breder binnen JenV worden geïmplementeerd.

Versterken van risicomanagement:
Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement en het is de basis voor passende beveiligingsmaatregelen. Risicomanagement is het systematisch opzetten, uitvoeren en bewaken van acties om risico's te identificeren, te prioriteren en te analyseren. Om vervolgens voor deze IB risico's beleid te definiëren, processen en oplossingen te bedenken, te selecteren, uit te voeren en periodiek te reviewen. Dit proces zal de komende jaren worden versterkt in afstemming met het risicobeleid van de organisatie en omvat samengevat de volgende acties:

- IB training (incl. standaard methoden van risico-analyses) is ingericht
- De inzet van een "vliegende brigade" om vanuit het departement taakorganisaties te helpen bij de implementatie van IB maatregelen
- IB en privacy risico's worden conform het vastgestelde proces geïdentificeerd, beoordeeld, toegewezen aan een eigenaar, vastgelegd in een risicolog en geadresseerd in goedgekeurde actieplannen (zoals voor ketensecurity)
- Trendanalyses worden periodiek uitgevoerd, gereviewd en intern gecommuniceerd
- Het (top)management ontvangt periodieke risicorapportages op basis van KPI's met daarin de voortgang van de lopende actieplannen. Risico beperkende maatregelen en daarmee samenhangende kosten en restrisico's worden formeel geaccepteerd door het management.
- Verhogen van risicobewustzijn van medewerkers (security awareness):
  Het is een verantwoordelijkheid van JenV en haar taakorganisaties dat naast producten en diensten op het terrein van Cybersecurity ook geïnvesteerd wordt in kennis en kunde van medewerkers met betrekking tot informatiebewust handelen. De factor mens is belangrijk aangezien bijna driekwart van de beveiligingsincidenten wordt veroorzaakt door - het onbewust handelen van - de menselijke factor . Het versterken van deze schakel vormt de basis voor dit speerpunt met het uiteindelijke doel dit in de lijn te beleggen en het onderdeel van het functioneren te maken. Activiteiten zijn erop gericht, om samen met de taakorganisaties en andere relevante betrokkenen van JenV, het risicobewustzijn van managers en hun medewerkers te vergroten en daarmee de risico's van cyberdreigingen te beperken.

Bij het versterken van risicomanagement zal JenV bijdragen aan de uitwerking van de volgende rijksbrede ambities en onderzoek doen naar de toepassing ervan binnen de eigen organisatie:

- Opstellen en toezien op naleving vereiste beveiligingsmaatregelen;
- Ontwikkelen van gezamenlijk kader voor een voorziening voor staatsgeheime toepassingen Baseline informatiebeveiliging overheid (BIO);
- Onderzoek welke aanvullende maatregelen bij inkoop ter bevordering van de digitale veiligheid van hard- en software (DVHS) nodig en gewenst zijn;
- Verhogen adoptie informatieveiligheidsstandaarden;
- Veilige overheidswebsites: Verplichten open informatieveiligheidsstandaard HTTPS
- Herkenbaarheid overheidswebsites en e-mail: Onderzoek onder ondernemers en burgers naar wenselijkheid om te komen tot één domeinnaam -extensie voor de overheid

Verbeteren van incidentmanagement:
Incident Management is het centrale proces voor het melden voor beveiligingsincidenten. Voor beveiligingsincidenten kan een andere, snellere procedure gelden dan voor gewone incidenten afhankelijk van de ernst of categorie van het incident. Het is dus van groot belang dat de organisatie een

beveiligingsincident als zodanig herkent.

De komende jaren zal dit proces worden verbeterd met (samengevat) de volgende acties op hoofdlijnen:

- Het proces van incidentafhandeling en –escalatie is formeel vastgesteld en de beschreven rollen en verantwoordelijkheden zijn formeel toegewezen.
- Rollen en verantwoordelijkheden zijn verder vastgelegd tussen JenV onderdeel en leveranciers.
- De incident- en escalatieprocedure en incident responsplannen zijn geïmplementeerd en worden aan de hand van oefeningen en incidenten geëvalueerd en verbeterd.
- De incident respons teams (Red & Blue teams) zijn aangewezen en adequaat opgeleid.
- Onderzoeken hoe Security Monitoring van ketens effectief en interdepartementaal kan worden ingevuld. (o.a. onderlinge afspraken, vliegende brigades, samenwerking SOC's etc,)
- Tertaal rapportages beschrijven in hoofdlijnen de afhandeling van significante beveiligingsincidenten en de opvolging van leerpunten.
- Het SOC richt zich in 2019 en 2020 op het verder professionaliseren om haar primaire doel: het generieke netwerk en de generieke dienstverlening (Internet, E-mail, IAM, DigiJust, SAM, etc.) te monitoren en te beschermen tegen dreigingen alsmede het ondersteunen van de aangesloten partijen met het beveiligen van hun primaire processen en meest kritische systemen. Daarbij wordt gestreefd naar het aansluiten van alle taakorganisaties met kritieke systemen.
- Het SOC JenV levert tevens een bijdrage aan de rijksbrede initiatieven voor de Implementatie van vulnerability scanning als centrale voorziening en de uitbouw van het Nationaal Detectie Netwerk (NDN) bij Rijksoverheid.

Bij het versterken van risicomanagement zal JenV bijdragen aan de uitwerking van de rijksbrede Incident response capaciteit.

Een overzicht en globale eerste planning van de relevante activiteiten is te zien in de roadmap 2018-2021 in bijlage 1. Op basis van de urgentie, voortgang en resultaten zal de roadmap jaarlijks worden herijkt, geactualiseerd en waar nodig worden bijgesteld.

5 Risico's, begroting en capaciteit

5.1 Risico's voor het uitvoering van dit PvA

Op basis van de huidige situatie zijn de volgende risico's geïdentificeerd:

Kenmerken	Risico's	Tegenmaatregelen
Risico management suboptimaal	Sturen op onjuiste KPI's belemmert effectieve sturing en legt verkeerde focus en prioriteit. Het rendement van de inspanningen is suboptimaal. Dit vermindert weerbaarheid van de organisatie.	Onderzoek doen naar KPI en toegepaste KPI's periodiek evalueren
Incident management suboptimaal	Het is een zekerheid dat er in de toekomst incidenten zullen optreden. Als de organisatie onvoldoende risicobewust is en geen beproefde incidentenprocedure heeft, leveren incidenten meer schade op en is de hersteltijd langer.	Periodiek oefenen met Incidenten procedure Na oefening en incidenten de procedure evalueren
Samenhang IB kaders ontbreekt	Zorgt voor onduidelijkheid bij medewerkers. Dit vergroot de kans op IB incidenten.	IB kader 1.0 is opgesteld, evaluatie nog te doen
Ontbreken visie en acties op trends & ontwikkelingen	Trends en ontwikkelingen gaan harder dan wij kunnen bijhouden, waardoor een achterstand ontstaat in het op peil houden van beveiliging. De kwetsbaarheid van de organisatie neemt toe voor nieuwe dreigingen.	Gebruiken van IB visie en trendwatching bij andere organisaties zoals NCSC. Mogelijkheden nagaan voor samenwerking in- en extern JenV. Nadrukkelijk capaciteit voor analyse inplannen
Gebrek aan capaciteit	Plannen en verbeteracties blijven liggen, waardoor kwetsbaarheden niet worden weggenomen. Dit vergroot de kans op incidenten en datalekken.	Inhuren van capaciteit en selectief zijn met de inzet ervan. Regelmatige review gevraagde en beschikbare capaciteit
Onvoldoende IB samenhang in de keten	Procedures, rollen en IB maatregelen en monitoring sluiten niet goed aan tussen de verschillende ketenpartners.	Op ketenniveau aandacht vragen voor gezamenlijke oplossingen
Geen werkwijze cq. tooling om de PDCA cyclus voor IB effectief in te vullen	Geen eenduidige wijze om het BIR ISMS in te richten en te beheersen. Taak- en sui generis organisaties nemen zelfstandige en ongecoördineerde initiatieven die inefficiënt zijn	Nagaan of een onderzoek van de Vliegende Brigade hier meerwaarde oplevert

5.2 Capaciteit

De uitvoering van het plan zal de komende jaren zowel van het bestuursdepartement als ook van de taakorganisaties een meerjarige inspanning vereisen. Voor het bestuursdepartement zal dit uitkomen op een minimale inspanning van 2 fte tot maximaal 5 fte. Dit laatste omvat de inzet van een "vliegende brigade" om vanuit het departement hulp te bieden aan de taakorganisaties bij de implementatie van de verschillende IB activiteiten en speerpunten.
De capaciteit die per JenV taakorganisatie noodzakelijk is hangt af van verschillende factoren en zal verder worden onderzocht en beschreven in de verschillende project- of programmaplannen. Tevens zal de benodigde capaciteit samen met de taakorganisaties nader worden onderzocht.

5.3 Begroting

Een exacte financiële impact is gegeven de fase van het plan van aanpak op hoofdlijnen nog niet te bepalen. Bovenstaande speerpunten en bijbehorende activiteiten zullen in deelprojectplannen moeten worden uitgewerkt. Gegeven het feit dat centraal coördinatie wordt verwacht op de activiteiten alsook het monitoren van de resultaten zal budget voor het aantrekken van (extern) personeel op centraal niveau benodigd zijn. Voorts is nog niet bekend wat de taakorganisaties van JenV nodig zullen hebben om in gezamenlijkheid de plannen uit te voeren.

Een eerste inschatting is dat voor het uitvoeren van de activiteiten alsook de centrale coördinatie en monitoring ervan 500.000 euro per jaar projectbudget benodigd is. De begroting zal op basis van de ambities in een apart programma- of projectplan verder worden uitgewerkt. Waar noodzakelijk zullen decentraal en centraal aanvullende middelen beschikbaar worden gesteld.