Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Kenmerk
2015-0000640775

Bijlagen
5

Datum 4 november 2015
Betreft Beslissing op uw Wob-verzoek

Geachte

Bij brief van 14 juli 2015, ontvangen op 15 juli 2015, heeft u bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een verzoek ingediend als bedoeld in artikel 3, eerste lid, van de Wet openbaarheid van bestuur (hierna ook: Wob). Uw verzoek heeft betrekking op de Taskforce Bestuur en Informatieveiligheid Dienstverlening (hierna ook: Taskforce BID).

Meer in het bijzonder verzoekt u om openbaarmaking van documenten die gaan over dan wel betrekking hebben op:

1. De geformuleerde doelstellingen van de Taskforce BID inclusief de vastgestelde definitie van 'Verplichtende Zelfregulering';
2. De geformuleerde evaluatiecriteria ten aanzien van het bereiken van bovengenoemde doelstellingen van de Taskforce BID (..);
3. Een overzicht van de concrete middelen welke zijn ontwikkeld 'om sturing op informatieveiligheid door bestuur en topmanagement binnen de overheid ook echt mogelijk te maken', uitgesplitst per concreet middel. Daarnaast (..) wat de gelieerde ontwikkelkosten zijn (per concreet middel) inclusief de personele kosten;
4. De feitelijke onderbouwing van het behalen van de eerder genoemde doelstelling(en) (..). Kortom hoe is vastgesteld dat de doelstellingen zijn behaald?;
5. De bijdragen van de Taskforce BID aan het regeringsbeleid;
6. De bijdragen van de Taskforce BID aan de beleidsdoelstellingen van de Cyber Security Strategie 2.0;
7. De personeelskosten voor de periode:
   a. 2013-2014 (eerste operationele jaar van de Taskforce BID);
   uitgesplitst per functie, uitgesplitst per leverancier.
   b. 2014-2015 (tweede operationele jaar van de Taskforce BID);
   uitgesplitst per functie, uitgesplitst per leverancier;

8. De aanbestedingsprocedure van leveranciers voor de inhuur van extern personeel die de Europese drempelwaarde voor overheidsopdrachten heeft overschreden zoals bepaald in de vigerende richtlijnen;
9. De overige (operationele kosten) voor de periode:
   c. 2013–2014 (eerste operationele jaar van de Taskforce BID); uitgesplitst per operatie, uitgesplitst per leverancier.
   d. 2013–2014 (eerste operationele jaar van de Taskforce BID); uitgesplitst per operatie, uitgesplitst per leverancier;
10. De totale kosten die zijn gemoeid met de uitvoering van de Taskforce BID inclusief de aanloopkosten om te komen tot de oprichting van de Taskforce BID en de kosten welke gemoeid zijn met het beëindigen c.q. overdracht van de Taskforce BID;
11. De aanbestedingsprocedure(s) van de overige leverancier(s) die de Europese drempelwaarden voor overheidsopdrachten heeft overschreden zoals bepaald in de vigerende richtlijnen".

Daarnaast heeft u, verwijzend naar de 'Eindrapportage Taskforce Bestuur en Informatieveiligheid Dienstverlening' verzocht om openbaarmaking van documenten "die gaan over dan wel betrekking hebben op:

1. 'De verankering van verplichtende zelfregulering per overheidslaag' (..).
   a. Hoe is deze 'verankering' gedefinieerd en wat is de gehanteerde grondslag om deze 'verankering' vast te stellen?
2. 'De gehanteerde leerstrategie' (..)
   a. Wat houdt deze 'leerstrategie' in?
3. 'Aanvullende risicoanalysemethodiek' (..)
   a. Wat is de beoogde datum van oplevering van de aanvullende risicoanalysemethodiek? Indien reeds opgeleverd, ontvang ik hiervan graag een kopie.
   b. Graag ontvang ik de conceptversie zoals hierboven beschreven".

Bij brief van 16 juli 2015, kenmerk 2015-0000403654, heb ik de ontvangst van uw verzoek bevestigd.

Bij brief van 4 augustus 2015, kenmerk 2015-0000447219, is de termijn om op uw verzoek te beslissen met vier weken verlengd.

Bij brief van 31 augustus 2015, kenmerk 2015-0000507375, is aan u meegedeeld dat de beslistermijn is opgeschort vanwege het vragen van zienswijzen aan een derde.
Bij brief van 2 oktober 2015, kenmerk 2015-0000574592, bent u geïnformeerd over de beëindiging van de opschorting van de beslistermijn en heb ik meegedeeld dat u met circa vier weken doch uiterlijk op 2 november 2015 een beslissing op uw verzoek tegemoet kunt zien. Helaas was nog net een enkele dag extra nodig om uw verzoek af te handelen.
Door de derde belanghebbende zijn geen bedenkingen ingediend.

In de eerste plaats attendeer ik u erop dat de Wet openbaarheid van bestuur niet van toepassing is op informatie die reeds openbaar is.
Verder heeft de Wob uitsluitend betrekking op bij het bestuursorgaan berustende informatie die is neergelegd in documenten over een bestuurlijke aangelegenheid.

Bestaan desbetreffende documenten niet, dan kunnen deze ook niet openbaar worden gemaakt. Ook kent de Wob geen verplichting om gegevens te verzamelen of te vervaardigen.

De door u gevraagde informatie is deels al openbaar. Ook stelt u deels feitelijke vragen die aan de hand van al openbare informatie kunnen worden beantwoord. Voor zover uw verzoek onder de reikwijdte van de Wob valt, zijn in totaal 5 documenten aangetroffen, te weten:

Nr.	Type	Naam document	Datum
1	Document	Inrichtingsplan Taskforce BID	04-12-2012
2	Document	Programmaplan Taskforce BID	03-06-2013
3	Document	Dechargeverzoek en eindafrekening project Taskforce BID	23-09-2015
4	Document	Leeraanbod	Juni 2013
5	Document	Opleidingsplan "leren binnen de overheid op informatieveiligheid"	Juni 2013

Hieronder loop ik de onderdelen van uw verzoek stuk voor stuk na.
Uw feitelijke vragen zal ik zo goed als mogelijk beantwoorden. Daar waar de door u verzochte informatie al openbaar is, attendeer ik u daarop en geef ik u als service de vindplaats van die informatie.
Ik heb besloten om aan uw Wob-verzoek tegemoet te komen door de 5 bij mij berustende documenten openbaar te maken.

Beantwoording vragen en bijhorende documenten

1. U vraagt naar de geformuleerde doelstellingen van de Taskforce BID, inclusief de definitie van verplichtende zelfregulering.
   Voor een antwoord op deze vraag verwijs ik u in de eerste plaats naar mijn brief aan de Tweede Kamer van 22 maart 2013 (TK 2012-2013, 26643 nr. 269).
   De overige documenten die hierop betrekking hebben zijn het inrichtingsplan van de Taskforce BID en het programmaplan van de Taskforce BID.
   U treft beide documenten bijgaand aan.
   Met name de hoofdstukken 2 en 3 van het inrichtingsplan hebben betrekking op dit onderdeel van uw verzoek. Wat betreft het programmaplan van de Taskforce BID, verwijs ik u naar hoofdstuk 4, waarin wordt ingegaan op de zelfregulering.

2. Ten aanzien van de geformuleerde evaluatiecriteria met betrekking tot het bereiken van de doelstellingen van de Taskforce BID verwijs ik u in de eerste plaats naar mijn brief aan de Tweede Kamer van 18 december 2014 (TK 2014-2015, 26643 nr. 344).
   In deze brief wordt ingegaan op de inbedding van verplichtende zelfregulering bij de diverse overheidslagen, hoofddoel van de Taskforce BID.
   Daar de Taskforce BID de verplichtende zelfregulering door de afzonderlijke overheidsorganisaties heeft gestimuleerd en per overheidslaag (Rijk, provincies, gemeenten en waterschappen) maatwerk heeft toegepast, verschillen de criteria per overheidslaag. Per overheidslaag is gerapporteerd aan de Tweede Kamer, waarbij is uitgewerkt op welke wijze de verplichtende

zelfregulering vorm en inhoud heeft gekregen. Hiermee zijn deze documenten reeds openbaar. De eindrapportage, waarmee u blijkens uw verzoek reeds bekend bent, is openbaar. Volledigheidshalve geef ik u de vindplaats op internet: https://zoek.officielebekendmakingen.nl/blg-441750.

3. Het door u verzochte overzicht van de concrete middelen welke zijn ontwikkeld om sturing op informatieveiligheid door bestuur en topmanagement binnen de overheid mogelijk te maken, treft u aan in het bij punt 1. genoemde programmaplan en in de reeds openbare eindrapportage van de Taskforce BID (vindplaats gegeven bij punt 2).

   Met betrekking tot de overige door u onder uw punt 3 genoemde aspecten informeer ik u dat de informatie die daarover bij mij berust, is te vinden in de zogenoemde decharge en in de eindafrekening. Op het moment van ontvangst van uw Wob-verzoek, welk moment bepalend is voor de beslissing op uw verzoek, had ik het dechargeverzoek en de eindafrekening van de Taskforce BID in gang gezet, maar nog niet afgerond. Om u zo goed mogelijk van dienst te zijn en zo volledig mogelijk te informeren maak ik in reactie op uw verzoek de definitieve decharge en eindafrekening van de Taskforce BID met als vaststeldatum 23 september 2015, openbaar. U treft deze documenten bijgaand aan. U vindt hierin een overzicht van de kosten van de Taskforce BID, uitgesplitst per jaar en aandachtsgebied.

4. U vraagt naar informatie over de feitelijke onderbouwing van het behalen van de eerder genoemde doelstelling(en) van verplichtende zelfregulering ten aanzien van informatieveiligheid per overheidslaag. Meer concreet vraagt u hoe is vastgesteld dat de doelstellingen zijn behaald.
   In zoverre verwijs ik u naar de eerder genoemde documenten, alsook naar de reeds openbare interbestuurlijke verklaring. Deze verklaring vindt u hier: http://www.wpm.nl/binaries/content/assets/wpm---website/bestuur/db/2014/2dec/a03a2-interbestuurlijk-samenwerking-informatieveiligheid-2014.25324.pdf
   In deze verklaring, van najaar 2014, hebben de medeoverheden en mijn ministerie met elkaar afgesproken door te gaan met de verplichtende zelfregulering na beëindiging van de Taskforce BID. Hieruit kunt u opmaken dat de doelstelling van de Taskforce BID, om als aanjager informatieveiligheid een structurele plek te geven in de reguliere bedrijfsprocessen van overheidsorganisaties, is bereikt en dat de medeoverheden hier de komende periode verder mee doorgaan.

5. De bijdragen van de Taskforce BID aan het regeringsbeleid zijn reeds publiek toegankelijk. Ik verwijs u op dit punt naar mijn brieven aan de Tweede Kamer van 23 mei 2013 (TK 2012-2013, 26643 nr. 280), 5 november 2013 (TK 2013-2014, 26643 nr. 292) en 23 juni 2014 (TK 2013-2014, 26643 nr. 316).

6. Ook de bijdragen van de Taskforce BID aan de beleidsdoelstellingen van de Cyber Security Strategie 2.0. zijn openbaar. Ik verwijs u op dit punt naar mijn zogenoemde Voortgangsbrief realisatie werkprogramma Nationale Cyber Security Strategie 2 van 18 december 2014 aan de Tweede Kamer (TK 014-2015, 26643 nr. 341).

Wat betreft de doelstelling 'Lokale overheden committeren aan een versterkte aanpak van informatieveiligheid' verwijs ik u naar hetgeen ik hiervoor heb uiteengezet onder de punten 2, 3 en 4 en naar de daar genoemde (Kamer)stukken. In deze Kamerstukken is uitgewerkt op welke wijze het versterken van de aanpak op informatieveiligheid door de lokale overheden gestalte heeft gekregen.

7. De door u gevraagde informatie over de personele kosten voor de perioden 2013-2014 en 2014-2015 vindt u in de eerder genoemde en bij dit besluit openbaar gemaakte decharge en eindafrekening van de Taskforce BID.
   Ik beschik niet over een uitsplitsing per functie en leverancier, zodat ik in zoverre uw verzoek niet kan inwilligen.

8. U vraagt naar de "aanbestedingsprocedures van leveranciers voor de inhuur van extern personeel die de Europese drempelwaarde voor overheidsopdrachten heeft overschreden zoals bepaald in de vigerende richtlijnen". Ik kan u daarover als volgt informeren.
   Voor alle inhuuropdrachten geldt dat het rijksbrede inkoopbeleid is gevolgd. Daar waar van toepassing zijn de geldende raamovereenkomsten benut. Buiten hun scope zijn inhuuropdrachten boven de €50K en onder de €207K (de in dit geval geldende Europese drempelwaarde voor overheidsopdrachten) meervoudig onderhands uitgezet. Voor inhuuropdrachten die deze drempelwaarde overschreden is een verlicht regime gevolgd, daar deze waren aangemerkt als 2B-dienst, te weten de categorie arbeidsbemiddeling. Verder kan ik u meedelen dat het totaalbedrag voor externe inhuur € 3.812.611, 42 bedraagt. Dit betreft een totaal van 31 inhuuropdrachten.

9. De door u gevraagde overige (operationele kosten) voor de perioden 2013-2014 en 2013-2014 (bedoeld zal zijn: 2013-2014 en 2014-2015) vindt u in de eerder genoemde en bij dit besluit openbaar gemaakte decharge en eindafrekening van de Taskforce BID.
   Ik beschik niet over een uitsplitsing per operatie en leverancier, zodat ik in zoverre uw verzoek niet kan inwilligen.

10. De door u gevraagde informatie over de totale kosten die zijn gemoeid met de uitvoering van de Taskforce BID inclusief de aanloopkosten om te komen tot de oprichting/inrichting van de Taskforce BID en de kosten die zijn gemoeid met het beëindigen dan wel de overdracht van de Taskforce BID, vindt u in de eerder genoemde en bij dit besluit openbaar gemaakte decharge en eindafrekening van de Taskforce BID.

11. U vraagt naar "de aanbestedingsprocedure(s) van de overige leverancier(s) die de Europese drempelwaarden voor overheidsopdrachten heeft overschreden zoals bepaald in de vigerende richtlijnen". Ik kan u daarover als volgt informeren.
    Voor alle opdrachten geldt dat het rijksbrede inkoopbeleid is gevolgd. Daar waar van toepassing zijn de geldende raamovereenkomsten benut. Buiten hun scope zijn opdrachten boven de €50K en onder de €207K meervoudig onderhands uitgezet (conform de circulaire zoals deze is opgesteld voor opdrachten boven de €50K en onder de van toepassing zijnde Europese drempelwaarde voor overheidsopdrachten).

Er zijn geen 2A diensten (niet gedekt zijnde door een raamovereenkomst) van overige leveranciers die een contractwaarde hebben hoger dan de Europese drempelwaarde, zodat ik in zoverre uw verzoek niet kan inwilligen.

Met betrekking tot de overige punten van uw verzoek informeer ik u als volgt.

1. Informatie over de verankering van de verplichtende zelfregulering en de wijze waarop die is gedefinieerd, vindt u in het hiervoor onder punt 1 genoemde en bij dit besluit openbaar gemaakte inrichtingsplan en het programmaplan van de Taskforce BID. Ook vindt u daar een antwoord op uw feitelijke vraag naar de gehanteerde grondslag om de verankering vast te stellen.

2. De door u gevraagde informatie over (de inhoud van) de leerstrategie van de Taskforce BID is te vinden in het leeraanbod en het opleidingsplan. Deze documenten maak ik in reactie op uw verzoek openbaar. U treft ze bijgaand aan.

3. In reactie op de door u gevraagde aanvullende risicoanalysemethodiek en uw feitelijke vraag naar de beoogde datum van oplevering van de risicoanalysemethodiek, informeer ik u in de eerste plaats dat het traject voor het opstellen van een handleiding voor het gebruik van Information Risk Assessment Methodology (IRAM) binnen de Rijksdienst in juni 2015 is afgerond.
   De handleiding is een zogenoemd "levend document" dat op basis van (verdere) ervaringen wordt onderhouden. Bovendien berust het copyright ervoor bij het Information Security Forum (ISF). De handleiding is beschikbaar voor gebruik binnen de Rijksoverheid omdat de Rijksdienst lid is van het ISF en daardoor het recht heeft op gebruik van de methodiek en bijbehorende hulpmiddelen. Vanwege deze omstandigheden kan ik uw verzoek om publiek toegankelijk maken van de handleiding niet inwilligen. De economische of financiële belangen van de Staat (artikel 10, tweede lid, aanhef en onder b, van de Wob) en het belang van het voorkomen van onevenredige bevoordeling of benadeling (artikel 10, tweede lid, aanhef en onder g, van de Wob) van het ISF dan wel van medewerkers die werken aan de handleiding of andere natuurlijke personen of rechtspersonen dan wel derden wegen in dit geval naar mijn oordeel zwaarder dan het algemene belang van openbaarmaking dat de Wob vooronderstelt.

U zult zien dat op enkele plaatsen in de bij dit besluit openbaar gemaakte documenten gegevens zijn zwartgemaakt. De zwartgemaakte informatie betreft (voor)namen, handtekeningen en directe contactgegevens zoals telefoonnummers en e-mailadressen van individuele ambtenaren en/of andere individuele personen. Deze gegevens maak ik niet openbaar in verband met het belang van de eerbiediging van de persoonlijke levenssfeer van de betrokken individuele personen. Dit belang, dat wordt vermeld in artikel 10, tweede lid, aanhef en onder e, van de Wob acht ik hier zwaarwegender dan het algemene belang van openbaarmaking van deze tot individuele personen herleidbare gegevens.

Dit Wob-besluit en de stukken die hiermee voor een ieder openbaar worden gemaakt, worden zo spoedig mogelijk na toezending gepubliceerd op de website www.rijksoverheid.nl.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Datum
4 november 2015

Kenmerk
2015-0000640775

Hoogachtend,
De minister van Binnenlandse Zaken en Koninkrijksrelaties,
namens deze,

Richard van Zwol
Secretaris-generaal

Bijlagen:
-Inrichtingsplan
-Programmaplan
-Decharge en eindafrekening
-Leeraanbod
-Opleidingsplan.

Belanghebbenden kunnen binnen zes weken na bekendmaking van het in deze brief opgenomen Wob-besluit daartegen per brief bezwaar maken. Het bezwaarschrift moet door de indiener zijn ondertekend en bevat ten minste zijn naam en adres, de dagtekening, een omschrijving van het besluit waartegen het bezwaar is gericht en de gronden waarop het bezwaar rust. Zo mogelijk dient een kopie van het besluit waartegen het bezwaar is gericht te worden bijgevoegd. Het bezwaarschrift moet worden gericht aan de minister van Binnenlandse Zaken en Koninkrijksrelaties/Directoraat-generaal Bestuur en Koninkrijksrelaties/Directie B&I, Postbus 20011, 2500 EA Den Haag.

Taskforce Bestuur en veilige dienstverlening

Inrichtingsplan: opdracht, strategie, programmeren, besturen, organiseren en begroten

[redacted]

4 december 2012

Taskforce Bestuur en veilige dienstverlening

Inrichtingsplan: opdracht, strategie, programmeren, besturen, organiseren en begroten

Inhoud Pagina

1. Inleiding

Mede naar aanleiding van het zogenaamde 'DigiNotar-incident' en de perikelen rond 'Lektober', is vanuit overheden en verbonden organisaties een pakket van maatregelen in voorbereiding om de uitvoering van de overheidsinformatiebeveiliging verder te verbeteren. Zie bijlage 1voor een overzicht van deze maatregelenen bijlage 2 voor de schetsvan het stelsel en de verantwoordelijke spelers. Een van de door BZK voorgenomen maatregelen is om in januari 2013 een interbestuurlijke taskforce in te stellen voor een periode van twee jaar. Met de instelling van de taskforce komt de minister van Binnenlandse Zaken en Koninkrijksrelaties tegemoetaan de aanbeveling van de Onderzoeksraad voor de Veiligheid om een programma te ontwikkelen 'om bestuurders te doordringen van het belang van digitale veiligheid en hen te voorzien van voldoende inzicht en vaardigheden'. Deze aanbeveling is gedaan in het onderzoek 'HetDigiNotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt'.De kabinetsreactie op dit onderzoeksrapport is apart bijgevoegd als bijlage 3.

De hoofdtekst van deze rapportage is gericht op de benodigde besluitvorming. De bijlagen bevatten de nadere uitwerking, waarbij op het terrein van de programmering en samenwerking per domein nadere invulling nadrukkelijk mogelijk is. Er is intensief overleg geweest met vertegenwoordigers vanuit de verschillende domeinen, zoals aangeven in bijlage 4. Een concept van deze rapportage is besproken in de Programmaraad DigiNotar.

De onderhavige rapportage bevat de voorstellen om de snelle start per 1 januari 2013 mogelijk te maken. De vertegenwoordigers van betrokken partners hebben hierop commitment gegeven in de projectgroep opvolging DigiNotar.

Het dagelijks bestuur van de regiegroep BRG E-overheid en dienstverlening heeft dit commitment bekrachtigd in haar vergadering op 30 november 2012. Voorzien is dat de formele bekrachtiging van de start van de taskforce plaatsvindt in de eerstvolgende BRG, die is gepland voor medio februari. Het streven is dat de deelnemers aan de BRG dan een gezamenlijk statement over de taskforce vaststellen. De opstelling van dit statement zal de komende weken plaats vinden in overleg met betrokken partijen.

Nog in december en januari vindt bij alle betrokken overheidsdomeinen nadere bestuurlijke besluitvorming plaats over de inrichting van de taskforce.

De deelnemers daarvan hebben daarin aangegeven aan te sturen op bestuurlijk commitment van hun organisatie

Eventueel noodzakelijk raadplegen van leden/ algemeen besturen zal overigens soms pas later plaats vinden. De volgende situatie geldt.

28/11 heeft dagelijks bestuur Unie van waterschappen zich positief uitgesproken, maar moet nog wel in overleg met leden; dat zal pas in april plaats vinden

7/12 vindt overleg plaats in de VNG Bestuurlijke Commissie Dienstverlening en ICT. Ook hier geldt dat een raadpleging van leden pas later kan.

12/12 kan de manifestgroep zich uitspreken.

13/12 IPO; besluitvorming daar zal niet meer lukken; wel zijn er ambtelijk en bestuurlijk positieve standpunten tot nu toe; in januari nadere standpuntbepaling.

7/12 Rijk, behandeling in stuurgroep opvolging DigiNotar; het ICCIO (interdepartementaal overleg CIO's) is in januari

2. Opdracht van de taskforce

Informatieveiligheid is te omschrijven als de bescherming van informatie en informatiestromen tegen bedreigingen die de continuïteit van de dienstverlening kunnen verstoren, schade kunnen veroorzaken en de goede werking kunnen verhinderen. De geformuleerde bedreigingen duiden in de allereerste plaats op aanzienlijke persoonlijke, maatschappelijke en politieke risico's ten gevolge van onvoldoende beveiliging.

Het risico van de continuïteit van dienstverlening dooraanvallen, maar even goed door technisch falen, is daarbij een heel ander risico dan dat van schending van vertrouwelijkheid en privacy, en weer anders dan van op bijvoorbeeld financieel voordeel gerichte cybercriminaliteit. De risico's zijn niet uit te bannen; het gaat om omgang met deze risico's en om lastige afwegingen zoals kosten en baten van veiligheid, openbaarheid en privacy.

Uit het genoemde OVV-onderzoek blijkt dat er bestuurlijk en topmanagerial binnen de overheid sprake is van onvoldoende risicobewustzijn en gerichtheid op veilige ICT-dienstverlening. De relevantie van het onderwerp is bijna niet te overschatten en de omgang ermee moet het karakter hebben van afwegingen van risico's en daarop toegespitst beleid en handelen.

De taskforce gaat zich dan ook richten op de bestuurlijke en managerial gerichtheid op informatie-veiligheid en de verankering daarvan in de reguliere werkprocessen van de verschillende overheids-domeinen. Afwegings- en handelingsbekwaamheid van bestuurders en topmanagers dienen voorop te staan. De technische complexiteit van informatieveiligheid, die tot de bijna natuurlijke reflex leidt om deze veiligheid vergaand aan de technici over te laten, is daarbij een van de grootste bedreigingen van het leerproces zelf. Die gerichtheid en handelingsbekwaamheid dienen dan ook verankerd te zijn in de primaire en bedrijfsvoerings- en controlprocessen van de organisatie. Juist bij kwesties van risicobewustzijn, is voortdurende interactie tussen ervaring in de organisatieprocessen en scherpe gerichtheid op omgang met risico's een noodzaak. Zonder die wisselwerking verzwakt het risicobewustzijn en komt actiegerichtheid vooral weer bij 'het volgende incident'.

Onderscheiden is naar de 'domeinen' gemeenten, waterschappen, provincies, ZBO's en Rijk. De taskforce moet dus het leerproces in deze domeinen faciliteren van verscherping van bewustzijn en handelingsgerichtheid op veilige ICT-dienstverlening en de operationalisatie van het leerproces in de organisaties en domeinen. De taskforce is gericht op het borgen daarvan in de processen van beleidsontwikkeling, bedrijfsvoering, control, toezicht en interbestuurlijke samenwerking en op de continuïteit van leerproces en borging.

De Taskforce heeft dus niet tot taak in alle lacunes te gaan voorzien;organisaties en domeinen zijn zelf verantwoordelijk voor een goed informatiebeveiligingsbeleid dat leidt tot een goed weerbaarheid en herstelvermogen. De doelen van leren en verankering staan wel in een breed kader van maatregelen om de informatiebeveiliging te verbeteren zoals in bijlage 1 en 2 geschetst. De taskforce zal ook tot taak hebben deze coördinatie te bevorderen en waar nodig over het gehele beleid nader te adviseren. Deze bevordering van coördinatie is een dringende wens van de andere overheden. De taskforce zal het in bijlage 1 en 2 geschetste overzicht na instelling overheidsbreed uitwerken. Zie verder hoofdstuk 5 over sturing en organisatie waar ook een opvolging van de programmaraad DigiNotar is voorgesteld.

De taskforce heeft een looptijd van twee jaar. Het doel is dat daarna in elk domein een verankerd informatieveiligheidsbeleid functioneert. Dat is geen vrijblijvende doelstelling en de realisatie van die doelstelling moet ook transparant zijn. Een **verplichtende** vorm van **zelfregulering** per **domein** lijkt geëigend, maar de taskforce evalueert de voortgang en doet nader onderzoek waar nodig. Indien informatieveiligheid na twee jaar onvoldoende geborgd is, heeft de minister van BZK aangekondigd wetgeving te overwegen. Aangezien de open standaarden voor informatiebeveiliging ISO 27001 en ISO 27002 al op de 'Comply or Explain' (pas-toe-of-leg-uit')-lijst van het Forum Standaardisatie zijn opgenomen als verplichte standaarden voor de hele overheid, ligt het in de rede dat deze standaarden de belangrijke leidraad zullen zijn voor het handelen dat vorm geeft aan deze zelfregulering.

De volgende opdracht voor de taskforce is geformuleerd:

1. De bewustwording te versterken van bestuur en managementtop van de eisen aan informatie-veiligheid, met name ook vanuit maatschappelijke en politieke risico's.
2. Een leerstrategie uit te voeren voor een actieve gerichtheid van bestuur en top op adequate aanpak van informatieveiligheid dienstverlening.
3. De lange termijn verankering van informatieveiligheid en gerichtheid daarop in de reguliere processen en informatieketens te versterken, waarbij gerichtheid op weerbaarheid en herstel deel zijn van die verankering. Een verplichtende vorm van zelfregulering per domein is het beoogde einddoel van die verankering.
4. De overheidsbrede coördinatie rond het stelsel van informatiebeveiliging te bevorderen en te adviseren over dit stelsel.
5. Voor zover nodig aanvullend onderzoek te doen verrichten.

3. Leerstrategie, zelfreguleringen programmering

De Minister van BZK heeft aangegeven na twee jaar de afweging te maken of wetgeving noodzakelijk is of niet. Een alternatief voor wetgeving is verplichtende zelfregulering per domein, waarvan de werking transparant is en die de minister in staat stelt zich over de werking van het stelsel naar de Tweede Kamer te verantwoorden. De opdracht van de taskforce is geoperationaliseerd naar een strategie die moet uitmonden in zelfregulering per organisatie en domein op basis van de volgende uitgangspunten:

Het einddoel van de taskforce is dus om per domein en organisatie te komen tot wat genoemd is 'verplichtende zelfregulering van de informatieveiligheid'. Die zelfregulering komt de komende twee jaar tot stand door een iteratief proces van 'leren' en 'het verankeren' daarvan in de organisatie en het domein.

3.1 Leerstrategie naar zelfregulering

Deze leerstrategie is uitgewerkt in bijlage 5 'Leerstrategie[1], zelfregulering en programmering' en komt in het kort neer op het volgende:

- Een stapsgewijs proces naar verankering van informatieveiligheid in organisatie en domein.
  - Het versterken van het risicobewustzijn en de kennis inzake informatieveiligheid.
  - Het ontwikkelen van een probleemanalyse en veranderstrategie gericht op continue informatieveiligheid.
  - De implementatie van die veranderstrategie in organisatie- en domeinprocessen met daarin ook vormen van leren en trainen.
  - Het oogsten en reviewen van de resultaten van het leer- en verankeringsproces.
- De opbouw van de leer- en verankeringsprocessen naar de specifieke situatie per domein en per organisatie. In bijlage 5 is het onderscheid 'eerste en tweede orde veranderen en leren' gemaakt. Bij tweede orde is een aantal structurele veranderingen vereist in gerichtheid en gedrag en verankering daarvan in structuren en werkprocessen. Tweede orde eist dus een andere leerstrategie als eerste-ordeverandering.Per domein en binnen de domeinen is de situatie verschillend en is dus ook een verschillende inrichting vereist.
- Vormgeven van leer- en verankeringsprocessen naar de principes van de veiligheidsketen van proactie, preventie, preparatie, respons,herstel.

---

[1] De leerstrategie is ook met name gebaseerd op de in de bijlage 5 bijgevoegde notitie van prof. dr. Ira Helsloot.

- Voortdurende trainen van een scherp risicobewustzijn en adequate handelingsgerichtheid door ook bestuurlijk te oefenen met situaties van omgang met verschillende soorten risico's als van continuïteit van dienstverlening en afwegingen van kosten en baten van mogelijke maatregelen.

3.2 Verplichtende zelfregulering

Deze leerstrategie moet uiteindelijk uitmonden in zelfregulering per organisatie en domein op basis van de volgende uitgangspunten. Zie de bijlage 5 voor een al iets verdere uitwerking, die na de instelling van de taskforce prioritair nader vorm moet krijgen.

Normatieve basis

Als normatieve basis voor de inrichting vanen oordelen over de informatieveiligheid geldt een Baseline Informatieveiligheid Richtlijn, per domein gebaseerd op de open standaarden voor informatiebeveiliging ISO 27001 en ISO 27002. Als aan de betreffende baseline is voldaan, zou in principe de informatieveiligheid op orde moeten zijn.

Verankering per organisatie

Elke betrokken organisatie regelt de informatieveiligheid op adequaat niveau, uitgaande van de informatieveiligheidsketen, zowel op het niveau van de primaire processen als van de bedrijfsvoeringsprocessen. Elke betrokken organisatie kent reguliere (jaarlijkse) auditing van de kwaliteit van de informatieveiligheid. De audit-oordelen zijn onderwerp van bestuurlijk en waar aan de orde politiek overleg en leiden tot nadere acties.

Verankering per domein

Op domeinniveau is er een instantie per domein direct belast met de sturing op de ontwikkeling van de informatieveiligheid in het domein en er is een stelsel van afspraken over de aansturing daarvan door koepel en organisaties. Op domeinniveau bestaan afspraken over de te verrichten audits mogelijk mede gebaseerd op zelfevaluaties en peer reviews, en een reguliere (bijvoorbeeld per vier jaar) externe visitatie. In elk geval de uitkomsten van die visitaties zijn onderwerp van dialoog van de betreffende organisatie met de instantie op domeinniveau. De uitkomsten van die dialoog zijn openbaar en kunnen adviezen inhouden aan andere instanties tot actie om de informatieveiligheid te waarborgen.

Een stelsel van single audit is de basis voor deze regulering per organisatie en per domein, zodat de administratieve lasten zo beperkt mogelijk zijn. De ontwikkeling van zo'n stelsel van single audit is een belangrijke stimulerende factoren vindt zo veel als mogelijk plaats.

Verankering op ketenniveau

De informatieketens per domein, over de domeinen heen en ook over de grens van het gehele domein, kennen een coördinerend ketenverantwoordelijke voor informatieveiligheid, gegeven de verantwoordelijkheid voor elke organisatie voor de eigen gegevenshuishouding in het betreffende deel van de keten. De coördinerende taken zijn op hoofdlijnen beschreven in de bijlage 5, maar zullen per keten invulling behoeven. Het streven is deze coördinerende verantwoordelijkheid te beleggen bij de instantie die op stelselniveau verantwoordelijkheid heeft voor de keten.

Verankering op stelselniveau
De verplichtende zelfregulering is gefaciliteerd door op landelijk domeinniveau belegde en daarvoor ingerichte voorzieningen. De minister van BZK is stelselverantwoordelijk en rapporteert over de ontwikkeling van het gehele stelsel van informatiebeveiliging. De inrichting van informatiebeveiliging van het stelsel richt zich op het verminderen van risico's die samenhangen met het gebruik en de continue beschikbaarheid van die informatie Specifieke aandacht daarbij is nodig voor het vergroten van de weerbaarheid en het herstelvermogen van organisaties De taskforce richt zich binnen haar opdracht op niet privacy-aspecten. De minister is daarbij ook verantwoordelijk voor het coördineren van de daarvoor noodzakelijke activiteiten bij landelijke voorzieningen en vergelijkbare initiatieven binnen domeinen. Het streven is daarbij gericht op maximale uitwisseling, afstemmingen hergebruik van het daarvoor benodigde instrumentarium.

Leren

Elke organisatie, nader ondersteund per domein, traint regulier op een actieve gerichtheid van bestuur, management, ICT-functionarissen en andere medewerkers op informatieveiligheid. Deze oefeningen zijn nadrukkelijk bestuurlijk geleid. Dit 'leren' is verankerd in de baseline en verkrijgt aparte aandacht bij auditing en visitatie.

Verandering per organisatie en per domein

Voor elke organisatie en elk domein wordt een probleemanalyse en veranderplan opgesteld die uiteindelijk leiden tot een verplichtende zelfregulering van informatieveiligheid. Op basis van deze probleemanalyses worden systematische implementatietrajecten doorlopen waarvan de voortgang meetbaar is.

3.3 De programmering naar zelfregulering: werkwijze

Op basis van de geformuleerde uitgangspunten tot nu toe dient een programmering tot stand te komen die uiteindelijk leidt tot de beoogde zelfregulering per domein. De werkwijze van die programmering is als volgt:

De domeinen programmeren nadrukkelijk zelf

De programmering is niet 'iets van de taskforce'. De domeinen zelf moeten immers tot die zelf-regulering komen. Wel zal de taskforce met de betrokkene partijen in het domein in overleg treden en zo spoedig mogelijk tot een concrete programmering komen. In de volgende paragraaf is dat nader uitgewerkt.

Uitgangspunt is de lopende ontwikkeling binnen het domein

In alle domeinen lopen ontwikkelingen naar betere informatieveiligheid zoals de ontwikkeling van een baseline informatieveiligheid. De situatie per domein en binnen domeinen is ook verschillend. De programmering zal dan ook domeinspecifiek zijn in drieledige zin.
Ten eerste in de zin van versterking en juist niet van verstoring van lopende ontwikkelingen, zoals in gang gezet vanuit de IBD (gemeenten), ICCIO (Rijk), SIO (provincie), Unie van Waterschappen en Waterschapshuis, CIP en Manifestgroep (ZBO's).Bovendien zijn op stelselniveau diverse partijen actief op het gebied van informatieveiligheid, elk met hun eigen verantwoordelijkheid en doelstelling, zoals Logius (als beheerder van stelselvoorzieningen), NCSC (als Emergency en Responsteam) die met genoemde instanties al programmering ontwikkelen. Het gaat hier vaak om veranderingen met hoge urgentie, zoals antwoorden op bedreigingen en organisatieherstel, die niet kunnen wachten op een meer algemene programmering en ontwikkeling.
Ten tweede zal de programmering domeinspecifiek zijn in de zin van afgestemd op de reeds bereikte situatie van zelfregulering in een domein. Afhankelijk van de wenselijkheid van tweede-orde verandering en tweede orde leren zal ook een bepaalde keuze voor werkvormen aan de orde zijn.
Op de derde plaats zal de programmering domeinspecifiek zijn in de zin van samen met belangrijke netwerken in het domeinen, zoals bij gemeenten met secretarissen (VGS), met hoofden ICT, met CIO-overleg G4. In bijlage 5 is dit samenspel van verschillende partijen bij de ontwikkeling en uitvoering van de programmering nader geschetst.

Doelgroepen en diffusie

Juist bij kwesties als van informatieveiligheid is voorbeeldgedrag van bestuur en (top)management wezenlijk. Zoals Helsloot stelt, geldt voor veiligheidsleren dat de dagelijkse werkpraktijk geen of niet voldoende prikkels bevat die de noodzaak van het leren duidelijk maken, omdat veiligheidsrisico's immers verborgen zijn. In de uitwerking van de leerstrategie zal het dan ook wenselijk zijn te onderscheiden naar verschillende doelgroepen die een verschillende benadering vragen. Hierna is onderscheiden naar de volgende groepen in de verschillende domeinen:

- Bestuur.
- Topmanagement, zoals gemeentesecretaris en directeuren.
- CIO/ICT-top.
- ICT-management en –professionals.
- Medewerkers organisatie in het algemeen.

Een strikt verplichte volgordevoor een effectieve benadering is er niet. Duidelijk is wel dat met name indien bestuur en topmanagement in gedrag en sturing de informatieveiligheid uitdragen, er diffusie van deze gerichtheid in de organisatie (en domein) zal optreden. De taak van de taskforce is meer gericht op benaderen van bestuur en topmanagement, ook daar overigens complementair aan de activiteiten vanuit het domein zelf. Bij de benadering van de andere doelgroepen kan de taskforce op alle mogelijke manieren ondersteunen. Het lijkt dan ook zaak de als eerste drie genoemde groepen in de leerstrategie apart te positioneren, al was het maar in de zin van de andere doelgroepen beïnvloeden.

Taskforce als interbestuurlijke drager voor ontwikkeling naar zelfregulering

De rol van de taskforce is dus complementair aan die van de ontwikkelingen in de domeinen zelf, gegeven een programmering van de domeinen zelf naar zelfregulering. De taskforce zal zich profileren als het interbestuurlijke voertuig (symbool en drager) van die ontwikkeling naar zelfregulering. Die positionering behelst twee rollen.

1. *Hulp bieden bij de ontwikkeling naar zelfregulering*

De taskforce stelt zich tot doel het veiligheidsbewustzijn te bevorderen, met verplichtende zelfregulering als eindbeeld, aanvullend op de initiatieven die door bestaande partijen zijn ontplooid. De taskforce organiseert activiteiten die de betreffende ontwikkeling stimuleren. Het betreft onder andere:

- het afstemmen van activiteiten van deze partijen in de diverse domeinen
- het stimuleren van hergebruik van ontwikkeld materiaal dat zich richt op de bevordering van bewustzijn over informatiemanagement (richtlijnen, formats, trainingen, conferenties, etc.)
- het identificeren van witte vlekken in de ontwikkeling van informatieveiligheid binnen de domeinen en in samenwerking met genoemde partijen in te zetten op invulling daarvan
- het helpen om ontwikkelde producten en systemen voor zelfregulering uiteindelijk te beleggen binnen de bestaande lijnorganisaties
- het waar nodig (doen) ontwikkelen van leer-en verankeringsactiviteiten in aanvulling op en in samenwerking met bestaande organisaties
- het organiseren van congressen; workshops; peer-to-peer-sessies die de ontwikkeling van informatieveiligheid in het overheidsdomein bevorderen
- het stroomlijnen van bestaande normen- en auditstelsels rond informatieveiligheid.

2. *Monitoren, signaleren en dialoog voeren over voortgang*

De tweede rol is dat de taskforce bijdraagt aan het niet-vrijblijvende karakter van de ontwikkeling naar zelfregulering. De taskforce zal na instelling dan ook overleggen met de betreffende instanties over het tot stand komen van een programmering, het monitoren van de voortgang van de ontwikkeling naar zelfregulering en daarover de dialoog te voeren. Na twee jaar dient die ontwikkeling in beeld te zijn (zie volgende paragraaf) en heeft de taskforce daarover een oordeel.

3.4 De programmering naar zelfregulering: inhoud

De uitgangspunten van ontwikkeling naar zelfregulering en van de geschetste werkwijze leiden tot een meer inhoudelijke programmering per domein en over domeinen heen. Als beoogde eindsituatie is geformuleerd dat mede door de taskforce binnen de kaders van haar opdracht na twee jaar een voor de diverse domeinen uitgewerkte systematiek van verplichtende zelfregulering tot stand moet zijn gekomen, dan wel dat er inzicht moet zijn wanneer die (op korte termijn) is bereikt. In termen van eindproducten is dat als volgt te omschrijven.

Eindproducten

- Een aantoonbare verbetering van veiligheidsbewustzijn en handelingsgerichtheid op informatieveiligheid.
- Een geharmoniseerd normenkader gebaseerd op NEN 27001 en 27002.
- De implementatie daarvan binnen de overheid.
- Een werkende en geaccepteerde systematiek om de voortgang van de implementatie te meten en inzichtelijk te maken.
- Een geharmoniseerd maar per domein specifiek ontwikkelde systematiek voor peer reviewing en selfassessments.
- Een per domein geharmoniseerd auditkader.
- Een voor elke organisatie uitgevoerde visitatie gericht op het vaststellen van de verplichtende zelfregulering.
- Een overdrachtsrapportage waarin de bereikte resultaten worden geduid en geaccepteerde voorstellen zijn opgenomen hoe het bereikte resultaat regulier wordt verankerd.

Programmering per domein en over domeinen heen

Zoals gesteld, is deze programmering nadrukkelijk van de domeinen zelf. Na instelling van de taskforce zal prioritair uitwerking van deze programmering plaatsvinden naar concrete activiteiten. Een belangrijke bevinding was dat de aansluiting bij de lopende ontwikkeling het niet mogelijk maakt om in aansluiting op de DigiD-assessments een meer lineaire ontwikkeling uit te zetten van eerste probleemanalyse naar veranderingsstrategie, naar implementatie en naar review en oogsten. Op de eerste plaats moeten, zoals gesteld, de ontwikkelingen met voorrang plaatsvinden die in samenwerking met NCSC en Logius in de domeinen plaatsvinden op het gebied van preventie en

response en herstel. Op de tweede plaats vindt de oplevering van de DigidD-assessments in een zeer verschillend tempo over 2013 plaats, waardoor het meer voor de hand ligt bij 'voorlopers' aan te sluiten en met hen ervaring, materiaal en instrumenten te ontwikkelen waar andere organisaties van kunnen profiteren. En er is ten derde, overigens zoals ook gesteld binnen de overheids-domeinen, al veel gaande op het gebied van de ontwikkeling van informatiebeveiliging, waarbij per domein verschil in situatie aanwezig is en dus ook verschil in programmering. Op departementaal niveau en binnen de deelnemers van de manifestgroep kent het thema adequate aandacht en is met name op het instrumentele vlak al een en ander ontwikkeld. De departementale CIO's hebben opdracht gegeven tot de ontwikkeling en implementatie van een op NEN 27002 gebaseerde richtlijn informatiebeveiliging. Daarbij hoort de ontwikkeling van een monitorsystematiek waarbij de voortgang van de implementatie inzichtelijk wordt. Hergebruik van dergelijke systematieken die op dit moment ook bij KING worden gebruikt bij bijvoorbeeld Operatie NUP is een interessante optie.

De aandacht voor informatiemanagement en beveiliging in de bestuurs- en gebruikskolom is voor verbetering vatbaar. De taskforce ziet mogelijkheden om in samenwerking met ABD CAP en CIP opleidings-, trainings- en oefenmateriaal te ontwikkelen dat erop gericht is het beveiligings-bewustzijn te verbeteren. De taskforce kan bijdragen aan de organisatie van passende activiteiten zoals conferenties en learn and share-bijeenkomsten. Hergebruik van dit materiaal bij mede-overheden ligt vervolgens voor de hand. Ook bij de provincie (SIO) is opleiding op het terrein van informatiebeveiliging ontwikkeld die breder bruikbaar kan zijn.

De taskforce kan een aanzienlijke bijdrage leveren aan het harmoniseren van het auditkader, gebaseerd op de ontwikkelde norm voor informatiebeveiliging. Dit vraagt echter om stevige betrokkenheid van ICCIO, stelsel- en domeinpartijen, departementale auditdienst en beroeps-organisaties.

Tot slot kan de taskforce een stimulans geven aan interdepartementale peer review en de ontwikkeling van daarvoor benodigde instrumenten voor uitvoering van selfevaluaties.

Het gemeentelijk, provinciaal en waterschapsdomein zijn doende met de ontwikkeling van een op het domein gericht informatiebeveiligingsbeleid. Dit beleid vraagt echter nog om een langer ontwikkelings-en implementatietraject. Zeker binnen het gemeentelijke domein vormt deze implementatie een uitdaging, gegeven het grote aantal gemeenten.

De inzet van de taskforce daar is erop gericht die implementatie te ondersteunen door de ondersteuning van relevante communicatietrajecten met name ook richting bestuur, topmanagement en CIO/CISO. Daarnaast stimuleert de taskforce de ontwikkelingen het beschikbaar stellen van opleidings-, trainings- en oefenmateriaal. De programmering richt zicht vervolgens op de ontwikkeling van monitoringinstrumenten; harmonisatie van auditkader; ontwikkeling en introductie van systematieken van bijvoorbeeld peer reviews en zelfevaluaties. De vereiste veranderstrategie en implementatie van instrumentarium zal aandacht krijgen met als een mogelijk startpunt het beschikbaar komen van het de resultaten van de DigiD-assesment voor een of groepen van organisaties. Gezocht wordt naar voorlopers die een good practice kunnen vormen. Bij het ontwikkelen van deze systematieken maakt de taskforce waar mogelijk gebruik van ontwikkeld materiaal binnen departementen en CIP. Deze domeinen kunnen op hun beurt weer gebruikmaken van de ervaring bij implementaties in gemeenten, provincies en waterschappen zoals die inmiddels tot stand komen en de komende twee jaar veel materiaal zullen opleveren. Het identificeren van de mogelijkheden voor hergebruik en het daadwerkelijk stimuleren daarvan zijn belangrijke onderdelen van de taak van de taskforce.

In bijlage 5 zijn deze programmering en de bijdrage daaraan van de taskforce uitgewerkt als een eerste bod. Met de Programmaraad is daar een eerste overleg over geweest. Op basis van dit eerste bod zal nog in december na instelling van de taskforce prioritair uitwerking plaatsvinden in overleg naar een activiteitenprogramma.

Uit deze programmering en het gevoerde overleg blijkt daarnaast dat een aantal onderwerpen met voorrang aandacht verdient, waarin de taskforce een rol zou kunnen vervullen:

- Het organiseren van de informatieveiligheid voor ketens.
- Het organiseren van informatieveiligheid in relatie tot opdrachtnemende partijen. Op veel informationele relaties heeft uitbesteding plaatsgevonden en voeren de overheidsorganisaties vooral regie.

Het ontwikkelen van nadere programmering op deze punten kan na instelling met prioriteit opgepakt worden.

3.5 Overige programmering

Accountmanagement

Per organisatie en domein gaat het om meer of minder ingrijpende veranderingen naar zelf-regulering. Per organisatie en domein zal het benodigde leren en verankeren dus uiteenlopen. Accountmanagement zal erop gericht moeten zijn uiteindelijk per organisatie door (leer)acties toteen adequate verankering te stimuleren. Het accountmanagement zal een stevige positie in de taskforce verkrijgen.

Accounts betreffen:

- overheidsorganisaties[2]
- faciliterende en sturende organisaties op stelselniveau (IBD; CIP; NCSC; LOGIUS)
- belangenorganisaties (VNG, IPO, UWV, ICCIO)
- kennisorganisaties (Universiteiten, TNO)
- beroepsorganisaties (NIvRA; NOREA)

De verwachting is dat binnen onder meer het gemeentelijk domein door de verscheidenheid accountmanagement veel vernuft zal vragen, zoals hiervoor al aangegeven met het onderscheid naar voorlopers. Uiteraard zal ook hier de taskforce in nauwe samenwerking opereren vanuit de complementaire rol met de belangenorganisaties bij het ontwikkelen van een relevante programmering.

Communicatiestrategie

Voor het realiseren van de doelstellingen van de taskforce is een daarop gerichte communicatiestrategie een belangrijke randvoorwaarde. Deze strategie zal zich enerzijds moeten richten op de ondersteuning van het bewustwordingsproces in de relevante netwerken en bij bestuurders. Anderzijds zal zij belangrijk zijn bij het steeds op adequate momenten communiceren over bereikte resultaten.

De aandacht is nu gericht op:

- een adequaat 'statement' als start van de taskforce, te onderschrijven interbestuurlijk uiterlijk 1 februari
- een gerichte benadering van de organisaties binnen de verschillende domeinen met een overtuigende argumentatie over het traject naar verplichtende zelfregulering en de rol van de verschillende partijen daarin; die communicatie moet verlopen via de koepels. De taskforce faciliteert deze benadering van organisaties via de koepels. ondersteuning van de inrichting van communicatiekanalen binnen en buiten taskforce, zoals een website.

---

[2] Departementen, ZBO's, Provincies, Waterschappen en Gemeenten

3.6 Coördineren

Te verwachten is dat rond de vraag naar zelfregulering een aantal coördinatievragen zal rijzen waar de taskforce een zinvolle rol kan spelen. Het is een dringende wens van de betrokken partijen om de taskforce die coördinatie te laten bevorderen. Deze start met de completering van het beeld van lopende ontwikkelingen overheidsbreed.

3.7 Onderzoeken en monitoren

Onderzoeken

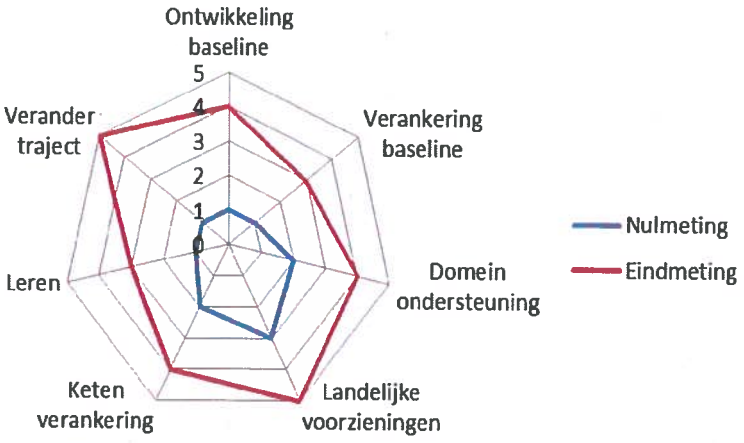
De taskforce heeft in haar opdracht een specifieke onderzoekstaak. Bij de programmering onderkennen we op dit moment de volgende specifieke onderzoeksactiviteiten. Het betreft:

- Inventarisatie relevante ontwikkelingen rond informatieveiligheid.
- Bezien of ontwikkeling van nadere wet- en regelgeving noodzakelijk is.
- Ketenonderzoek, met als startpunt het lopende onderzoek naar de Suwiketen

De verwachting is dat bij het nader uitwerken van de agenda aanvullende onderzoeksvoorstellen worden geformuleerd.

Meten en monitoren

De taskforce ontwikkelt een methodiek waarmee de voortgang van de verplichtende zelfregulering gemeten en gemonitord kan worden. Op basis van de zeven in deze notitie geformuleerde kaders voor die ontwikkeling zou een dergelijk meetinstrument als volgt vorm kunnen krijgen. Resultaten van die meting worden dan zowel op organisatie- als domeinniveau inzichtelijk.



De betreffende meting kan een plaats krijgen in de te ontwikkelen systematiek voor audits, peer reviews, zelfevaluaties en externe visitaties. Bij King is ervaring opgedaan met het ontwikkelen van een dergelijk meetinstrumentarium, zowel vanuit benchmarking perspectief als bij het meten van de voortgang van Operatie Nup. Het ligt in de rede om bij de ontwikkeling van dit instrumentarium de ervaring van KING te betrekken.

3.8 Uitwerking programmering

Per domein is het eerste bod uiteenlopend; zie daarvoor uitdrukkelijk bijlage 5. Een grove gemeenschappelijke noemer is als volgt te schetsen.

1. Uitwerking verplichtende zelfregulering;
   - het streven is die uitwerking nog vóór de volgende BRG E-overheid en dienstverlening gereed te doen zijn en voor zover nodig in het statement van de BRG van februari te verwerken. Punten die daarin onder meer aan de orde moeten komen zijn de volgende.
     - Aparte aandacht zal het streven naar zoveel mogelijk single audit krijgen; dit zal nader verankerd moeten worden in interbestuurlijke afspraken
     - Een ander belangrijk punt is de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.
   - De taskforce kan vanaf januari de dialoog bevorderen over de vormgeving aan zelfregulering. De taskforce zou bijvoorbeeld samen met de VNG met name ook bestuurders en raadsleden kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie en de rol van de raden daarin benadrukken, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten. Deze bijeenkomsten kunnen eerst gekoppeld zijn aan de hieronder benoemde kennis- en bewustwordingssessies, maar op dit terrein zal de gehele twee jaar organiseren van dialoog plaats vinden.

2. De voortgaande programmering per domein naar activiteitenprogramma is zoals gezegd zeer uiteenlopend; een grove gemeenschappelijke noemer van de bijdrage van de taskforce daaraan gedurende het volgende kwartaal is de volgende.
   - In beeld brengen van voorlopers DigiD-assessment en starten van nadere trajecten met groepen daarvan. De taskforce kan bijvoorbeeld gemeenten behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de Baseline Informatie Gemeenten en het koppelen aan de uitkomsten van de DigiD assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learn and share' overleg met gemeenten die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieén en implementatie. In januari zullen de eerste bijeenkomsten met voorlopers plaats vinden, met conclusies in februari/ maart hoe het traject voort te zetten
   - De programmering van bewustwordings- en kennissessies meer algemeen voor bestuur en topmanagement voor zover nog nodig vanaf januari/februari; in het verlengde daarvan

interessante activiteiten als excursies naar interessante sectoren/bedrijven met gerichte uitnodigingen aan bestuurders en top management
- Het proces van ontwikkeling van de BIG faciliteren en daardoor versnellen; in ieder geval rond de baseline informatiebeveiliging eind januari/beginfebruari gerichte bijeenkomsten of en andersoortige communicatie organiseren
- Een start met het ondersteunen van het stroomlijnen van het raamwerk van respectievelijk self-assessments; peer reviews, externe auditinstrumenten. Een inventarisatie in het eerste kwartaal, nadrukkelijk verbonden ook met het uit te zetten traject rond het streven naar singel audit
- Het ontwikkelen van voor het domein relevante handleidingen; instructies; oefenmateriaal etc. Steeds in nauwe samenhang met de concrete situatie in het betreffende domein. In het eerste kwartaal zal inventarisatie van bestaande opleidingen plaats vinden, zal overleg plaats vinden met bestaande aanbieders en voorstellen ontwikkeld zijn voor uit te voeren cursussen/opleidingen vanaf het tweede kwartaal
- Het experiment met een digivaardigheidsbewijs verder ondersteunen en over de verschillende domeinen helpen verspreiden.
-

3. De taskforce zal met spoed op een aantal ketens een initiatief nemen met betrokken partijen over hoe de regulering van de informatieveiligheid in te richten. In ieder geval op het terrein van identiteit, veiligheid justitieel, decentralisaties waaronder Suwi, enige ketens in de zorg. Het rijk zal hier mede een trekkende rol moeten vervullen.

4. De taskforce start het eerste kwartaal met het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein.

5. Communicatie met het veld uitwerken. In ieder geval zullen de relevante besturen een brief met adequate toelichting ontvangen; te overwegen is een zeer goede brochure als bijlage met het vraagstuk van informatieveiligheid nog eens goed neerzetten

6. Overzicht lopende ontwikkelingen informatieveiligheid overheidsbreed. Dit zal in het eerste kwartaal gereed zijn

7. Ontwikkeling van meet- en monitoringinstrumenten om de voortgang in leren en verankeren te kunnen meten. .Een ontwerp gereed in het eerste kwartaal

8. Starten geïdentificeerde onderzoeken.

Dat resulteert in de volgende globale planning als basis voor de activiteiten vanaf januari. De onderstaande planning is indicatief en vraagt nadrukkelijk nadere uitwerking in de komende weken per domein.

Weeknummer	1	2	3	4	5	6	7	8	9	10	11	12	13
Uitwerking verplichtende zelfregulering.													
• ontwikkelen statement													
• formuleren uitgangspunten single audit													
• formuleren uitgangspunten visitatie													
Programmering per domein naar activiteitenprogramma.													
• In beeld brengen van voorlopers DigiD-asesssment en starten van nadere trajecten met groepen daarvan.													
• organisatie bewustwordingssessies													
• steunen ontwikkeling BIG													
• formuleren uitgangspunten self-assessment, peerreview en monitoring													
• ontwikkelen handreikingen													
• formuleren opleidingsuitgangspunten													
• verspreiding digivaardigheidsinitiatief													
Informatieveiligheid keten oppakken voor aantal belangrijke ketens.													
Informatieveiligheid opdrachtnemende partijen als vraagstuk in beeld brengen.													
Communicatie met veld uitwerken.													
Overzicht lopende ontwikkelingen informatieveiligheid overheidsbreed.													
Ontwikkeling van meet- en monitoringinstrumenten.													
Starten geïdentificeerde onderzoeken													

Een globale planning over de gehele twee jaar moet uitmonden in de realisatie van de genoemde eindproducten. Een zinvolle opstelling daarvan eist een nader overleg per domein. De nu onderscheiden activiteiten zulle over die twee jaar in nader te concretiseren vorm en fasering zeker voortzetting behoeven.

4. Governance en organisatie van de taskforce

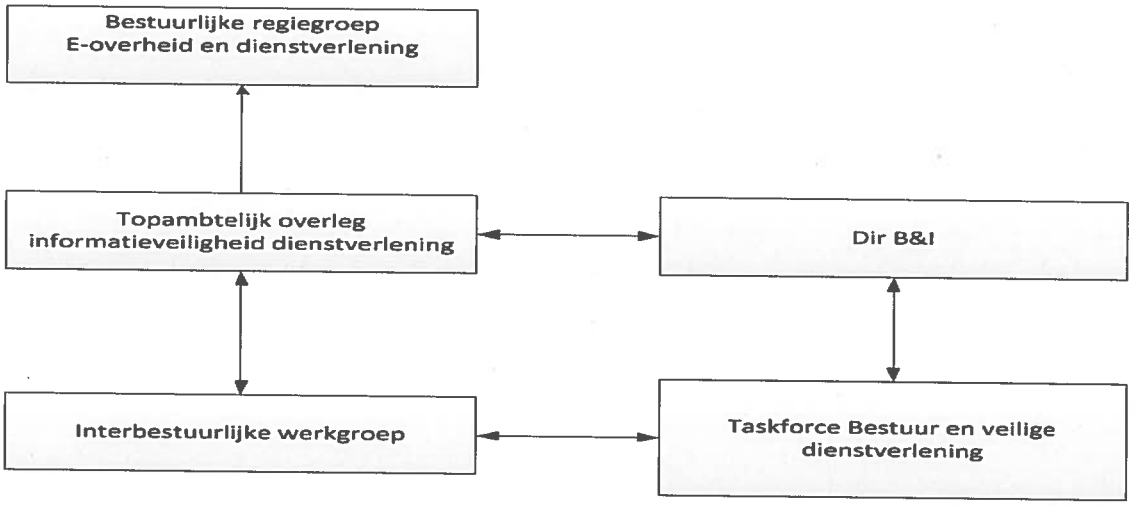
In bijlage 6 is de organisatie verder uitgewerkt in wat de vorm moet krijgen van een handzaam handboek organisatie.

4.1 Governance

De voorstellen voor sturing en organisatie zijn gebaseerd op de volgende uitgangspunten:

- Het huidige stelsel van bevoegdheden en verantwoordelijkheden rond informatieveiligheid is uitgangspunt.
- Elke overheidsorganisatie blijft zelf verantwoordelijk voor realisatie eigen informatieveiligheid.
- Coördinatie op bestaande initiatieven is een noodzaak om overheidsbrede informatieveiligheid te verbeteren.
- De taskforce kent een interbestuurlijke aanpak; collegiaal en in vertrouwen.
- De taskforce wordt klein en wendbaar opgezet zodanig dat zij in een netwerk van organisaties stimulerend werkt.
- De governance van de taskforce sluit aan de bestaande BRG E-overheid en dienstverlening.

Uit de gesprekken blijkt een tweeledige behoefte. Ten eerste geen aparte nieuwe overlegstructuren en ten tweede geconcentreerde, aparte aandacht voor het vraagstuk van informatieveiligheid met de mogelijkheid tot interbestuurlijke coördinatie, gegeven de verantwoordelijkheid van de verschillende betrokken organisaties. Het voorstel is om de daarmee samenhangende governance als volgt vorm te geven.



De BRG E-overheid en Dienstverlening is een goed forum voor overleg en coördinatie van informatieveiligheid. Vanuit V en J is aangegeven dat een dergelijke afstemming gewenst is en V en J kan aan de regiegroep deelnemen. Voor een snelle en krachtige besluitvorming in het netwerk van de geschetste vierhoek is een topambtelijk overleg van de vijf domeinen gewenst. De directie B&I van BZK is met name ook opgenomen vanwege de taak inzake stelselverantwoordelijkheid en coördinatie. De programmaraad 'Follow-up DigiNotar' vindt een opvolger in de interbestuurlijke werkgroep 'Informatieveiligheid dienstverlening'.

Invulling per domein

DG BO (dir. B en I) stuurt op de voortgang van het geheel. Deze stelselverantwoordelijkheid laat de specifieke verantwoordelijkheid van rijkspartijen op specifieke terreinen onverlet (NCSC, OPTA enz.)

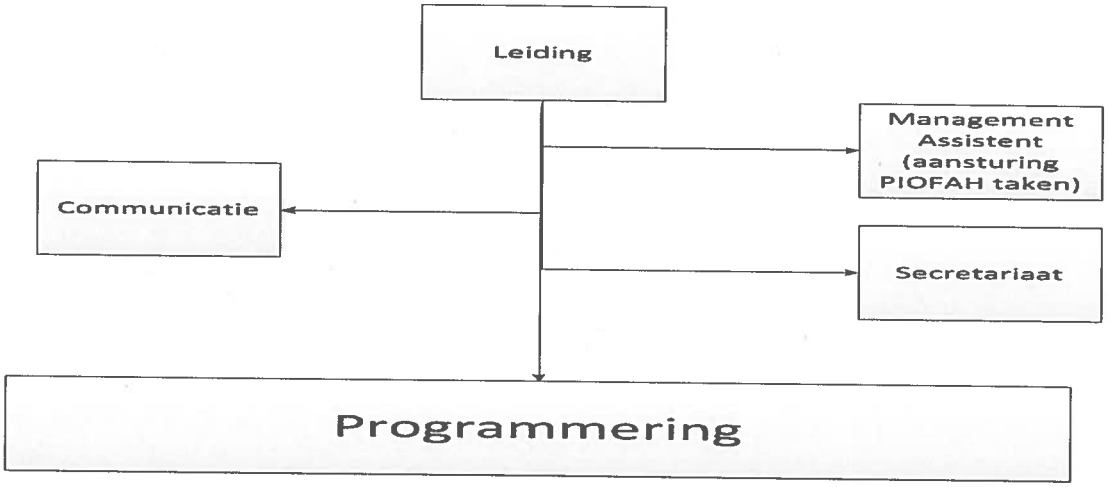
Per domein zullen op de voortgang aanspreekbare partijen aanwezig moeten zijn op de voortgang van de programmering. Steeds is daarbij te onderscheiden naar de bestuurlijk eerstverantwoordelijke en de meer uitvoerend verantwoordelijke.

- Rijk: DG BRO en ICCIO
- Gemeenten: VNG en IBD
- Provincies: IPO en Overleg directeuren bedrijfsvoering met ICT strategisch overleg
- Waterschappen: UVW en Waterschapshuis
- ZBO: in overleg met Rijk, de Manifestgroep en CIF
- Speciale verantwoordelijkheden zullen voortkomen uit de ketenprogrammering

4.2 Leiding en organisatie

De leiding behoeft een tweeledige set van competenties dat lastig te verenigen is. Ten eerste toegang hebben tot bestuurlijk en topmanagerial arena's en mede vanuit de resultaten van het overleg daarin aansturen van de taskforce. Ten tweede een creatieve, hoogwaardige vormgeving aan de programmering en het 'hands on' dagelijks leiding geven daaraan. Het advies is de leiding in te richten door aanstelling van een eindverantwoordelijk interbestuurlijk ervaren manager/ ex-bestuurder, die met gemiddeld 0,4 fte wel 'echt' leiding geeft aan de taskforce .In die taak wordt hij ondersteund door een dagelijks programmanager voor 0,8 fte.

De taskforce is een eenheid van beperkte omvang, gepositioneerd binnen ICTU. De PIOFAH-taken verzorgt ICTU conform een programmaovereenkomst. Hiërarchische aansturing geschiedt door de directeur B&I.



In de taskforce zijn kennis en vaardigheden aanwezig inzake communicatie, informatieveiligheid, leerprocessen, organisatie en sturing (verankering) en kennisprocessen. Uiteraard is er ondersteuning, gericht op een krachtige programmering.

Taskforce opzet	Fte	**Schaal**
Leiding	1,2	
Directeur	0,4	contract
Programmamanager	0,8	15
Ondersteuning	**2**	
Secretaresse	1	6
Communicatiemedewerker	1	12
Programmering	**7**	
Beleidsmederwerker Leren	1	13
Beleidsmedewerker Verankeren	1	12
Beleidsmedewerker informatieveiligheid	1	13
Beleidsmedewerker onderzoek/monitoren	1	12
Junior beleidsmedewerkers	3	10/11
Totaal formatie	**10,2**	

Het streven is de formatie mede in te vullen met medewerkers vanuit de andere overheden. Een zogenaamde romptaskforce waarmee het mogelijk is de werkzaamheden te starten, bestaat in elk geval uit de leiding, ondersteuning, een overeenkomst met ICTU en twee beleidsmedewerkers.

5. Begroting

De voorlopige opbouw van de begroting op hoofdlijnen van 2013 en 2024 is als volgt.

Formatie	€ 1.000
Inkoop PIOFAH-taken	€461
Programmering	€3.539

Het spreekt voor zich dat deze uiterst summiere begroting binnen de bovenstaande budgettaire kaders nader wordt gedetailleerd.

Naar verwachting zal voor 2014 eenzelfde bedrag voor de taskforce ter beschikking staan.

Bijlage 1. Geheel van acties

Verantwoordelijkheid van de minister van Binnenlandse Zaken

De minister van Binnenlandse Zaken is stelselverantwoordelijk voor een veilige informatie-uitwisseling tussen overheden en overheid en burger. Informatiebeveiliging van overheidsinformatie is een wezenlijk onderdeel van de bestuurlijke verantwoordelijkheid in de huidige samenleving. Het NCSC heeft geconstateerd dat de response op ICT-crisis onvoldoende georganiseerd is, ook bij de overheden en hun organisaties. Dit betekent dat de minister van Binnenlandse Zaken zorg moet dragen dat de overheden en hun organisaties bestuurlijk hun verantwoordelijkheid pakken op minimaal twee concrete gebieden:

- Het aansluiten op de crisisorganisatie op ICT-gebied die nu wordt opgebouwd met het NCSC.
- Het creëren van herstel- en weerbaarheidsvermogen van hun organisaties en de ketens waar zij in werken.

De bestuurders zijn verantwoordelijk voor een kwalitatief hoge, efficiënte, effectieve, betrouwbare en veilige dienstverlening.

De zwaardere eisen die aan de rol van de minister van Binnenlandse Zaken worden gesteld en de daarmee reeds gedane en voorgenomen toezeggingen, vragen echter ook om meer beleidsmatige inzet op:

- het ontwikkelen en uitrollen van de CIO-regiefunctie in de richting van alle overheden, inclusief het vormgeven van de bijbehorende institutionele afspraken
- het versterken van het PKI-stelsel (voor de gehele overheid)
- het nader vormgeven aan de toezichtrol op PKI- en DigiD-stelsel in relatie tot algemene (nieuwe) veiligheidsaspecten
- het verder (doen) uitvoeren en monitoren van de DigiD-assessments en de opvolging van de aanbevelingen voor alle DigiD-gebruikers
- het invulling geven aan de kritische noties rondom de ketenrelatie van een aantal overheids-brede basisvoorzieningen (basisregistraties, stelselvoorzieningen, DigiD, PKI, INUP-voorzieningen, Digipoort,etc.)
- het ontwikkelen en uitvoeren van beleid rondom de informatiepositie van de burger zelf in relatie tot sterker beveiligde dienstverlening en (nieuwe zienswijzen op) de bijbehorende privacy-vraagstukken: onderzoeken waar de grenzen liggen van de verschillende verantwoordelijkheden
- het in gang zetten en uitwerken van wetgeving en/of beleidskaders en convenanten om ook in de toekomst veilige én effectieve ICT-dienstverlening te borgen.

Het afgelopen jaar is door de Programmaraad Follow-up DigiNotar veel in gang gezet en ook geregeld. Maar ook is aangegeven op welke punten verdere actie nodig is vanuit de opdracht van de stuurgroep; het betreft:

- de positionering van CSP's in relatie tot definitie vitale sectoren (naar B&I, PKI)
- het vraagstuk van de doorwerking van calamiteiten in ketens(op basis van Suwi-ketenonderzoek komen tot de inrichting van een generiek model voor informatiebeveiliging op het niveau van ketens, nagaan of er aanknopingspunten zijn voor een toetsingskader voor ketenbrede audits).

Belangrijk is dat elke speler zijn rol pakt vanuit de verantwoordelijkheid die hij heeft. Er is op dit moment een samenspel van drie posities. Deze drie posities zijn ten eerste de rollen en verantwoordelijkheden van de organisaties/overheden, ten tweede de Programmaraad Follow-up DigiNotar en ten derde de op te richten interbestuurlijke taskforce.

Bijlage 2. Stelselverantwoordelijkheden spelers

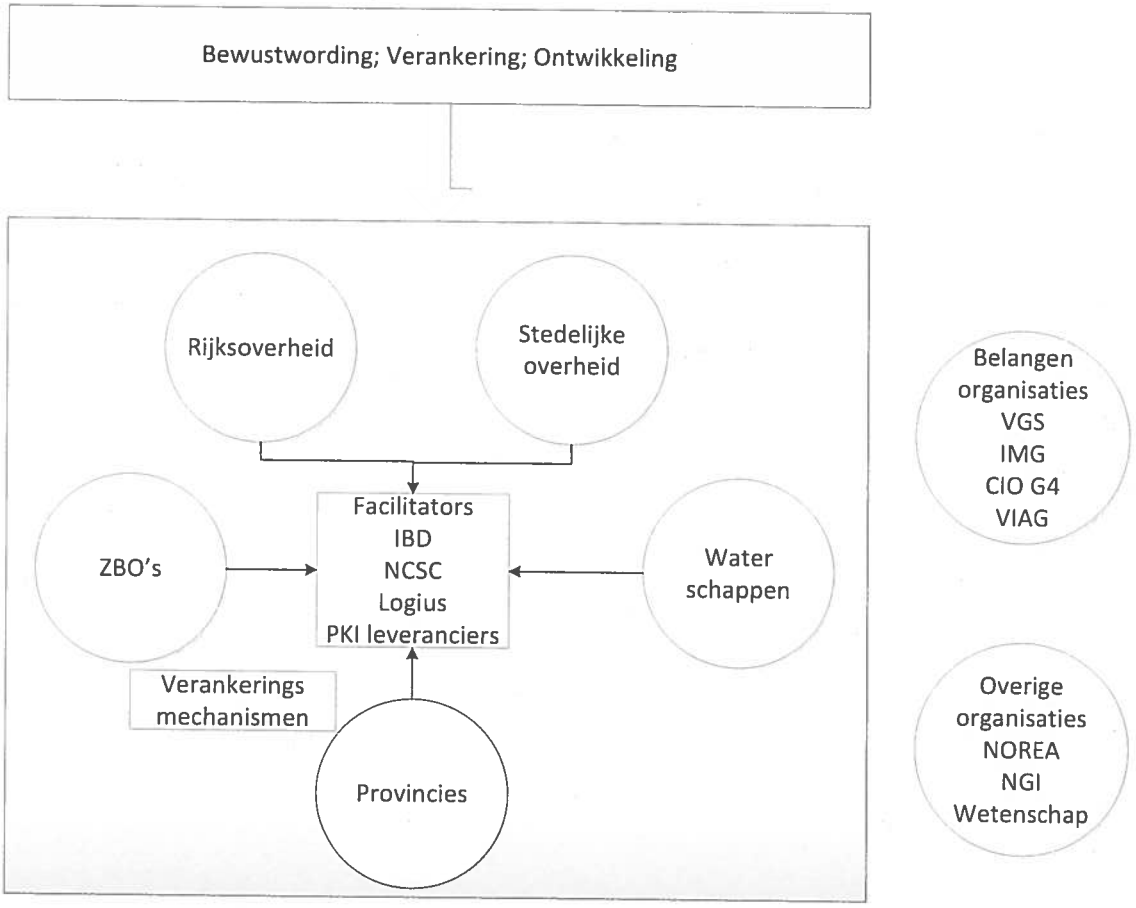
Overheden met eigen democratische verantwoordingsorganen:

- Rijk - Tweede Kamer (DG OBR ten aanzien van sector en DG BKten aanzien van systeemverantwoordelijkheid).
- Gemeente – Gemeenteraad.
- Provincie – Provinciale Staten.
- Waterschappen – Algemeen Bestuur Waterschappen.
- Manifestgroep – via Rijk Rijk (verschillende departementen, bijv. RDW via I&M, UWV en SVB via SZW, DUO via OCW / / Tweede Kamer.

Overige spelers in het veld:

- Logius.
- NCSC.
- VNG
- IPO
- UvW
- MFG
- CIP
- KING.
- Informatiebeveiligingsdienst.
- Waterschaphuis.
- IPO.
- Andere ministeries V&J, ELI.
- OPTA.
- Leveranciers.
- CSP
- NOREA
- NCSC

De weergave van het huidige veld



De figuur is niet uitputtend. Zo is NCSC is niet alleen facilitator, maar het is wel één van de rollen (naast coördinator en actor). In dit geval facilitator/organisator van kennis- en (tooling voor) bewustwordingsactiviteiten.

Bijlage 3. Reactie OVV-rapport (apart bijgevoegd)

Bijlage 4.Lijst gesprekspartners

Waterschappen

[redacted]

Provincie

[redacted]

Gemeenten

[redacted]

ZBO

[redacted]

[redacted]

Rijk

[redacted]

Medewerkers directie B en I

Stelsel

[redacted]

[redacted]V en J)

Medewerkers NCSC (V en J)

Wetenschap en deskundigen

[redacted]

Bijlage 5. Leerstrategie, zelfregulering, programmering

1. Leerstrategie van verankeren

In afstemming met experts op het terrein van leerstrategie en risicobewustzijn is een globale leerstrategie opgesteld die tot nadere programmering in de verschillende domeinen zal leiden. De belangrijkste basis daarvoor is de bijgevoegde notie van Ira Helsoot.

Risico's, informatiebeveiliging en veiligheidsbewustzijn

Informatieveiligheid wordt wel omschreven als de bescherming van informatie en informatiestromen tegen bedreigingen, die de continuïteit van de dienstverlening kunnen verstoren, schade kunnen veroorzaken en de goede werking kunnen verhinderen. De volgende accenten zijn daarbij van belang.

De geformuleerde bedreigingen duiden op de eerste plaats op aanzienlijke persoonlijke, maatschappelijke en politieke risico's ten gevolge van onvoldoende beveiliging.

De risico's zijn niet uit te bannen; het gaat om omgang met deze risico's en om lastige afwegingen van kosten en baten veiligheid, openbaarheid en privacy. Classificatie van soorten informatie naar aard en ernst van de risico's is een wezenlijk onderdeel van

Het besef van en inzicht in deze complexe aard van risico's en informatieveiligheid moet voorop staan bij een leerstrategie inzake informatieveiligheid. De relevantie van het onderwerp is bijna niet te overschatten en de omgang er mee moet het karakter hebben van afwegingen van risico's en daarop toegespitst beleid.

De technische complexiteit van informatieveiligheid die tot de bijna natuurlijke reflex leidt deze veiligheid vergaand aan de technici over te laten, is dan ook een van de meest grote bedreigingen van het leerproces zelf.

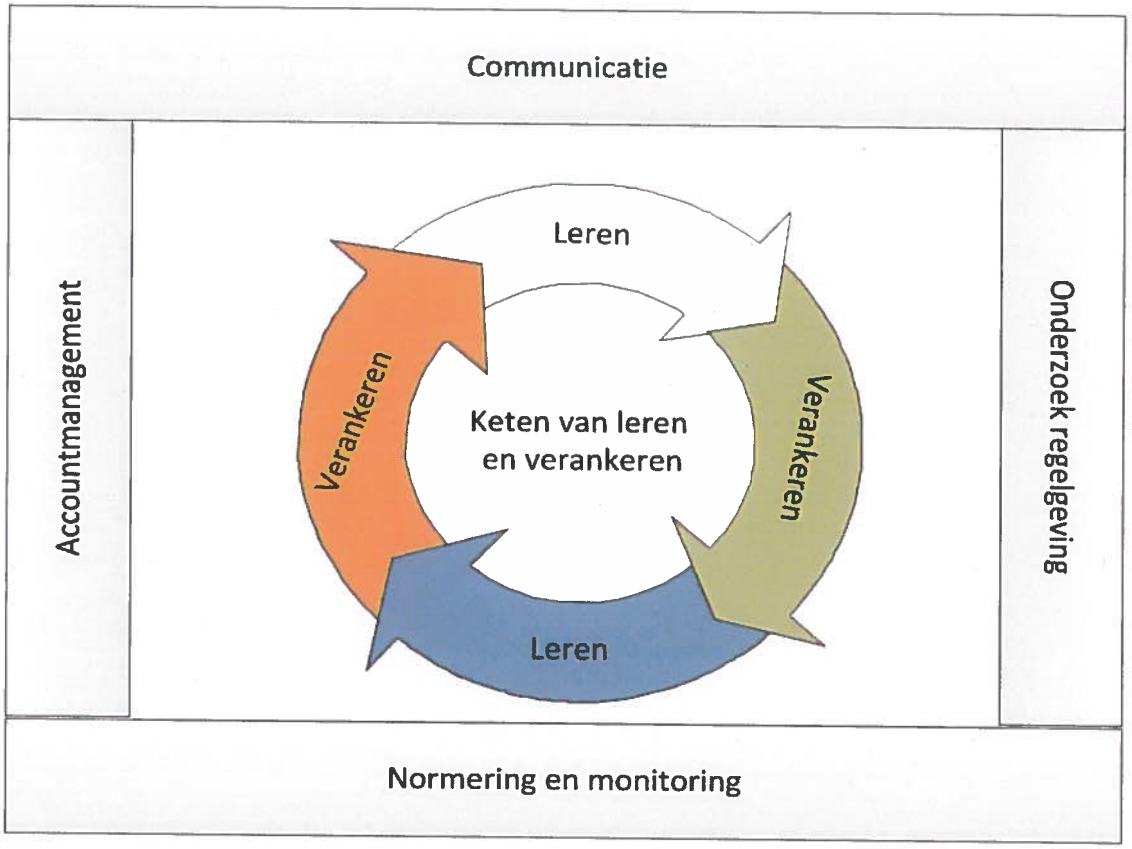
Ira Helsloot stelt het volgende:

> *"In algemene zin is uniek voor 'veiligheidsleren' dat de dagelijkse werkpraktijk geen of niet voldoende prikkels bevat die de noodzaak van het leren duidelijk maken. Veiligheidsrisico's zijn immers verborgen. Voorschriften leveren wel een bijdrage aan de veiligheid, maar kunnen (zeker op de langere termijn) niet waarborgen dat er geen onveilige situaties ontstaan. Veiligheid start met het te onderhouden besef welke risico's en gevaren er zijn, het zien en onderkennen hoe gevaarlijke situaties kunnen ontstaan, welke omstandigheden niet gewenste ontwikkelingen beïnvloeden en hoe moet worden opgetreden om de gewenste condities te kunnen beheersen. Criminelen zijn slim, de informatieveiligheid moet nog slimmer zijn. Veiligheid impliceert daarmee kennis en inzicht in de aanwezige omstandigheden en het vermogen om zelfstandig en adequaat in deze omgeving te kunnen ingrijpen. Voorschriften en instructies als zodanig kunnen en doen dat niet. Ze kunnen er wel voor zorgen dat iemand begrijpt en zich er bewust van is (of wordt) welke handelingen in bepaalde omstandigheden noodzakelijk zijn om een gewenste veilige situatie te bereiken. Het bewustzijn van risico's en*

gevaren en het begrijpen van de maatregelen waarmee een gewenste situatie kan worden gerealiseerd, zijn de basisvoorwaarden voor een adequate inrichting van een veilige omgeving. Uiteraard moet uiteindelijk een en ander gedocumenteerd worden in handleidingen en richtlijnen (...)

Leren en verankeren in de veiligheidsketen

De in hoge mate op de notitie van Helsloot gebaseerde hieronder weergegeven leercyclus omvat in feite een voortgaand proces van leren in wisselwerking met verankeren in de organisatie en institutionalisering daarvan. Dat is in onderstaande figuur weergegeven. De aspecten van monitoring, onderzoek, communicatie en accountmanagement komen hierna aan de orde.



Informatieveiligheidsketen als uitgangspunt leren en verankeren

Het gaat om leren in de veiligheidsketen, hetgeen specifieke eisen stelt. Inhoudelijk stellen wij daarom voor om in welke leerstrategie ook gekozen wordt de veiligheidsketen centraal te stellen.In het veiligheidsmanagement gaat het, als bij alle management, om een proces van besluitvorming, sturen en regelen gericht op het bereiken van de geformuleerde veiligheidsdoelstellingen. Kern van

die aanpak is voor informatieveiligheid is dat prognoses worden gemaakt van de verwachte dreigingsontwikkelingen in de omgeving en dat op basis van scenarioanalyses handelingsperspectieven worden ontworpen om situaties en omstandigheden te kunnen beheersen.'

De leerketen is dus te richten op vijf stappen informatieveiligheidsketen

- Pro-actie: vaststellen van het beleids- en uitvoeringskader;
- Preventie: risicoanalyse en realiseren van adequate beveiligingsmaatregelen;
- Preparatie: (planmatig) opbouwen van weerbaarheid tegen kwetsbaarheden informatieveiligheid;
- Respons: alertheid en vermogen snel en adequaat op kwetsbaarheden en incidenten te kunnen reageren;
- Nazorg en herstel: informatiefunctie kunnen herstellen.

Van belang is dat de evaluatie en het toezicht op de uitvoering van de veiligheidsketen per organisatie en per domein apart aandacht behoeft.

Eerste en tweede orde

Leren en verankeren zullen zich dus in wisselwerking ontwikkelen met toenemende aandacht voor verankering. De vraag is hoe de opbouw naar zo'n situatie kan plaats vinden. Die opbouw is sterk afhankelijk van de specifieke situatie per domein en per organisatie en met name ook of er sprake moet zijn van tweede orde verandering en bijbehorend leren. Bij tweede orde treedt een aantal structurele veranderingen in gerichtheid en gedrag op en verankering daarvan in structuren en werkprocessen. Tweede orde eist dus een andere leerstrategie als eerste orde verandering zoals in onderstaande tabel van Helsloot illustratief is weergegeven.

Helsloot stelt het volgende.

> *'De taskforce dient derhalve ten behoeve van tweede orde leren als eerste in te zetten op het ontdekken en activeren van dit basisbesef en verdiepend inzicht. Niet op het aanleren van richtlijnen voor bestuurlijk handelen dus, maar wel op een confrontatie met omgevingen waarin risico's en gevaren zich manifesteren en waarin bestuurders keuzes moeten maken welke oplossingen een bijdrage leveren aan de doelstellingen die zij voor het eigen veiligheidsbeleid hebben geformuleerd. Simpele problemen en oplossingen staan niet op het menu. Om de waakzaamheid en weerbaarheid voor risico's en gevaren te vergroten dient de doelgroep als eerste geconfronteerd te worden met complexe en unieke situaties, waarin meerde oplossingsperspectieven mogelijk zijn. In discussies en debatten moet vervolgens een dieper inzicht in de informatieveiligheidsproblematiek worden verkregen, bepalen analyses de oplossingsrichtingen, moeten besluiten worden gemotiveerd en maatregelen worden verdedigd. In een tijd dat de cybercriminaliteit zich sterker dan ooit ontwikkelt moet de bestuurder het debat aan hoe zijn organisatie adequaat weerstand tegen deze ontwikkelingen kan en moet bieden.*

Het verwijzen naar voorschriften zal daarbij niet in alle omstandigheden de meest passende oplossing zijn. Er zal meer moeten gebeuren.'

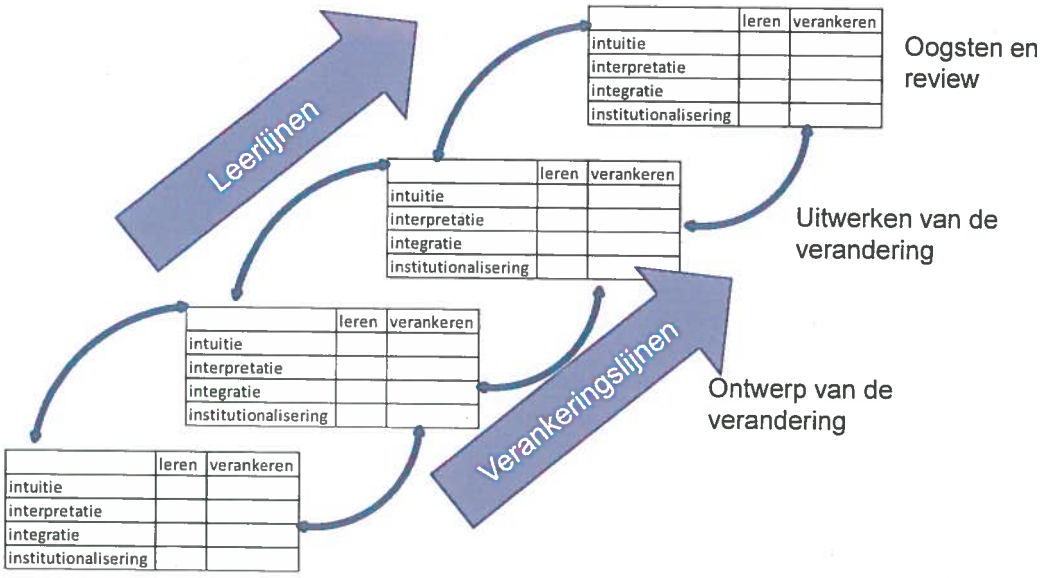
Uit de analyse van Helsloot wordt duidelijk dat met name als er sprake is van tweede orde verandering toewerken van breed leren naar verankeren een goede strategie kan zijn. Het eindpunt van deze strategie kan in alle gevallen, dus ook bij eerste orde leren, een visitatie zijn. We verbeelden deze onderlinge wisselwerking in onderstaande figuur.

Volgorde: van probleemanalyse naar oogsten

De notitie van Helsloot bevat een nadere fasering die van nadruk op bewustwording en verkrijgen van kennis en inzicht naar steeds meer nadruk op verankering in organisatie en bestel verloopt. Deze fasering is vertaald naar een fasering van probleemanalyse, ontwerp verandering, implementatie verandering en oogsten en reviewen. Van belang is dat ten eerste reeds in iedere fase leren en verankering in samenhang geïmplementeerd worden met steeds meer nadruk op verankering. Ten tweede is het model cyclisch van karakter.Na het doorlopen van de verschillende fasen zou sprake moeten zijn van een nadruk op eerste orde leren, maar ook dan zal steeds opnieuw het doorlopen van deze fases aan de orde zijn.[3]

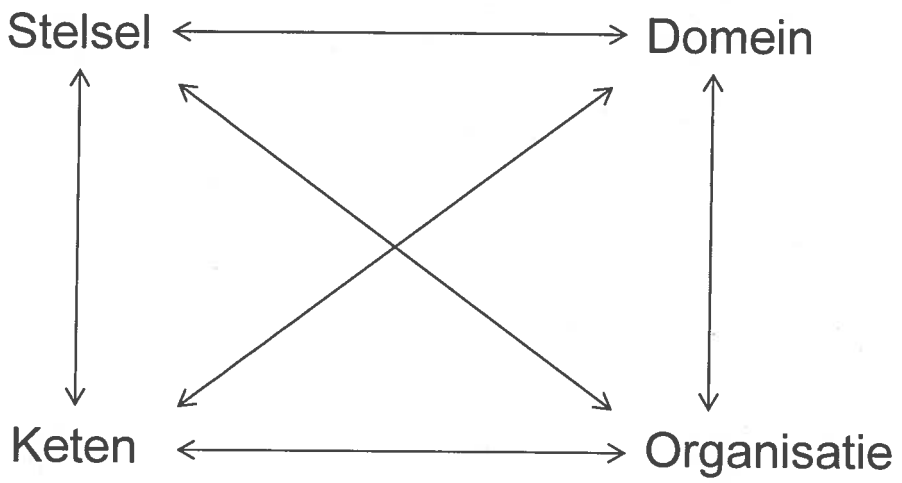
Let op: terminologie en invulling in model wijzigt; veilheidsketen in plaats van interpretatie, intuïtie enz. Wordt zo simpel mogelijk gemaakt en steeds verder ingevuld bij volgende paragrafen.

[3] De fasen probleemanalyse en plan van aanpak omvat eerste twee fasen van Helsloot van intuïtie en interpretatie; implementatie en review/oogsten omvat laatste twee fasen Helsloot van integratie en institutionalisering. Zie voor het cyclische karakter o.a. de verwijzing van Helsloot naar de leercyclus van Kolb



Dienstbaar aan domein

In de verschillende domeinen en bij organisaties daarbinnen verschilt zoals gezegd de situatie nogal. Er is een analyse per domein gemaakt die bij de concrete invulling nader aan de orde komt. Bij het Rijk en op het niveau van het stelsel lijkt op regulier organisatieniveau vooral eerste orde verankering aan de orde, met nog benodigde accenten van tweede orde leren. Bij de andere domeinen is dat meer gemengd. Als het gaat om het functioneren van en in ketens is een eerste indicatie dat tweede orde verankeren en leren in de meeste domeinen intensief aan de orde zal zijn. Een van de opgaven zal zijn om het leren en verankeren in wisselwerking vorm te geven. Nu al is duidelijk dat de vormgeving van de informatieveiligheid in ketens bijzondere aandacht zal vragen.

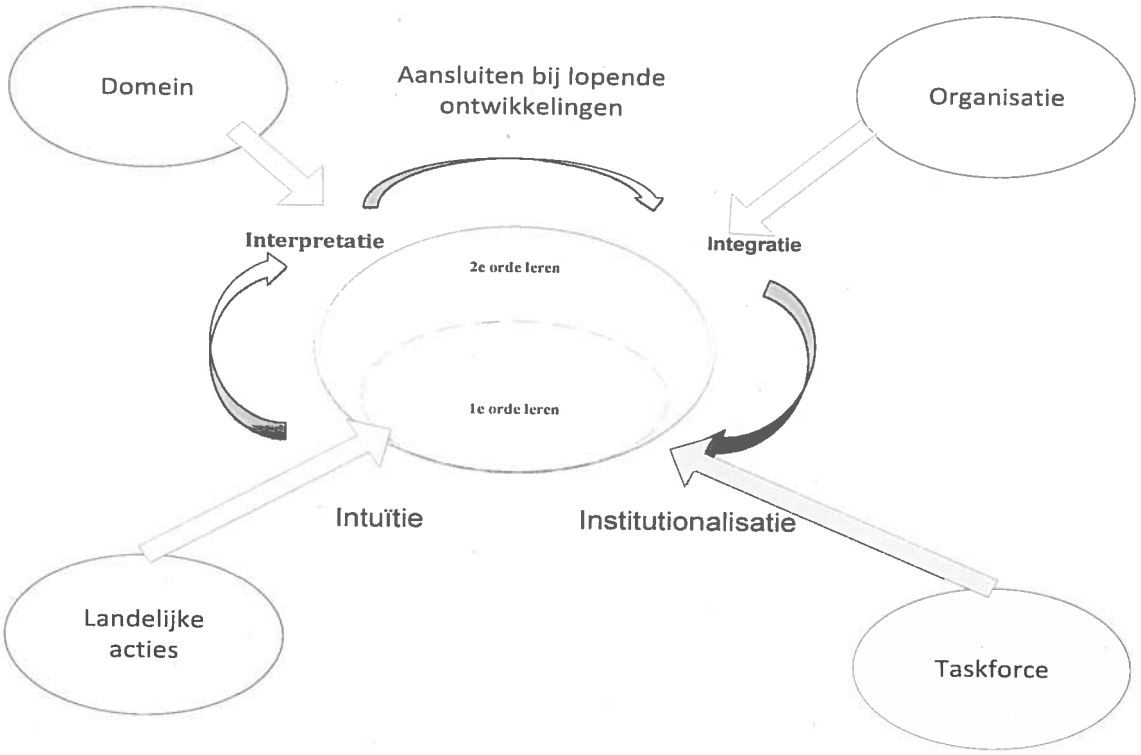


Te denken valt aan lichte feed back en coördinatie mechanismen over de grenzen van organisaties en domeinen heen bij de belangrijkste ketens

De uiteindelijk te kiezen leerstrategie is afhankelijk van een nauwkeuriger analyse van de situatie per domein en per organisatie. In de onderstaande figuur is dat weergegeven waarbij het er om gaat de leer- en verankeringsstrategie aan te sluiten bij alles dat al loopt en zich richt op het verbeteren van de informatieveiligheid op de volgende gebieden:

- Uitgangssituatie informatieveiligheidsbeleid.
- Eigen organisatiekracht om verandering te realiseren.
- Eigen domeinkracht om te ondersteunen (bijvoorbeeld door IBD, domein specifieke kenniscentra).
- Ondersteuning door overheidsbrede programma.

Let op: terminologie van intuïtie enz. vervangen door vier fasen van probleemanalyse enz.



Al deze verschillende aspecten zijn hierna bij de concrete invulling per domein nader aan de orde.

Volgorde fasering en werkvormen

De geformuleerde uitgangspunten tot nu toe leiden bij de programmering tot een bepaalde keuze in aanpak.

In een situatie dat tweede orde verandering en tweede orde leren nog daadwerkelijk aan de orde zijn zal een fasering optreden van nadruk op bewustwording, maar probleemanalyse, naar implementatie en naar review. In een situatie van vooral eerste orde verandering en leren zal wellicht een andere instap in de fase aan de orde zijn, bijvoorbeeld omdat vooral de nadruk ligt op enige organisatorische aanpassingen.

Afhankelijk van de wenselijkheid van tweede orde verandering en tweede orde leren zal ook een bepaalde keuze voor werkvormen aan de orde zijn. Bij behoefte aan tweede orde leren zal tot uitdrukking komen in de keuze voor bepaalde werkvormen. De onderstaande tabel geeft dat aan.

Werkvormen behorende bij de vier leerstappen		
Leerstap	Eerste orde leren (lower level learning)	Tweede orde leren (higher level learning)
INTUITIE Het herkennen en erkennen van het belang van informatieveiligheid voor de organisatie.		- Voorbeeldconfrontatie - Serious gaming - Peer to peer - Analyse van voorbeelden - Uitvoeren QuickScan
INTERPRETATIE Het betekenis geven aan de intuitie over informatieveiligheid; dit gebeurt binnen de omgeving van de bestuurder en top ambtelijk.	- Conferentie (presentatie en uitwerking) - Handleidingen - Uitvoeren onderzoek op hoofdlijnen	- Interactieve workshops - Themagerichte analyses - Debat en discussie - Starten risico-inventarisatie - Bepalen en vaststellen aanwezig en gewenst veiligheidsniveau
INTEGRATIE Het borgen van de aangeleerde kennis over informatieveiligheid naar andere onderdelen en medewerkers binnen de organisatie.	- Workshops voor het koppelen van thema's - Discussie en debat voor rest organisatie - Inventarisatie en beoordeling situaties en oplossingen	- Interactieve conferentie - Confrontaties met situaties en oplossingen - Praktijksimulaties en dilemmatraining - Uitwerking opdrachten voor presentatie - Inventarisatie van maatregelen per schakel van de veiligheidsketen
INSTITUTIONALISATIE Het organiseren van institutionalisatie van de informatieveiligheid binnen de organisatie.	- Conferentie, toelichten werkwijze voor stappen organisatie - Uitvoeren audits, praktijksimulaties en oefeningen	- Bieden van handleidingen en ondersteuning - Collegiale consultatie met uitwisselen van kennis en ervaringen

Doelgroepen en diffusie

Juist bij kwesties als van informatieveiligheid is voorbeeldgedrag van bestuur en (top)management wezenlijk. Zoals Helsloot stelt geldt (zie hiervoor) voor veiligheidsleren dat de dagelijkse werkpraktijk geen of niet voldoende prikkels bevat die de noodzaak van het leren duidelijk maken omdat veiligheidsrisico's immers verborgen zijn. In de uitwerking van de leerstrategie zal het dan ook wenselijk zijn te onderscheiden naar verschillende doelgroepen, die een verschillende benadering vragen. Hierna is onderscheiden naar de volgende groepen in de verschillende domeinen.

- Bestuur
- Topmanagement zoals gemeentesecretaris en directeuren
- CIO/ICT-top
- ICT management en professionals
- Medewerkers organisatie in het algemeen

Een strikt verplichte volgordevoor een effectieve benadering is er niet. Duidelijk is wel dat met name als bestuur en topmanagement in gedrag en sturing de informatieveiligheid uitdragen er diffusie van deze gerichtheid in de organisatie (en domein) zal optreden. Het lijkt dan ook zaak de als eerste drie genoemde groepen in de leerstrategie apart te positioneren, al was het maar in de zin van de andere doelgroepen beïnvloeden.

Belangrijke didactische aandachtspunten voor programmering

In de gesprekken met de diverse vertegenwoordigers van de verschillende domeinen is een groot aantal waardevolle aandachtspunten geformuleerd voor de invulling van de leerstrategie. Een aantal belangrijke stippen we hieronder kort aan.

- Bestuurders werkelijk vertrouwd maken met risico's eist oefenen bijvoorbeeld via spellen en door te leren hoe risico's daadwerkelijk gemeten en tegemoet getreden worden.
- Veel is leren van nadere terreinen zowel in termen van analogie zoals van fysieke veiligheid waarborgen als in termen van informatieveiligheid op andere terreinen.
- Bijzonder benadrukt is in de gesprekken het belang van gezaghebbende bronnen, personen, netwerken en communicatie waarop de taskforce een beroep moet doen in haar werk van leren en verankeren.
- In het verlengde daarvan volgt een nadruk op gevarieerde, ervaring gestuurde leervormen.
- Eerste orde leren volgt op tweede orde leren, maar innovatie van informatieveiligheid zal voortdurend aan de orde zijn met altijd een gevraagde bereidheid tot tweede orde verandering. De samenwerking binnen en over domeinen zal die aandacht voor en bereidheid tot innovatie moeten ondersteunen.
- Er valt veel van elkaar te leren en over te nemen aan instrumentarium; de inrichting van de leerstrategie moet gericht zijn op dat wederzijds leren. Het principe zou moeten zijn 'eerste orde helpt tweede orde'.
- Etc.

2. Verankering als verplichtende zelfregulering

Leren in de zin van bewustzijn en kennis van, maar ook actieve gerichtheid op informatieveiligheid is alleen effectief en duurzaam als het verankerd wordt in organisatie-, domein- en stelselprocessen. In de figuren hierboven over de wisselwerking is dat nader aangegeven. Als beoogde eindsituatie is aangegeven dat in ieder domein zelfregulering plaats vindt voor de ontwikkeling en handhaving van de informatieveiligheid, gegeven de verschillende verantwoordelijkheden en de ontwikkelingen op stelselniveau zoals van NCSC en Logius. De samenwerking tussen landelijke organisaties en domein alsmede de rol die de Taskforce daar kan spelen komt het volgende hoofdstuk nader aan de orde. Dit hoofdstuk handelt over de verankering in een arrangement van verplichtende zelfregulering per domein.

Er is een aantal factoren van invloed voor het draagvlak en de werking van zo'n verplichtende zelfregulering. We noemen er vier die nu van belang zijn.

- Op de eerste plaats daadwerkelijke gerichtheid op informatieveiligheid; zie daarvoor het vorige hoofdstuk en hierna de uitwerking naar programmering. Van belang is dus wel dat na de eerste twee jaar, dus ook na 2014 dat leren een plek heeft in de aanpak van informatieveiligheid (door oefenen etc.)

- Ten tweede transparante van de gehanteerde normatiek, oordeelsvorming en sanctionering; zie hierna in dit hoofdstuk.
- Ten derde een maximaal streven naar efficiency door vermindering van de administratieve lasten met name ook door efficiënte (externe) auditing verplichtingen. Zie dit hoofdstuk.
- Ten vierde een goede samenwerking in het domein en op stelselniveau. Zie dit hoofdstuk en het hoofdstuk over samenwerking en taakverdeling.

Afspraken normatiek

*'De open standa*arden voor informatiebeveiliging NEN 27001 en NEN 27002 al op de '"Comply or Explain"" (Pas-toe-of-leg-uit')-lijst van het Forum Standaardisatie zijn opgenomen als verplichte standaarden voor de hele overheid ligt het inde rede dat deze standaarden in voornoemde organisaties de belangrijke leidraad zullen zijn voor het handelen. Binnen de Rijksoverheid zijn deze standaarden uitgewerkt in de Baseline Informatiebeveiliging Rijk (BIR). Tevens zal er dit jaar een baseline informatiebeveiliging voor gemeenten worden ontwikkeld, die aansluit bij de baseline van de Rijksoverheid Binnen de werkzaamheden in het kader van de Taskforce zal het belang van deze NEN-standaarden bij de bestuurders worden beklemtoond. .

Ook bij provincie en waterschappen bestaat de gedachte en het initiatief een BIR uit te werken in deze zin. Een dergelijke BIR kan dan de basis vormen voor zelfevaluatie en externe toetsing.

NEN Auditing en visitatie per organisatie per domein en oordeelsvorming

Het doel is dat uiteindelijk alle betrokken organisaties een adequaat veiligheidsbeleid verankeren, zich zelf daarover een oordeel vormen en dat daarop adequaat toezicht is. De combinatie van een adequate BIR per domein, een jaarlijkse zelfevaluatie als basis ook voor een accountantsoordeel en een vierjaarlijkse visitatie, met als streven eind 2014 een eerste visitatie gepleegd te hebben. Uiteindelijk dienen alle organisaties oordelen als hieronder weergegeven over zich zelf te kunnen vellen en extern te kunnen valideren. Binnen rijk en zbo's bestaan al verplichtingen tot het doen uitvoeren van EDP-audits. Ook de G4 is aan een dergelijk regime onderworpen. De minister benadrukt verder de verantwoordingsplicht over de informatieveiligheid als een normaal onderdeel van de bestuurlijke verantwoordelijkheid te zien en suggereert opname er van in de jaarlijkse auditcycli. De minister benadrukt ook dat de periode van twee jaar tevens gebruikt zal worden om een analyse te maken van bestaande en noodzakelijke wet- en regelgeving, inclusief de handhaving van al bestaande regels. Bij onvoldoende resultaat volgt beraad op nadere wetgeving. Het lijkt raadzaam per domein zelf naar transparantie en oordeelsvorming te streven en de uitkomsten van audits en visitaties op domeinniveau inzet van gesprek te kunnen maken, al of niet met verdergaande sturingsmogelijkheden dan openbaarheid van dat gesprek. Openbaarheid van gesprek zou de regel kunnen zijn.

DigiD-assessments

De nu afgesproken DigiD-assessments zijn een goede start voor een toets op informatieveiligheid. Dit assessment bestrijkt echter slechts een deel van de relevante informatie en informatiestromen

binnen de overheid. Het zal een goed startpunt zijn voor een bredere analyse van de stand van de informatieveiligheid in de eigen organisatie. Zie hierna bij concrete programmering.

Een veelheid aan audit en visitatie verplichtingen en initiatieven

Inmiddels bestaan voor verschillende informatieketens verschillende auditing verplichtingen. En er lijken er meer te volgen. Geadviseerd wordt deze verplichtingen te inventariseren en analoog aan het streven naar 'single audit' en beperking van informatieverplichtingen tot waarop sturing plaats vindt, uitgaande van een adequate BIR. De problematiek van ketens behoeft apart aandacht.

3. Eindproducten, producten per fase

De aard van de opdracht van de taskforce leidt er toe dat de doelstellingen 'smart' te formuleren moeten zijn, de benodigde middelen (tussen producten) effectief zijn en zo een sterk operationeel optreden mogelijk is. Na de hieronder geformuleerde eindproducten volgt op basis van de hiervoor geformuleerde inzichten een opbouw per fase en overzicht van te leveren tussenproducten. Na een inschatting van de huidige situatie per domein volgt een eerste invulling van de programmering per domein.

Eindproduct

Samenvattend zal mede door de taskforce binnen de kaders van haar opdracht na twee jaar een voor de diverse domeinen uitgewerkte systematiek van verplichtende zelfregulering tot stand moeten zijn gekomen, dan wel inzichtelijk zijn. In termen van eindproducten is dat als volgt te omschrijven.

- Een aantoonbare verbetering van veiligheidsbewustzijn en handelingsgerichtheid op informatieveiligheid.
- Een geharmoniseerd normenkader gebaseerd op NEN 27001 en 27002.
- De implementatie daarvan binnen de overheid.
- Een werkende en geaccepteerde systematiek om de voortgang van de implementatie te meten en inzichtelijk te maken.
- Een geharmoniseerd maar per domein specifiek ontwikkelde systematiek voor peer-reviewing en self-assessmentss.
- Een per domein geharmoniseerd auditkader.
- Een voor iedere organisatie uitgevoerde visitatie gericht op het vaststellen van de verplichtende zelfregulering.
- Een overdrachtsrapportage waarin de bereikte resultaten worden geduid en geaccepteerde voorstellen zijn opgenomen hoe het bereikte resultaat regulier wordt verankerd.

Modelinvulling per fase

Gebaseerd op de hiervoor gemaakte onderscheidingen naar eerste orde en tweede orde en leren en verankeren leidt dat tot een eerste invulling per fase van probleemanalyse tot oogsten/review.

Probleemanalyse algemeen

Leerdoelen	Leermethoden	Verankering
Het **herkennen** van het belang van informatieveiligheid voor de **eigen** organisatie met in ieder geval zicht op - Omvang en intensiteit daarvan - Oplossingsrichtingen voor verbetering daarvan Het betekenis geven aan informatieveiligheid; Identificatie met beveiligingsdoelstellingen	**2e orde** • Bewustwordingsconferentie obv DigiD-assessments • Introductie quick scans • Richting geven aan oplossingsrichtingen • Voorbeeldconfrontatie door vliegende brigades **1e orde** • Conferentie (presentatie en uitwerking) • Introduceren Opleidingsaanbod • Ontwikkelen handleidingen	Opdracht adequate quickscan Uitvoeren quick scan • Besluiten over bestaand niveau informatiebeveiliging • Formuleren en beslissen over gewenst beveiligingsniveau van de organisatie • Opdracht tot uitvoering' ontwerp van de verandering' • Aanmeldingen voor opleidingsaanbod • Opdracht tot oplossen urgente vraagstukken

Ontwerp van de verandering algemeen

Leerdoelen	Leermethoden	Verankering
Kennis over relevante veranderingsstrategieën rond informatieveiligheid Bewustwording van het belang van deze strategieën voor eigen organisatie Verandering willen doorvoeren (betrokkenheid)	**2e orde** Interactieve conferentie gericht op formuleren veranderingsplannen. Onderdeel daarvan maken uit: • Interpretatie van de resultaten quick scan • Confrontaties met situaties en oplossingen	Opleveren organisatie veranderingsplan Besluit over de inhoud Opdracht tot implementatie Gerealiseerde urgente verbeteringen

	• Praktijksimulaties en dilemmatraining • Introductie in de veiligheidsketen • Serious gaming (oefenen in veilgheidssimulaties) **1e orde** • Vakinhoudelijke trainingen op het gebied van informatieveiligheid • Vakinhoudelijke trainingen op het gebied van inrichting van de veiligheidsketen • Vakinhoudelijke trainingen rond organisatie van informatieveiligheid • Workshops voor het koppelen van informatieveiligheid en veiligheidsketen	

Uitvoering van de verandering

Leerdoelen	Leermethoden	Verankering
Organisatie vaardigheden bijbrengen voor een succesvolle implementatie op het gebied van: • informatieveiligheid • het belang van denken in veiligheidsketen • project en programmamanagement • auditing • borging en toetsing Gerichtheid op uitvoeren van verbeterplannen rond informatieveiligheid	**2e orde** • Bieden en borgen van handleidingen en ondersteuning • Collegiale consultatie met uitwisselen van kennis en ervaringen • Praktijksimulaties en dilemmatraining per organisatie **1e orde** • Vakinhoudelijke trainingen • Veiligheidsketen • Informatieveiligheid • Project/programmanagement	Implementeren veranderplan Oplevering rapportage gerealiseerde organisatieverandering • Opdracht tot uitvoeren van visitatie

	• Uitvoeren audits, praktijksimulaties en oefeningen	

Oogsten en reviewen

Leerdoelen	Leermethoden	Verankering
Hoe de inrichting van beveiligingsorganisatie en beveiligingsbewustzijn blijvend te verankeren door 1e orde leerdoelstellingen (waar nodig 2e)	**2e orde** • Continue voeden van peer-groups **1e orde** • Periodiek organiseren van relevante oefensituaties, gebaseerd op de principes van de veiligheidsketen. • Volgen Vakinhoudelijke trainingen • Gebruik maken van handleidingen die beschikbaar zijn bij stelselpartijen	• Visitatie van de organisatie uitgevoerd Visitatie ondergebracht in een cyclus (periodiek), jaarlijkse audit Peer groups geïnstitutionaliseerd

Samenvatting te leveren producten

Deze analyse per fase leidt samenvattend tot de volgende tussenproducten

Eindproducten leren	**Eindproducten verankering**
Bewustwording, kennis, inzicht, handelingsgerichtheid; zie eerdere sheets - -	Reguliere audits, oefening etc etc.; zie eerdere sheets - -
Leerproducten	**Verankeringsproducten**
• Bewustwordingsconferentie • Verdiepings, learn and share obv DigiD-assessments • Voorbeeldconfrontatie door vliegende brigades • Conferentie (presentatie en uitwerking) • Introduceren Opleidingsaanbod • Simulaties, serious gaming oefeningen etc. • Etc. etc.	• Introductie quick scans • Methodiek Quick scans • Model veranderingsplannen • Handleidingen • Modelaudits, • Overzichten resultaten • Etc. etc.

4. Zelfregulering en programmering nader vorm gegeven

Op basis van de leerstrategie en de geformuleerde opdracht is de volgende eerste uitwerking van de programmering uitgewerkt. Een aanzet van een programmeringsboek naar domein over de twee jaar voor concrete activiteiten is gemaakt maar behoeft eerst overeenstemming over de hoofduitwerking hieronder.

Verplichtende zelfregulering

Het streven is per domein en organisatie te komen tot wat genoemd is 'verplichtende zelfregulering van de informatieveiligheid' zoals in de leerstrategie uiteengezet. Dat is hier als volgt nader geoperationaliseerd als basis voor de nadere programmering per domein.

Normatieve basis

- Als normatieve basis voor de inrichting van en oordelen over de informatieveiligheid geldt een Baseline Informatie Richtlijn per domein gebaseerd op de open standaarden voor informatiebeveiliging ISO 27001 en ISO 27002 (BIR voor het Rijk, BIG voor gemeenten, Petra voor Provincie, evenzo voor waterschappen en, in iets andere vorm, ZBO's; zie ook relatie met Nora)
- Als aan de betreffende BIR is voldaan, is in principe de informatieveiligheid op orde

Verankering per organisatie

- Basis voor de inrichting van de informatieveiligheid is de informatieveiligheidsketen van
    a. Pro-actie
    b. Preventie
    c. preparatie
    d. Respons
    e. Herstel
- Iedere betrokken organisatie regelt de informatieveiligheid op adequaat niveau, uitgaande van deze informatieveiligheidsketen, zowel op het niveau van de primaire processen als van de bedrijfsvoeringsprocessen, waarbij reguliere procesvoering en ontwikkeling daarvan beide de benodigde aandacht krijgen. Daarbij is er aandacht voor processen die zijn uitbesteed en voor leveranciers.
- Iedere betrokken organisatie kent reguliere auditing (jaarlijkse), auditing van de kwaliteit van de informatieveiligheid. De auditoordelen zijn onderwerp van bestuurlijk en waar aan de orde politiek overleg en leiden tot nadere acties.

Verankering per domein

- Op domeinniveau is er een instantie per domein direct belast met de sturing op de ontwikkeling van de informatieveiligheid in het domein en er is een stelsel van afspraken over de aansturing daarvan door koepel en organisaties.
- Op domeinniveau zijn er voorzieningen die de ontwikkelingen op organisatieniveau ondersteunen, zodanig dat de actuele ontwikkeling in informatieveiligheid, de eisen die dat stelt en de mogelijkheden daaraan te voldoen helder zijn en zodanig dat waar mogelijk op domein niveau 'shared services' tot stand komen die organisaties helpen zo efficiënt mogelijk aan de eisen van informatieveiligheid te voldoen. Met IBD, CIF, GBO-provincies, HWH, DG Rijk zijn daar al stappen in gezet.
- Op domein niveau bestaan afspraken over de te verrichten audits en een reguliere (bijv. per vier jaar) externe visitatie. In ieder geval de uitkomsten van die visitaties kunnen onderwerp van dialoog zijn van de betreffende organisatie en enigerlei instantie op domeinniveau. De uitkomsten van die dialoog zijn openbaar en kunnen adviezen inhouden aan andere instanties tot actie om de informatieveiligheid te waarborgen.

Verankering op ketenniveau

- De informatieketens per domein, over de domeinen heen en ook over de grens van het gehele overheidsdomein kennen een coördinerend ketenverantwoordelijke voor informatieveiligheid, vaak instantie die verantwoordelijk is voor regie op de betreffende keten-primaire processen. Daarbij is er het besef dat ketens al vaak een te eenvoudige aanduiding is; vaak is sprake van netwerken van informatienetwerken met meervoudige stromen en verantwoordelijkheden. Er wordt overeenstemming bereikt over de domeinen heen welke instantie de coördinerende verantwoordelijkheid heeft.
- Deze coördinerende verantwoordelijkheid is gegeven de bestaande verantwoordelijkheid van iedere organisatie voor de eigen gegevenshuishouding in het betreffende deel van de keten.
- Deze ketenverantwoordelijke heeft tot taak:
  - de stromen en afhankelijkheden in kaart te brengen;
  - te rapporteren over de stand van de informatieveiligheid op basis van informatie van de keten (netwerk)partners;
  - overleg over informatieveiligheid te voeren met de relevante keten (netwerk)partners;
  - in dat overleg te streven naar verbetering van de informatieveiligheid;
  - over de uitkomsten eventueel (openbaar) aanbevelingen te doen aan bevoegde instanties.

Verankering op stelsel niveau

- Deze verplichtende zelfregulering is gebaseerd op de vigerende verantwoordelijkheden en landelijke voorzieningen.
- Deze voorzieningen zijn gericht op optimale ondersteuning van organisaties en domeinen.
- Deze landelijke voorzieningen, in relatie tot de ontwikkeling op domeinniveau zijn onderwerp van coördinatie gericht op afstemming en verbetering.
- De minister van BZK is stelsel verantwoordelijk en rapporteert regulier over ontwikkeling van het gehele stelsel.
- Uitgangspunt is omgang met risico's en risicovermindering. Het streven is naar slimme oplossingen; aan openbare informatie zijn bijvoorbeeld naar de aard minder **informatie**veiligheidsrisico's verbonden dan aan vertrouwelijke informatie, niet alle risico's zijn even ernstig (er is prioritering nodig) etc.
- Zowel op domeinniveau als op stelselniveau vindt uitwisseling van ervaringen en instrumenten plaats; opnieuw steeds het eigen wiel uitvinden geldt als ultieme domheid.

Leren

- Iedere organisatie, ondersteunt per domein, traint regulier in een actieve gerichtheid van bestuur, management, ICT-functie en andere medewerkers op informatieveiligheid. Deze oefeningen zijn nadrukkelijk bestuurlijk geleid.

- Dit 'leren' is verankerd in de BIR en verkrijgt aparte aandacht bij auditing en visitatie; aandacht is er daar ook voor de daadwerkelijke gerichtheid als uitkomst van dat leren.
- Uitgangspunt van BIR, processen van ondersteuning op domein en stelselniveau, is het bewustzijn dat sprake is van omgang met risico's en niet van risico's volledig kunnen bestrijden.

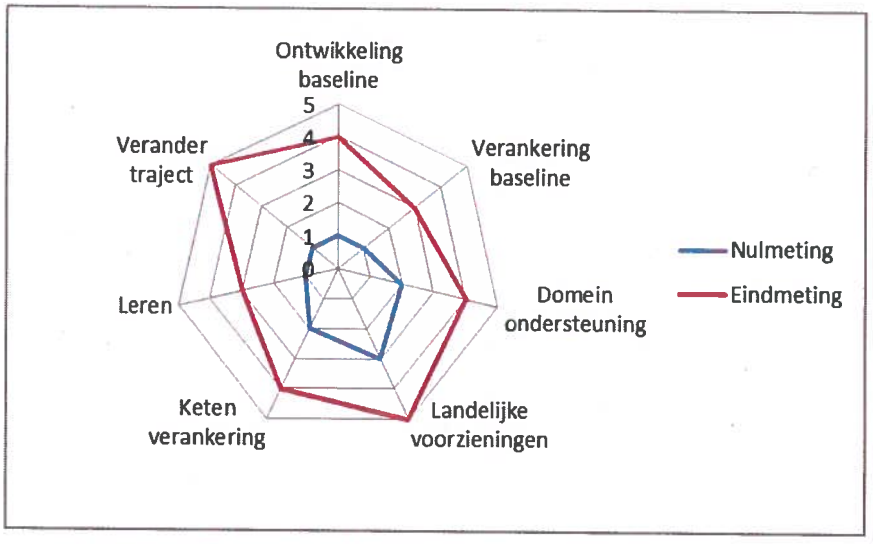
6. Verandering per organisatie en per domein

- Iedere organisatie en ieder domein kent een probleemanalyse en een veranderplan.
- Er is een implementatietraject dat systematisch doorlopen wordt en waarvan de voortgang meetbaar is.

5. De programmering per domein algemeen en samenwerking taskforce

De programmering per domein moet gericht zijn op dit doel van verplichtende zelfregulering. Die programmering zal per domein dus afhankelijk zijn van hoe het staat met de volgende standaards.

- De ontwikkeling van een adequate baseline informatie richtlijn (BIR).
- De verankering van de BIR per organisatie.
- De ondersteuning daarvan en voeren van dialoog op domeinniveau.
- Het gebruik van landelijke voorzieningen als NCSC, Logius voor verankering op organisatie en domeinniveau.
- De verankering van informatieveiligheid in relevante ketens.
- Het leren per organisatie en op domeinniveau van gerichtheid op informatieveiligheid.
- De aanwezigheid van een verandertraject dat in voortgang meetbaar is.



6. Programmering gemeente en samenwerking met Taskforce

Een eerste toepassing van de zeven standaards op de situatie in het gemeentelijk domein levert een globaal beeld, met mogelijke programmering en een mogelijke samenwerking met de taskforce.

De Baseline Informatiebeveiliging Gemeenten (BIG)

Afgeleid van de Basisrichtlijn informatiebeveiliging Rijk is een basisrichtlijn informatierichtlijn gemeenten in ontwikkeling. De basisrichtlijn is gebaseerd op de NEN 27002; code voor informatiebeveiliging. Deze aandacht voor informatieveiligheid zou met de implementatie van de richtlijn in ieder geval binnen de IT kolom afdoende geregeld zijn. De aandacht voor informatiebeveiliging in de gebruikskolom en bij nieuwe ontwikkeling van de primaire en secundaire processen krijgt in de richtlijn aandacht, zij het beperkter dan die van de IT kolom. Als direct uitvloeisel van de Diginotar en Lektober affaires zijn door Logius richtlijnen geformuleerd die nu dienen als basis voor de DigiD-assessments. Deze richtlijnen zijn afgeleid van de NEN norm die ook onderliggend zijn aan de Basisrichtlijnen. Daarnaast bestaan in het gemeentelijk domein meerdere normenstelsels voor het voldoen aan onder andere BAG en GBA normen. Gedeeltelijk zijn deze normen specifiek toegesneden op de betreffende basisadministratie; zij zullen ook stevige overlap kennen met de basisrichtlijn. Vanuit het gemeentelijk domein wordt sterk aangedrongen op uniformering van normenstelsel.

Programmering en taskforce

De implementatie van de BIG is topprioriteit. De doelstelling kan zijn in 2013 normenstelsels en BIG te integreren zodat inderdaad gesproken kan worden van een baseline informatiebeveiliging voor gemeenten. Dat betekent dus dat gebruik van huidige normenstelsels en daarop ingezette audit initiatieven vooralsnog doorgaat tot de BIG in werking is.

De werking van het normenstelsel moet goed gemeten worden. Binnen KING is en wordt ervaring opgedaan met diverse instrumenten als benchmarks en i-spiegel voor operatie NUP. Het is vooral van belang dat de inzet van een meetinstrument past binnen de kaders van een samenhangend normenstelsel dat met een slimme inzet van self-assessment, peer-review en externe visitatie leidt tot een zichzelf regulerend systeem van informatiebeveiliging binnen het gemeentelijk domein. Aanvullend op de stroomlijning van normenstelsel kan de taskforce de IBD ondersteunen om het auditraamwerk voor gemeenten te stroomlijnen en toe te werken naar een maximale efficiency bij het inzetten van respectievelijk self-assessments; peer reviews samenhangend externe auditinstrumenten.

Verankering per organisatie

Ook bij gemeenten geldt dat adequate implementatie en toepassing van de BIG in principe betekent dat aan de eisen van informatieveiligheid is voldaan. De verankering van informatieveiligheid in de gemeentelijke organisatie is vanuit dat oogpunt nog zeer verschillend. Het meest voortgeschreden lijkt de situatie in de G4 gemeenten die een CIO hebben aangesteld en waar analoog aan het Rijk de implementatie van verankering van informatieveiligheid gericht vorm krijgt. Ook daar zal het nog enige tijd duren voor sprake is van volledige implementatie van de BIG. In de andere gemeenten is de situatie verscheiden, maar globaal gesproken is niet sprake van een systematische vormgeving

aan informatiebeveiliging. De informatiebeveiligingsdienst (IBD) is beoogd per 1 januari 2013 operationeel te zijn en zal zich vooral richten op preventie en respons en herstel.

Het inzetten van het audit instrumentarium om daarmee structurele verbeteringen te realiseren in de veiligheid van informatievoorziening komt slechts beperkt op de agenda. De diversiteit in audits en veelal net overlappende scopes zijn dan niet behulpzaam om dit onderwerp adequaat te programmeren. De uitkomsten van het DigiD assessment is in principe een goed uitgangspunt om meer systematisch de probleemanalyse en veranderingsstrategie te starten Er is echter geen zicht op wanneer precies die DigiD assessment resultaten er zullen zijn.

Programmering en taskforce

In het verlengde van de beoogde activiteiten van de IBD inzake preventie en respons is er vooral ook behoefte aan het uitrollen en implementatie van de BIG. Gemeenten moeten echter middelen en methoden aangereikt krijgen op basis waarvan zij implementatie van richtlijn systematisch vorm kunnen geven en verankeren. De meer algemene strategie om dat te stimuleren kan in principe belegd worden bij de IBD. Daar is immers voldoende kennis van de opzet van gemeente brede implementatietrajecten. De huidige plannen voorzien niet in zo'n uitrol gericht op een systematische implementatie van de BIG per organisatie. De wijze waarop de organisaties invulling moeten geven is aan zelfregulerend vermogen is nog niet systematisch uitgewerkt, behoudens bij de G4 en wellicht enige andere gemeenten. Het niet systematisch gepland zijn van de voltooiing van de DigiD-assessments maakt een planning ook moeilijk.

De taskforce kan de IBD en gemeenten behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de BIG en het koppelen aan de uitkomsten van de DigiD-assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learn and share' overleg met gemeenten die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieén en implementatie. Zie bij verandertraject.

De taskforce kan IBD ondersteunen bij het inregelen van pro-actie en preventieprocessen door het ontwikkelen van voor het domein relevante handleidingen, instructies, oefenmateriaal etc. Steeds in nauwe samenhang met de doelstellingen van de IBD, met tegelijkertijd de focus op het realiseren van een systeem van zelfregulering.

Mogelijk dat de taskforce met de IBD ook bestaande organisaties als VIAG en IMG bij de ontwikkeling van dergelijk instrumentarium kan betrekken. KING kan daarbij een rol vervullen bij het beheren van dit instrumentarium.

De verankering in het domein

De komst van de IBD is een majeure interventie om informatiebeveiliging binnen het domein aandacht te geven. De rol van IBD is in eerste instantie gericht op het tijdig onderkennen en opvangen van bedreigingen. De intentie van IBD is dat zij zich binnen het domein richt op preventie en pro-actie/respons. Er is echter niet een systematische gerichtheid op een stelsel van zelfregulering. In termen van uitrol van de BIG kan de IBD in de toekomst die rol zeker op zich

nemen.Samen met NCSC, Logius en andere stelselvoorzieningen zou dan een goed functionerend stelsel kunnen ontstaan voor technische voorzieningen en de implementatie daarvan. Als het gaat om de bredere scope van de inrichting van zo'n stelsel zal de VNG/KING die rol moeten vervullen en zal daarop een aantal punten nader gesprek moeten plaats vinden, met name ook inzake externe visitaties en eventueel vellen van openbare oordelen en mogelijke maatregelen uitlokken.

Programmering en taskforce

De taskforce kan de dialoog binnen het gemeentelijk domein over de vormgeving aan zelfregulering stimuleren. De taskforce zou met de VNG met name ook bestuurders en raadsleden kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie en de rol van de raden daarin benadrukken, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten.

De taskforce zou kunnen bijdragen aan het gesprek over en de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.

De verankering in ketens

Het Rijk is regisseur van belangrijke ketens, zoals die van identiteit (GBA, paspoort etc.), of van de justitiële ketens zoals rechtsgang, vreemdelingen. Gemeenten zijn in veel van deze ketens betrokken in de uitvoering. Aparte aandacht verdienen de basisregistraties. Op veel van die ketens is nog geen coördinerende verantwoordelijkheid voor informatieveiligheid geregeld. Wel zijn stukken van informatieveiligheid geregeld in allerlei auditverplichtingen. Dit leidt tot een bont geheel van verplichtingen voor keten (netwerk)partners. Bij een aantal ketens is coördinerende verantwoordelijkheid van gemeenten, of organisaties uit andere domeinen te overwegen. In het kader van de decentralisaties van de jeugdhulp bijvoorbeeld.

Programmering en taskforce

Het gaan werken aan keten informatieveiligheid heeft een hoge prioriteit. Samen met de taskforce en samen met andere domeinen is inrichting van een ketenregime op een aantal prioritaire ketens, een voor de hand liggende activiteit die nu onvoldoende tot stand komt. (Wellicht heeft het Rijk hier een dringender rol). Er loopt onderzoek naar de eisen te stellen aan de SUWI keten; daarop wachten is niet noodzakelijk. De resultaten zullen liggen in termen van welke eisen te stellen aan een keten.

Gebruik landelijke voorzieningen

Het NCSC is het landelijke samenwerkingsplatform voor expertise en advies alsmede respons en crisisbeheering op het gebied van ICT-veiligheid. Het NCSC vervult daarbij tevens een rol als CERT (Computer Emergency Response Team), met als primaire doelgroepen de Rijksoverheid en vitale organisaties. Andere overheden, bedrijfsleven en de burger zijn secundaire doelgroepen. Het NCSC monitort constant bronnen en detecteert bedreigingen op de informatievoorziening, geeft waar nodig aanwijzingen om de betreffende bedreigingen te weerstaan en is in het uiterste geval verantwoordelijk voor operationele coördinatie tijdens een crisisorganisatie. In die zin versterkt het NCSC de weerbaarheid van de departmentenale en vitale informatievoorziening. De IBD (met

gemeenten juist als primaire doelgroep) gaat in samenwerking met het NCSC voor het gemeentelijk domein de preventie en respons versterken. Zij volgt de analyses en richtlijnen van NCSC een draagt zorg voor de (crisis) communicatie in samenhang met de NCSC informatievoorziening.

Programmering en samenwerking taskforce

De taskforce kan in het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein.

Leren

De aandacht voor het onderwerp informatiebeveiliging binnen gemeenten is zeer wisselend van aard en lijkt maar deels afhankelijk te zijn van de omvang of grootte van de betreffende gemeente. Zie wel de opmerkingen over de G4. DigiNotar en Lektober hebben het bewustzijn voor het thema aangewakkerd. Dat is versterkt door allerlei communicatie zoals bijeenkomsten georganiseerd door de VNG. Dit bewustzijn is binnen de ICT kolom sterker en in veel mindere mate binnen de gebruikskolom. Bestaande audit initiatieven worden meer ingezet als toets achteraf, dan als middel om informatiebeveiliging als structureel onderwerp op de agenda te zetten. Er is nog geen systematische gerichtheid op oefenen, dan wel anderszins duurzaam de gerichtheid op informatieveiligheid te bewerkstelligen.

Programmering en taskforce

In termen van het model van leren en verankeren is een stevige impuls nodig op het creëren van bewustzijn voor verankering. Met erkenning van alle verscheidenheid en alle aandacht die er al geweest is en nog is, lijkt een systematische aandacht voor leren van bestuurders en top management nog geboden. Dat moet niet meer door algemeen bijeenkomsten, maar nauw gekoppeld aan de verdere ontwikkeling naar zelfregulering. Eerder in dit document is al aangegeven dat de verankering van een baseline binnen gemeenten een gericht leerproces vereist. De taskforce zou (in nauwe samenwerking met de IBD een dergelijk ondersteunend programma moeten faciliteren. Gegeven de problematiek en diversiteit van gemeentelijke organisaties is daarbij een gefaseerde aanpak wenselijk die allereerst inzet op bewustwording en probleemanalyse, vervolgens een planmatige aanpak van verandering ondersteunt en tot slot afsluit met een werkende systematiek van zelfregulerende visitatie en auditinstrumenten. In een bijlage hebben we een mogelijke invulling van een dergelijk meerjarig programma gericht op de gemeentelijke omgeving ingevuld. Hierna, bij verandertraject is aangegeven dat de complexe situatie in het gemeentelijk domein een meer pragmatische aanpak vraagt. De fasering is echter uiterst nuttig als referentiepunt om te toetsen of doordacht gericht op leren en verankeren te werk wordt gegaan.

De IBD en de taskforce kunnen gebruik maken van de van de inmiddels bij KING opgebouwde ervaring rond implementatie van landelijke programma's.

In praktische zin is er rond het vergroten van bewustwording al een aantal initiatieven van NCSC tegengekomen die erop is gericht om awareness te vergroten. Ook binnen CIP zijn interessante aanzetten gegeven om invulling te geven aan bewustzijn rond informatiebeveiliging. Ook deze aanzetten kunnen in deze programmering specifiek voor gemeenten een plaats krijgen.

Binnen het departement BZK wordt geëxperimenteerd met een digivaardigheidsbewijs. Het betreft een korte training van eindgebruikers door middel van een e-leanring omgeving. De training wordt bij positief resultaat afgesloten met een certificaat. Het experiment is overgenomen van de Rabobank waar al langer met een dergelijk instrument getracht wordt informatiebeveiligings-bewustzijn te vergroten. Ook een dergelijk instrument kan in de gemeentelijk programmering een plaats krijgen.

Op het terrein van leren is nog weinig binnen het domein voorhanden. Het doen ontwikkelen van opleidingsfaciliteiten en cursusaanbod kan een activiteit van de taskforce zijn in afstemming met IBD en afnemers.

Voortgang verandertraject

In het gemeentelijk domein moet nog veel gebeuren om bewustwording en verankering van informatiebeveiliging te realiseren. De stap naar een zelfregulerend systeem vraagt vaak nog tweede orde verandering en tweede orde leren. In de auditing zou de aanwezigheid van probleemanalyse, plan en implementatie dan ook systematisch aan de orde moeten komen.

Programmering en taskforce

Het veranderingstraject vereist een pragmatische insteek, waarin de verschillende lopende processen en de verschillen die er tussen de organisaties zijn op een creatieve manier inzetbaar zijn. Vanuit de DigiD-assessments lijkt een modelaanpak geëigend van probleemanalyse, naar veranderstrategie, naar implementatie en naar review zoals die in de bijlage omschreven. Die is in die vorm niet goed uitvoerbaar gezien het verschil tussen organisaties (sommigen zijn al in de fase naar eerste orde leren) en door de verschillende stromen van interventies die er lopen. Verbeteringen op terrein van response moeten snel en kunnen niet wachten. De onzekere planning van de DigiD-assessments en de grote eisen die decentralisaties en bezuinigingen eisen stellen leiden eveneens maatwerk in de voortgang naar een zelfregulerend stelsel. Hiervoor is al aangegeven dat de start van een systematisch verandertraject zou kunnen liggen bij de systematische bespreking met groepen gemeenten van de uitkomsten van de DigiD-assessments. Van de G4 en andere gemeenten die al verder zij kan dan veel geleerd worden. In het algemeen zal aandacht bestaan voor bestaande instrumenten, goede praktijken en de uitwisseling daarvan.

Van groot belang wordt de voortgang in het proces van verandering te kunnen meten. Het zal zaak zijn het proces van verankering en leren ook in de BIG te doen opnemen. Zie voor de meting dan verder hiervoor bij normering.

Recapitulerend Gemeenten en Taskforce

De taskforce kan naar steekwoord op de volgende kunnen bijdragen aan de programmering van het gemeentelijk domein naar verplichtende zelfregulering.

- De taskforce kan het proces van ontwikkeling van de BIG faciliteren en daardoor versnellen.
- Het kan dit proces ook ondersteunen door de programmering van bewustwordings- en kennissessies rond de richtlijn; zie bij leren.

- Aanvullend op de stroomlijning van normenstelsel kan de taskforce de IBD ondersteunen om het auditraamwerk voor gemeenten te stroomlijnen en toe te werken naar een maximale efficiency bij het inzetten van respectievelijk self-assessments; peer reviews samenhangend externe auditinstrumenten.
- Het ontwikkelen van voor het domein relevante handleidingen; instructies; oefenmateriaal etc. Steeds in nauwe samenhang met de doelstellingen van de IBD
- De taskforce kan de IBD en gemeenten behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de BIG en het koppelen aan de uitkomsten van de DigiD-assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learn and share' overleg met gemeenten die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieën en implementatie. Zie bij verandertraject.
- Het experiment met een digivaardigheidsbewijs verder ondersteunen.
- De taskforce kan de dialoog binnen het gemeentelijk domein bevorderen over de vormgeving aan zelfregulering. De taskforce zou met de VNG met name ook bestuurders en raadsleden kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie en de rol van de raden daarin benadrukken, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten.
- De taskforce zou kunnen bijdragen aan het gesprek over en de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.
- De taskforce zou met spoed op een aantal ketens een initiatief kunnen nemen met betrokken partijen over hoe de regulering van de informatieveiligheid in te richten.
- De taskforce kan in het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein. Ook een dergelijk instrument kan in de gemeentelijk programmering een plaats krijgen.
- Op het terrein van leren is nog weinig binnen het domein voorhanden; Het doen ontwikkelen van opleidingsfaciliteiten en cursusaanbod kan een activiteit van de taskforce zijn in afstemming met IBD en afnemers.

Een en ander kan resulteren in de volgende bijdragen van de taskforce aan de producten in de programmering. Let wel, het gaat hier om een eerste proeve die nadrukkelijk uitwerking behoeft met VNG en KING/IBD.

Producten programmering gemeenten

Bijdrage taskforce aan programmering	Activiteiten taskforce; steeds gaat het om in afstemming met IBD leveren van 'bijdragen

	aan'; IBD heeft normaliter 'the lead'.
De taskforce kan het proces van ontwikkeling van de BIG faciliteren en daardoor versnellen.	• Vaststellen status • Hoe versnelling te realiseren • Ontwikkelen communicatiestrategie rond BIG • Ontwikkelen stappenplan implementatie BIG voor gemeenten
Het kan dit proces ook ondersteunen door de programmering van bewustwordings- en kennissessies rond de richtlijn; zie bij leren.	• Ontwikkelen bewustwordingssessie rond BIG en belang informatiebeveiliging • Organisatie Roadshow rond BIG • Externe sprekers buiten overheidsdomein • Confrontatieworkshops
Aanvullend op de stroomlijning van normenstelsel kan de taskforce de IBD ondersteunen om het auditraamwerk voor gemeenten te stroomlijnen en toe te werken naar een maximale efficiency bij het inzetten van respectievelijk self-assessments; peer reviews samenhangend externe auditinstrumenten.	• Inventarisatie normenstelsels • Onderzoek harmonisatie normenstelsels • Harmonisatie normenstelsels in lijn brengen met BIG • Opzetten self-assessment rond geharmoniseerd normenkader • Organisatie periodieke peer review rond geharmoniseerd normenkader • Toetsen van auditconsequenties als gevolg van introductie BIG self-assessments; peer reviews:
Het ontwikkelen van voor het domein relevante handleidingen; instructies; oefenmateriaal etc. Steeds in nauwe samenhang met de doelstellingen van de IBD	• Ontwikkeling handreiking informatiebeveiliging • Organiseren gecertificeerde marktplaats training informatiebeveiliging • Ontwikkeling oefenstrategie informatiebeveiliging ism veiligheidsregio's en Certs • Organiseren van een peer to peer netwerk rond informatiebeveiliging voor bestuurders en secretarissen. (een halfjaarlijks thema op de VGS?)
De taskforce kan de IBD en gemeenten behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de BIG en het koppelen aan de uitkomsten van de DigiD-assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learnand share' overleg met gemeenten die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieën en	• Ontwikkeling monitoring voortgang realisatie BIG. Hier goed nota nemen van lessons learned van Operatie NUP en BRP.

implementatie. Zie bij verandertraject.	
Het experiment met een digivaardigheidsbewijs verder ondersteunen.	• Omwerken van het instrumentarium voor gemeentelijke omgevingen • Toesnijden op normenkaders BIG • Organiseren van beheer en beschikbaarheid tooling • Opzetten communicatie rond deze tooling tbv HRM kanaal
De taskforce kan de dialoog binnen het gemeentelijk domein bevorderen over de vormgeving aan zelfregulering. De taskforce zou met de VNG met name ook bestuurders en raadsleden kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie en de rol vande raden daarin benadrukken, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten.	• Plaatsen van instrumenten self-assessements; peer review en externe audits in een systematiek van gecontroleerde zelfregulering. • Benoemen van een aanspreekpunt voor inregeling van de systematiek bij ofwel KING ofwel IBD. • Organiseren beveiligde toegankelijkheid van de resultaten
De taskforce zou kunnen bijdragen aan het gesprek over en de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.	• Zie voorgaand punt
De taskforce zou met spoed op een aantal ketens een initiatief kunnen nemen met betrokken partijen over hoe de regulering van de informatieveiligheid in te richten..	• Zie voorgaand punt, maar dan in relatie tot ketens. Concreet minimaal het gesprek met SUWIketen; Veiligheidsketen
De taskforce kan in het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein. Ook een dergelijk instrument kan in de gemeentelijk programmering een plaats krijgen.	• Hier aansluiten bij acties van KING op het gebied van convenantvorming. • Taskforce faciliteert uitbreiding convenantafpraken rond voldoen leveranciers aan BIG afspraken. • Mogelijk ontwikkeling van een DIID testplaform
Op het terrein van leren is nog weinig binnen het domein voorhanden; Het doen ontwikkelen van opleidingsfaciliteiten en cursusaanbod kan een activiteit van de taskforce zijn in afstemming met IBD en afnemers/	• Al eerder benoemd

7. Programmering provincie en samenwerking met taskforce

Een eerste toepassing van de zeven standaards op de situatie in het provinciaal domein levert het volgende globale beeld, met mogelijke programmering en een mogelijke samenwerking met de taskforce.

De Baseline Informatiebeveiliging provincies (onderdeel van de PETRA)

Er is een Baseline Informatiebeveiliging Provincies, vastgesteld in AAC Middelen en IPO bestuur. De basisrichtlijn is gebaseerd op de NEN 27002; code voor informatiebeveiliging en NORA. De aandacht voor informatieveiligheid zou met de implementatie van de richtlijn in ieder geval binnen de IT kolom afdoende geregeld zijn. De aandacht voor informatiebeveiliging in de gebruikskolom en bij nieuwe ontwikkeling van de primaire en secundaire processen krijgt in de richtlijn aandacht, zij het beperkter dan die van de IT kolom. Als direct uitvloeisel van de Diginotar en Lektober affaires zijn door Logius richtlijnen geformuleerd die nu dienen als basis voor de DigiD-assessments. Deze richtlijnen zijn afgeleid van de NEN norm die ook onderliggend zijn aan de Basisrichtlijnen. Daarnaast bestaan in het provinciaal domein meerdere normenstelsels voor het voldoen aan informatiebeveiliging. Gedeeltelijk zijn deze normen specifiek toegesneden op specifieke informatiestromen; zij zullen ook een stevige overlap kennen met de basisrichtlijn en net als bij gemeenten wordt sterk aangedrongen op uniformering van normenstelsel.

Programmering en taskforce

Bij provincies staat PETRA (en daarmee ook de Baseline Informatiebeveiliging Provincies) op de agenda van het SIO, strategisch ICT Overleg, dat wordt aangestuurd door het overleg van de directeuren Middelen. In dit SIO zitten de hoofden I&A van alle provincies, of hun vervanger. Het CIBO over informatieveiligheid valt daaronder.

De doelstelling kan zijn in 2013 nieuwe normenstelsels zoals de BIR en Baseline Informatiebeveiliging Provincies verder te integreren en in te zetten op implementatie bij alle provincies.

De werking van het normenstelsel moet goed gemeten worden. Het is vooral van belang dat de inzet van een meetinstrument past binnen de kaders van een samenhangend normenstelsel dat met een slimme inzet van self-assessment, peer-review en externe visitatie leidt tot een zichzelf regulerend systeem van informatiebeveiliging binnen het gemeentelijk domein. Aanvullend op de stroomlijning van normenstelsel kan de taskforce het CIBO ondersteunen om het auditraamwerk voor gemeenten te stroomlijnen en toe te werken naar een maximale efficiency bij het inzetten van respectievelijk self-assessments; peer reviews samenhangend externe auditinstrumenten.

Verankering per organisatie

Implementatie en toepassing van de Baseline Informatiebeveiliging Provincies betekent dat in principe betekent aan de eisen van informatieveiligheid kan zijn voldaan. De verankering van informatieveiligheid in de provinciale organisatie is vanuit dat oogpunt nog zeer verschillend. Het meest voortgeschreden lijkt de situatie in provincies waar een CIO stelsel goed wekt. Precieze informatie per provincie hierover is op dit moment bij ons nog niet aanwezig. Maar ook in meer

gunstige situaties zal het nog enige tijd duren voor sprake is van volledige implementatie van de Baseline. Het CIBO heeft op dit moment nog geen vergelijkbare opdracht als de IBD. Provincies zijn echter organisaties met een omvang die het mogelijk maakt ook meer zelfstandig en in afstemming tot goede implementatie van de Baseline te komen

De uitkomsten van het DigiD assessment is in principe een goed uitgangspunt om meer systematisch de probleemanalyse en veranderingsstrategie te starten Er is echter geen zicht op wanneer precies die DigiD assessment resultaten er zullen zijn.

Programmering en taskforce

Naast bijvoorbeeld concrete activiteiten van inzake preventie en respons is er vooral ook behoefte aan het uitrollen en implementatie van de BIG. De middelen en methoden kunnen provincies met SIO/CIBO systematisch vorm geven en zelf verankeren.. De huidige plannen voorzien niet in zo'n uitrol gericht op een systematische implementatie van de BIG per organisatie. De wijze waarop de organisaties invulling moeten geven is aan zelfregulerend vermogen is nog niet systematisch uitgewerkt, althans niet op niveau van SIO/CIBO. Het niet systematisch gepland zijn van de voltooiing van de DigiD-assessments maakt een planning op provinciaal niveau ook moeilijk.

De taskforce kan behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de Baseline Informatiebeveiliging Provincies en het koppelen aan de uitkomsten van de DigiD-assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learn and share' tussen provincies die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieën en implementatie. Zie bij verandertraject.

De taskforce kan het CIBO ondersteunen bij het regelen van het domein voor relevante handleidingen, instructies, oefenmateriaal etc. Steeds in nauwe samenhang met de doelstellingen van de IBD, met tegelijkertijd de focus op het realiseren van een systeem van zelfregulering.

De verankering in het domein

De rol van SIO/CIBO is maar deels vergelijkbaar met die van KING/IBD, dat een aan de brancheorganisatie gekoppelde opdracht heeft die ook een financieringsbasis kent.In termen van implementatie van de baseline informatiebeveiliging kan SIO/CIBO in de toekomst zeker een rol vervullen, maar de vraag is of die rol nu voldoende verankerd is. Indien een duidelijke opdracht en financiering tot stand zou komen dan zou in de samenwerking tussen CIBO, IBD, NCSC, Logius en andere stelselvoorzieningen een goed functionerend stelsel kunnen ontstaan voor technische voorzieningen en de implementatie daarvan. Een andere mogelijkheid is een orgaan als de IBD gelieerd aan het koepelniveau.

Als het gaat om de bredere scope van de inrichting van zo'n stelsel zal ook IPO een rol moeten vervullen en zal op een aantal punten nader gesprek moeten plaats vinden, met name ook inzake externe visitaties en eventueel vellen van openbare oordelen en mogelijke maatregelen uitlokken.

Programmering en taskforce

De taskforce kan de dialoog binnen het provinciaal domein stimuleren over de vormgeving aan zelfregulering. De taskforce zou met de IPO en SIO/CIBO en overleg directeuren middelen met name ook bestuurders en statenleden kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie en de rol van de staten daarin benadrukken, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten.

De taskforce zou kunnen bijdragen aan het gesprek over en de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.

De verankering in ketens

Het Rijk is regisseur van een belangrijke ketens, zoals die van identiteit (GBA, paspoort etc.), of van de justitiële ketens zoals rechtsgang, vreemdelingen. Provincies zijn in een beperkter aantal ketens betrokken dan gemeenten. Ook op veel van die ketens is nog geen coördinerende verantwoordelijkheid voor informatieveiligheid geregeld. Wel zijn stukken van informatieveiligheid geregeld in allerlei auditverplichtingen. Nader overleg moet plaats vinden waar die coördinerende verantwoordelijkheid te beleggen en hoe die auditverplichtingen in de Baseline Informatiebeveiliging voor Provincies te integreren.

Programmering en taskforce

Het gaan werken aan keten informatieveiligheid heeft een hoge prioriteit. Samen met de taskforce en samen met andere domeinen is inrichting van een ketenregime op een aantal prioritaire ketens, een voor de hand liggende activiteit die nu onvoldoende tot stand komt (Wellicht heeft het Rijk hier een dringender rol). Er loopt onderzoek naar de eisen te stellen aan de SUWI keten; daarop wachten is niet noodzakelijk. De resultaten zullen liggen in termen van welke eisen te stellen aan een keten.

Gebruik landelijke voorzieningen

Het NCSC is het landelijke samenwerkingsplatform voor expertise en advies alsmede respons en crisisbeheering op het gebied van ICT-veiligheid. Het NCSC vervult daarbij tevens een rol als CERT (Computer Emergency Response Team), met als primaire doelgroepen de Rijksoverheid en vitale organisaties. Andere overheden, bedrijfsleven en de burger zijn secundaire doelgroepen. Het NCSC monitort constant bronnen en detecteert bedreigingen op de informatievoorziening, geeft waar nodig aanwijzingen om de betreffende bedreigingen te weerstaan en is in het uiterste geval verantwoordelijk voor operationele coördinatie tijdens een crisisorganisatie. In die zin versterkt het NCSC de weerbaarheid van de departmentale en vitale informatievoorziening. De IBD (met gemeenten juist als primaire doelgroep) gaat in samenwerking met het NCSC voor het gemeentelijk domein de preventie en respons versterken. Zij volgt de analyses en richtlijnen van NCSC een draagt zorg voor de (crisis) communicatie in samenhang met de NCSC informatievoorziening.

Programmering en samenwerking taskforce

Een systematische samenwerking met NCSC moet verder vorm krijgen.

De taskforce kan het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein..

Leren

De aandacht voor het onderwerp informatiebeveiliging binnen gemeenten is zoals gesteld wisselend van aard. DigiNotar en Lektober hebben het bewustzijn voor het thema aangewakkerd. Dat is versterkt door allerlei communicatie. Dit bewustzijn is binnen de ICT kolom sterker en in veel mindere mate binnen de gebruikskolom. Bestaande auditinitiatieven worden meer ingezet als toets achteraf, dan als middel om informatiebeveiliging als structureel onderwerp op de agenda te zetten. Er lijkt nog geen algemene, systematische gerichtheid op oefenen, dan wel anderszins duurzaam de gerichtheid op informatieveiligheid te bewerkstelligen.

Programmering en taskforce

Met erkenning van alle verscheidenheid en alle aandacht die er al geweest is en nog is, lijkt een systematische aandacht voor leren van bestuurders en top management nog wenselijk, hoewel nadere analyse vereist is. Dat moet niet meer door algemene bijeenkomsten, maar nauw gekoppeld aan de verdere ontwikkeling naar zelfregulering. De taskforce zou (in nauwe samenwerking met het CIBO) een dergelijk ondersteunend programma moeten faciliteren. Daarbij is een gefaseerde aanpak denkbaar die allereerst inzet op bewustwording en probleemanalyse, vervolgens een planmatige aanpak van verandering ondersteunt en tot slot afsluit met een werkende systematiek van zelfregulerende visitatie en auditinstrumenten. In een bijlage hebben we een mogelijke invulling van een dergelijk meerjarig programma gemaakt. Hierna is bij verandertrajecten aangegeven dat gegeven de problematiek en veronderstelling van diversiteit van provinciale organisaties, maar ook de eigen kracht van deze organisaties een meer pragmatische aanpak nodig is. De fasering is echter uiterst nuttig als referentiepunt om te toetsen of doordacht gericht op leren en verankeren te werk wordt gegaan.

In praktische zin zijn er rond het vergroten van bewustwording al een aantal initiatieven van NCSC tegengekomen die erop is gericht om awareness te vergroten. Ook binnen CIP zijn interessante aanzetten gegeven om invulling te geven aan bewustzijn rond informatiebeveiliging. Ook deze aanzetten kunnen in deze programmering specifiek voor provincies een plaats krijgen.

Binnen het departement BZK wordt geëxperimenteerd met een digivaardigheidsbewijs. Het betreft een korte training van eindgebruikers door middel van een e-leanring omgeving. De training wordt bij positief resultaat afgesloten met een certificaat. Het experiment is overgenomen van de Rabobank waar al langer met een dergelijk instrument getracht wordt informatiebeveiligingsbewustzijn te vergroten. Ook een dergelijk instrument kan in de gemeentelijk programmering een plaats krijgen.

Op het terrein van leren heeft het provinciale domein ingezet op een leergang informatiebeveiliging (10 dagen), die door alle leden van het CIBO is gevolgd.

Voortgang verandertraject

De stap naar een zelfregulerend systeem zal ook binnen provincies nog tweede orde verandering en tweede orde leren vragen, hoewel zoals gesteld de situatie per provinciale organisatie verschillend is en de omvang van de organisaties het varen op eigen kracht goed mogelijk maakt. In

de auditing zou de aanwezigheid van probleemanalyse, plan en implementatie systematisch aan de orde moeten komen om de voortgang naar informatieveiligheid te meten.

Programmering en taskforce

Het veranderingstraject vereist een pragmatische insteek, waarin de verschillende lopende processen en de verschillen die er tussen de organisaties zijn op een creatieve manier inzet zijn. Vanuit de DigiD-assessments lijkt een modelaanpak geëigend van probleemanalyse, naar veranderstrategie, naar implementatie en naar review zoals die in de bijlage omschreven is. Die is in die vorm niet goed uitvoerbaar gezien het verschil tussen organisaties (sommigen zijn al in de fase naar eerste orde leren) en door de verschillende stromen van interventies die er lopen. Verbeteringen op terrein van response moeten snel en kunnen niet wachten. De onzekere planning van de DigiD-assessments leiden eveneens maatwerk in de voortgang naar een zelfregulerend stelsel. Hiervoor is al aangegeven dat de start van een systematisch verandertraject zou kunnen liggen bij de systematische bespreking van de uitkomsten van de DigiD-assessments. In het algemeen zal aandacht bestaan voor bestaande instrumenten, goede praktijken en de uitwisseling daarvan.

Van groot belang wordt de voortgang in het proces van verandering te kunnen meten. Het zal zaak zijn het proces van verankering en leren ook in PETRA te doen opnemen. Zie voor de meting dan verder hiervoor bij normering.

Recapitulerend Provincies en Taskforce

De taskforce kan naar steekwoord op de volgende kunnen bijdragen aan de programmering van het provinciaal domein naar verplichtende zelfregulering.

- De taskforce kan het proces van ontwikkeling van de Baseline Informatiebeveiliging Provincies faciliteren en daardoor versnellen.
- Het kan dit proces ook ondersteunen door de programmering van bewustwordings- en kennissessies rond de richtlijn.
- Aanvullend op de stroomlijning van normenstelsel kan de taskforce ondersteunen om het auditraamwerk te stroomlijnen en toe te werken naar een maximale efficiency bij het inzetten van respectievelijk self-assessments; peer reviews samenhangend externe auditinstrumenten.
- Het ontwikkelen van voor het domein relevante handleidingen; instructies; oefenmateriaal etc.
- De taskforce kan SIO en CIBO behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de Baseline Informatiebeveiliging Provincies en het koppelen aan de uitkomsten van de DigiD-assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learn and share' overleg met provincies die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieën en implementatie. Zie bij verandertraject.

- Het experiment met een digivaardigheidsbewijs, zoals uitgevoerd bij het ministerie van BZK doorontwikkelen voor provincies.
- De taskforce kan de dialoog binnen het provinciaal domein bevorderen over de vormgeving aan zelfregulering. De taskforce zou met IPO met name ook bestuurders kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie en de rol van de raden daarin benadrukken, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten.
- De taskforce zou kunnen bijdragen aan het gesprek over en de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.
- De taskforce zou met spoed op een aantal ketens een initiatief kunnen nemen met betrokken partijen over hoe de regulering van de informatieveiligheid in te richten.
- De taskforce kan in het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein. Ook een dergelijk instrument kan in de gemeentelijk programmering een plaats krijgen.
- Op het terrein van leren ligt er al een uitgewerkte en gebruikte leergang informatiebeveiliging. Deze zou, in overleg met IBD en NCSC, opgewaardeerd kunnen worden naar de nieuwe situatie, en eventueel ook bij de IBD gebruikt kunnen worden.

Een en ander kan resulteren in de volgende producten waar de taskforce een bijdrage aan levert. Let wel, dit is slechts een proeve die nadrukkelijk uitwerking behoeft met IPO en SIO.

Bijdragen aan producten in programmering provincies

• **Bijdrage taskforce aan programmering**	• Activiteiten taskforce; steeds gaat het om in afstemming met SIO leveren van 'bijdragen aan'; SIO heeft normaliter 'the lead'.
• De taskforce kan het proces van ontwikkeling van de Baseline Informatiebeveiliging Provincies faciliteren en daardoor versnellen.	• Vaststellen status • Overleg met IPO over hoe versnelling te realiseren • Ontwikkelen communicatiestrategie rond PETRA • Ontwikkelen stappenplan implementatie PETRA •
• Het kan dit proces ook ondersteunen door de programmering van bewustwordings- en kennissessies rond de richtlijn	• Ontwikkelen bewustwordingssessie rond PETRA en belang informatiebeveiliging • Organisatie Roadshow rond PETRA • Externe sprekers buiten overheidsdomein • Confrontatieworkshops • Wat gaat U morgen doen rond beveiliging •
• Aanvullend op de stroomlijning van normenstelsel kan de taskforce ondersteunen om het auditraamwerk te stroomlijnen en toe te werken naar een maximale	• Inventarisatie normenstelsels • Onderzoek harmonisatie normenstelsels

efficiency bij het inzetten van respectievelijk self-assessments; peer reviews samenhangend externe auditinstrumenten.	• Harmonisatie normenstelsels in lijn brengen met Petra • Opzetten self-assessment rond geharmoniseerd normenkader • Organisatie periodieke peer review rond geharmoniseerd normenkader • Toetsen van auditconsequenties als gevolg van introductie BIG self-assessments; peer reviews: • Bij BPR/VROM
• Het ontwikkelen van voor het domein relevante handleidingen; instructies; oefenmateriaal etc.	• Ontwikkeling handreiking informatiebeveiliging • Organiseren gecertificeerde marktplaats training informatiebeveiliging • Ontwikkeling oefenstrategie informatiebeveiliging ism veiligheidsregio's en Certs • Organiseren van een peer to peer netwerk rond informatiebeveiliging voor bestuurders en secretarissen.
• De taskforce kan SIO en CIBO behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de Baseline Informatiebeveiliging Provincies en het koppelen aan de uitkomsten van de DigiD-assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learn and share' overleg met provincies die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieën en implementatie. Zie bij verandertraject.	• Ontwikkeling monitoring voortgang realisatie Petra. Hier goed nota nemen van lessons learned van Operatie NUP en BRP. • Aanpak samen ontwikkelen met vergelijkbare aanpak in gemeentelijk domein.
• Het experiment met een digivaardigheidsbewijs, zoals uitgevoerd bij het ministerie van BZK doorontwikkelen voor provincies.	• Omwerken van het instrumentarium voor gemeentelijke omgevingen • Toesnijden op normenkaders BIG • Organiseren van beheer en beschikbaarheid tooling • Opzetten communicatie rond deze tooling tbv HRM kanaal
• De taskforce kan de dialoog binnen het provinciaal domein bevorderen over de vormgeving aan zelfregulering. De taskforce zou met IPO met name ook bestuurders kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie en de rol vande raden daarin benadrukken, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten.	• Plaatsen van instrumenten self-assessements; peer review en externe audits in een systematiek van gecontroleerde zelfregulering. • Benoemen van een aanspreekpunt voor inregeling van de systematiek. Dit zal in nauwe samenspraak met IPO moeten worden belegd • Organiseren beveiligde toegankelijkheid van de resultaten
• De taskforce zou kunnen bijdragen aan het gesprek over en de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.	• Zie voorgaand punt

• De taskforce zou met spoed op een aantal ketens een initiatief kunnen nemen met betrokken partijen over hoe de regulering van de informatieveiligheid in te richten..	• Zie voorgaand punt, maar dan in relatie tot ketens. Concreet minimaal het gesprek met SUWIketen; Veiligheisketen
• De taskforce kan in het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein. Ook een dergelijk instrument kan in de gemeentelijk programmering een plaats krijgen.	• Hier aansluiten bij acties binnen het gemeentelijk domein van KING op het gebied van convenantvorming. • Gebruik maken van ervaringen bij NSCS rond inregeling opdrachtgever/opdrachtnemerschap en beveiliging • Mogelijk ontwikkeling van een DIID testplaform
• Op het terrein van leren ligt er al een uitgewerkte en gebruikte leergang informatiebeveiliging. Deze zou, in overleg met IBD en NCSC, opgewaardeerd kunnen worden naar de nieuwe situatie, en eventueel ook bij de Provincies gebruikt kunnen worden.	• Is al eerder benoemd

8. Programmering Waterschap en samenwerking met de taskforce

Soortgelijke situatie

Bij de waterschappen lijkt de situatie veel op die bij provincies en gemeenten.

- Ook hier hebben de ontwikkelingen tot een verhoogde 'awareness' geleid.
- Ook bij de waterschappen is het voornemen te komen tot een Baseline Informatiebeveiliging Waterschappen en is de uitrol topprioriteit, al is de situatie op dit punt minder in een afrondend stadium dan bij gemeente, provincie en Rijk.
- Er is verschil per waterschapsorganisatie in de mate waarin informatieveiligheid verankerd is in de organisatie en de systematische gerichtheid van bestuur en topmanagement op informatieveiligheid.
- Het Waterschapshuis kan in principe een soortgelijke rol vervullen als SIO/CISO bij de provincies in termen van faciliteren van ontwikkelingen naar voorzieningen en implementeren daarvan, maar daarvoor moeten nog systematischer afspraken tot stand komen.
- Ook hier is samenwerking met de IBD een (complementaire) optie.
- Ook hier zal de ontwikkeling naar een verplichtende zelfregulering op stelsel niveau, met eventueel ook externe visitaties en vormen van oordelen een rol vragen van de Unie van Waterschappen.
- Ook hier is verankering in de ketens een vraag, waarbij bij de waterschappen op de primaire processen grote aandacht is voor de informatieveiligheid. Op een wezenlijke keten als die van water zal verankeren van deinformatieveiligheid over de domeinen heen nog de nodige aandacht vragen.
- Het leren kan dus op een aantal punten nader vorm krijgen en ook hier kunnen de uitkomsten van de DigiD-assessments een aangrijpingspunt zijn het proces van leren en verankering nader te structureren naar probleemanalyse, veranderingsstrategie, implementatie en review.
- Ook hier zal een pragmatisch proces van leren en implementeren van zelfregulering vereist zijn omdat de processen van probleemanalyse, veranderingsstrategie en implementatie door elkaar lopen en omdat de situatie per organisatie verschillend is.

Per saldo is het voorstel hier dan ook een programmering en soortgelijke samenwerking met de taskforce als bij gemeenten en provincie.

De taskforce kan naar steekwoord op de volgende kunnen bijdragen aan de programmering van het provinciaal domein naar verplichtende zelfregulering.

- De taskforce kan het proces van ontwikkeling van de baseline informatiebeveiliging waterschappen faciliteren en daardoor versnellen.
- Het kan dit proces ook ondersteunen door de programmering van bewustwordings- en kennissessies rond de richtlijn.

- Aanvullend op de stroomlijning van normenstelsel kan de taskforce ondersteunen om het auditraamwerk te stroomlijnen en toe te werken naar een maximale efficiency bij het inzetten van respectievelijk self-assessments; peer reviews samenhangend externe auditinstrumenten.
- Het ontwikkelen van voor het domein relevante handleidingen; instructies; oefenmateriaal etc.
- De taskforce kan het waterschapshuis behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de baseline en het koppelen aan de uitkomsten van de DigiD-assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learn share' overleg met provincies die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieën en implementatie. Zie bij verandertraject.
- Het experiment met een digivaardigheidsbewijs zoals bij BZK gestart verder ondersteunen.
- De taskforce kan de dialoog binnen het waterschapsdomein bevorderen over de vormgeving aan zelfregulering. De taskforce zou met de Unie van waterschappen met name ook het bestuurlijk niveau kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten.
- De taskforce zou kunnen bijdragen aan het gesprek over en de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.
- De taskforce zou met spoed op een aantal ketens een initiatief kunnen nemen met betrokken partijen over hoe de regulering van de informatieveiligheid in te richten.
- De taskforce kan in het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein. Ook een dergelijk instrument kan in de gemeentelijk programmering een plaats krijgen.
- Op het terrein van leren is nog weinig binnen het domein voorhanden; Het doen ontwikkelen van opleidingsfaciliteiten en cursusaanbod kan een activiteit van de taskforce zijn in afstemming met IBD en afnemers.

Een en ander kan resulteren in de volgende producten waar de taskforce een bijdrage aan levert. Let wel, dit is slechts een proeve die nadrukkelijk uitwerking behoeft met waterschappen

Bijdragen aan producten in programmering waterschappen

• De taskforce kan het proces van ontwikkeling van de Baseline Informatiebeveiliging Waterschappen faciliteren en daardoor versnellen.	• Vaststellen status • Overleg met Waterschapshuis over hoe versnelling te realiseren • Ontwikkelen communicatiestrategie rond Richtlijn informatiebeveiliging ism Waterschapshuis • Ontwikkelen stappenplan implementatie Richtlijn informatiebeveiliging in

	samenwerking met Waterschapshuis •
• Het kan dit proces ook ondersteunen door de programmering van bewustwordings- en kennissessies rond de richtlijn	• Ontwikkelen bewustwordingssessie rond belang informatiebeveiliging • Organisatie Roadshow rond richtlijn informatiebeveiliging • Externe sprekers buiten overheidsdomein • Confrontatieworkshops • Wat gaat U morgen doen rond beveiliging •
• Aanvullend op de stroomlijning van normenstelsel kan de taskforce ondersteunen om het auditraamwerk te stroomlijnen en toe te werken naar een maximale efficiency bij het inzetten van respectievelijk self-assessments; peer reviews samenhangend externe auditinstrumenten.	• Inventarisatie normenstelsels • Onderzoek harmonisatie normenstelsels • Harmonisatie normenstelsels in lijn brengen met informatiebeveiliging waterschappen • Opzetten self-assessment rond geharmoniseerd normenkader • Organisatie periodieke peer review rond geharmoniseerd normenkader • Toetsen van auditconsequenties als gevolg van introductie informatierichtlijn self-assessments; peer reviews: • Bij BPR/VROM • Interne Auditors • Externe auditors •
• Het ontwikkelen van voor het domein relevante handleidingen; instructies; oefenmateriaal etc.	• Ontwikkeling handreiking informatiebeveiliging • Organiseren gecertificeerde marktplaats training informatiebeveiliging • Ontwikkeling oefenstrategie informatiebeveiliging ism veiligheidsregio's en Certs • Organiseren van een peer to peer netwerk rond informatiebeveiliging voor bestuurders en secretarissen.
• De taskforce kan behulpzaam zijn met plannen van een systematische voortgang van de implementatie van de Baseline Informatiebeveiliging Provincies en het koppelen aan de uitkomsten van de DigiD-assessments. Met name is te denken aan het bevorderen van het afronden van het DigiD assessment, het systematisch organiseren van 'learn and share' overleg met provincies die het assessment voltooid hebben, het aanreiken van verbredende quick scans (DigiD gaat over web applicaties) voor het maken van bredere probleemanalyses, instrumentarium voor veranderstrategieën en implementatie. Zie bij verandertraject.	• Ontwikkeling monitoring voortgang realisatie beveiligingsrichtlijn. Hier goed nota nemen van lessons learned van Operatie NUP en BRP. • Aanpak samen ontwikkelen met vergelijkbare aanpak in gemeentelijk domein.
• Het experiment met een digivaardigheidsbewijs, zoals uitgevoerd bij het ministerie van BZK doorontwikkelen voor provincies.	• Omwerken van het instrumentarium voor gemeentelijke omgevingen • Toesnijden op normenkaders • Organiseren van beheer en

	beschikbaarheid tooling • Opzetten communicatie rond deze tooling tbv HRM kanaal
• De taskforce kan de dialoog binnen het provinciaal domein bevorderen over de vormgeving aan zelfregulering. De taskforce zou met WATERSCHAPSHUIS met name ook bestuurders kunnen betrekken bij deze ontwikkeling naar zelfregulering per organisatie en de rol vande raden daarin benadrukken, alsmede de noodzakelijke ontwikkelingen op domein en stelsel niveau kunnen toelichten.	• Plaatsen van instrumenten self-assessements; peer review en externe audits in een systematiek van gecontroleerde zelfregulering. • Benoemen van een aanspreekpunt voor inregeling van de systematiek. Dit zal in nauwe samenspraak met het waterschapshuis moeten worden belegd • Organiseren beveiligde toegankelijkheid van de resultaten
• De taskforce zou kunnen bijdragen aan het gesprek over en de ontwikkeling van mogelijke vormen van externe visitatie en de omgang met de uitkomsten daarvan.	• Zie voorgaand punt
• De taskforce zou met spoed op een aantal ketens een initiatief kunnen nemen met betrokken partijen over hoe de regulering van de informatieveiligheid in te richten..	• Zie voorgaand punt, maar dan in relatie tot ketens. Concreet minimaal het gesprek met SUWIketen; Veiligheisketen
• De taskforce kan in het leveranciersvraagstuk systematisch in beeld brengen. Hier ligt een eerste verantwoordelijkheid van BZK op landelijk niveau, maar het vraagstuk speelt in ieder domein. Ook een dergelijk instrument kan in de gemeentelijk programmering een plaats krijgen.	• Hier aansluiten bij acties binnen het gemeentelijk domein van KING op het gebied van convenantvorming. • Gebruik maken van ervaringen bij NSCS rond inregeling opdrachtgever/opdrachtnemerschap en beveiliging • Mogelijk ontwikkeling van een DIID testplaform
• Op het terrein van leren ligt er al een uitgewerkte en gebruikte leergang informatiebeveiliging. Deze zou, in overleg met IBD en NCSC, opgewaardeerd kunnen worden naar de nieuwe situatie, en eventueel ook bij de Provincies gebruikt kunnen worden.	• Is al eerder benoemd

9. Programmering Rijken ZBO's en samenwerking met Taskforce

Een eerste toepassing van de zeven standaards op de situatie in het Rijk levert een globaal beeld, met mogelijke programmering en een mogelijke samenwerking met de taskforce.

De Baseline Informatiebeveiliging Rijk (BIR)

In het interdepartementale CIO overleg is in september de basisrichtlijn informatiebeveiliging Rijk (BIR) bekrachtigd. De definitieve versie daarvan komt binnenkort beschikbaar. De basisrichtlijn is gebaseerd op de NEN 27002; code voor informatiebeveiliging. De BIR vervangt de komende periode de implementatie van voor departementen specifiek ontwikkelde richtlijnen. De BIR richt zich voornamelijk op het borgen van informatieveiligheid in de beheerfase van informatiesystemen. Deze aandacht voor informatieveiligheid zou met de implementatie van de richtlijn in ieder geval binnen de IT kolom afdoende geregeld zijn. De aandacht voor informatiebeveiliging in de gebruikskolom en bij nieuwe ontwikkeling van de primaire en secundaire processen krijgt in de richtlijn aandacht, zij het beperkter dan die van de IT kolom.

Programmering en taskforce

De spoedige implementatie van de BIR is topprioriteit, ook als voorbeeld voor andere domeinen. Er moet dus nu geen nieuw gesprek over de BIR worden gevoerd. De taskforce kan over bijvoorbeeld een jaar wel bijdragen aan een gesprek over de verschillende domeinen heen of en hoe de gebruikerskolom/nieuwe ontwikkelingen scherper aandacht moeten krijgen. Zo'n gesprek is gezien de gelijksoortigheid van de richtlijnen van de verschillende domeinen relevant.

Verankering per organisatie

Informatiebeveiliging staat op de agenda van de departementale CIO's. Er is per departement en regime voor reguliere toetsing en rapportage bij de accountantscontrole. De aandacht voor response en herstel lijkt in het algemeen al beter geborgd dan voor pro-actie en preventie. Hier lijkt vooral sprake van de noodzaak van cyclisch aandacht blijven besteden aan eerste orde vernederen.

Van groot belang is wel dat daar routines ontstaan die scherp houden.Het sluitstuk van de implementatie van de BIR is een daarop gerichte audit. Een dergelijke audit lijkt echter dermate omvangrijk dat hiermee hetzij een lange doorlooptijd gemoeid is (meerdere jaren) dan wel hoge kosten. Geen van beide opties lijkt wenselijk. De departementale CIO's zoeken naar wegen om met behulp van peer-reviews en self-assessments te komen tot een andere vorm waaruit de voortgang, dan wel realisatie van die implementatie blijkt.

Daarnaast speelt ook binnen de departementale omgeving de behoefte om bestaande audit en assessments te stroomlijnen. Mogelijk dat een meer gestroomlijnde audit aanpak bijdraagt aan een voor zelfregulering.

Programmering en taskforce

Het nader verankeren van de BIR per organisatie vindt de komende periode wel plaats en sluit aan bij lopende processen. Bij het vormgeven van een relevant stelsel van audit; self-assessement en peer-review kan de taskforce een goede bijdrage leveren aan zelfregulering binnen departementen.

De verankering in het domein

Met DGOBR, CIO stelsel is de organisatorische verankering van sturing op domein goed geregeld. Inhoudelijk lijkt met name de toets op departementale ontwikkelingen door bijvoorbeeld externe visitatie eens in de vier jaar nog niet geregeld.

Programmering en taskforce

- Ontwikkelen van een lange termijn visitatie methodiek
- Bijdragen aan externe toets/visitatie

De verankering in ketens

Het Rijk is regisseur van een belangrijke ketens, zoals die van identiteit (GBA, paspoort etc.), of van de justitiële ketens zoals rechtsgang, vreemdelingen. Op veel van die ketens is nog geen coördinerende verantwoordelijkheid voor informatieveiligheid geregeld. Wel zijn stukken van informatieveiligheid geregeld in allerlei auditverplichtingen. Dit leidt tot een bont geheel van verplichtingen voor keten (netwerk)partners.

Programmering en taskforce

Het gaan werken aan keten informatieveiligheid heeft een hoge prioriteit. Samen met de taskforce is inrichting van een ketenregime op een aantal prioritaire ketens, samen met andere domeinen een voor de hand liggende die nu onvoldoende tot stand komt. Er loopt onderzoek naar de eisen te stellen aan de SUWI keten; daarop wachten is niet noodzakelijk. De resultaten zullen liggen in termen van welke eisen te stellen aan een keten.

Gebruik landelijke voorzieningen

Het NCSC is het landelijke samenwerkingsplatform voor expertise en advies alsmede respons en crisisbeheering op het gebied van ICT-veiligheid. Het NCSC vervult daarbij tevens een rol als CERT (Computer Emergency Response Team), met als primaire doelgroepen de Rijksoverheid en vitale organisaties. Andere overheden, bedrijfsleven en de burger zijn secundaire doelgroepen. Het NCSC monitort constant bronnen en detecteert bedreigingen op de informatievoorziening, geeft waar nodig aanwijzingen om de betreffende bedreigingen te weerstaan en is in het uiterste geval verantwoordelijk voor operationele coördinatie tijdens een crisisorganisatie. In die zin versterkt het NCSC de weerbaarheid van de departmentale en vitale informatievoorziening. De IBD (met gemeenten juist als primaire doelgroep) gaat in samenwerking met het NCSC voor het gemeentelijk domein de preventie en respons versterken. Zij volgt de analyses en richtlijnen van NCSC een draagt zorg voor de (crisis) communicatie in samenhang met de NCSC informatievoorziening.

Grote hiaten in wat voor de vijf fasen van de veiligheidsketen nodig is, lijken er op dit moment niet te zijn vanuit wat van landelijke organisaties verwacht kan worden. Wel zijn er vragen zoals van betrouwbaarheid leveranciers, maar dit betreft meer algemene stelselvragen. Zie hierna bij stelsel.

Leren

Er is Rijksbreed aandacht geweest voor 'awareness' van het topmanagement. In gesprekken komt erkenning van het belang duidelijk tot uitdrukking. De mate waarin die awareness ook duurzaam is en leidt tot een actieve gerichtheid op informatieveiligheid verschilt mede afhankelijk van de mate waarin risico's aanwezig zijn. Daar waar die risico's groter zijn en meer ervaren worden is de actieve gerichtheid op informatieveiligheid intenser volgens een aantal gesprekspartners

Het lijkt dat de managementlaag niet algemeen voldoende aandacht besteedt aan risicoanalyse die samenhangt met het gebruik van gedigitaliseerde informatie. Het onderwerp leeft onvoldoende op DG/SG niveau. Dit geldt ook voor de aandacht die aan informatiebeveiliging wordt gesteld bij het initiëren van vernieuwingsprojecten. Bij het versterken van opdrachten daartoe vindt volgens de gesprekspartners niet altijd voldoende risicoanalyse plaats.

De aandacht voor informatiekundige vraagstukken voor de departementale managementlaag is belegd binnen ABD APP. In deze opleidingen komen de PIOFAH aspecten aan bod. Relatief gezien lijkt de aandacht voor informatiekundige onderwerpen beperkt te zijn. Een module die zich richt op risicomanagement en informatiebeveiliging ontbreekt.

Binnen het departement BZK wordt geëxperimenteerd met een digivaardigheidsbewijs. Het betreft een korte training van eindgebruikers door middel van een e-leanring omgeving. De training wordt bij positief resultaat afgesloten met een certificaat. Het experiment is overgenomen van de Rabobank waar al langer met een dergelijk instrument getracht wordt informatiebeveiligingsbewustzijn te vergroten.

Programmering en taskforce

De rol van de taskforce zou zich kunnen richten op het in samenwerking met ABD APP ontwikkelen van een leermodule voor management dat zich specifiek richt op risicomanagement en informatiebeveiliging en die ook bruikbaar is voor managementlagen in andere domeinen

In het uitbouwen van haar rol ontwikkelt NCSC producten op het gebied van security awareness. De taskforce zal tussen ADB APP en NCSC een coördinerende rol vervullen bij het identificeren van noodzakelijk opleidings- en trainingsmateriaal, de inhoud daarvan en tenslotte zorg dragen dat deze relevante inhoud breed binnen de overheid verspreid en gebruikt kan worden. Waar nodig kan de taskforce inzetten op de ontwikkeling van materiaal.

Voortgang verandertraject

Bij het Rijk is voor het domein een traject van verandering. De belangrijkste punten van mogelijke aanscherping zijn hiervoor aangegeven. Dat geldt ook voor de departementen zover wij in de korte tijd hebben kunnen nagaan; er wordt gewerkt aan probleemanalyse en implementatie van verbetering; hoe compleet dat is, blijft moeilijk na te gaan. Op Rijksniveau is dan ook vooral nodig dat de huidige ontwikkeling vanuit tweede orde verandering naar eerste orde verandering voortgang blijft vinden. In de auditing zou de aanwezigheid van probleemanalyse, plan en implementatie dan ook systematisch aan de orde moeten komen. Het Rijk kan hier, bijvoorbeeld samen met G4 en andere gemeenten wellicht 'goede voorbeelden' leveren.

Programmering en taskforce

De voortgang van de verbetering zal in de reguliere cyclus verankering vinden waar op die voortgang wel toetsing moet plaatsvinden. De taskforce kan samen met CIO stelsel 'goede voorbeelden selecteren'.

De situatie bij ZBO's

De situatie bij ZBO's en uitvoeringsorganisaties is deels vergelijkbaar met de situatie bij het Rijk, zij het dat de mate van implementatie Een groot verschil is dat er geen centrale regulerende instantie voor de laag ZBO's is, met dien verstande dat het regime compacte Rijksdienst ook voor ZBO's moet gelden en dat per ZBO een moederdepartement vaak nog een toezichthoudende rol vervult. De Manifestgroep bundelt wel steeds meer organisaties, maar is niet een formele brancheorganisatie . De wijze waarop verplichtende zelfregulering op stelselniveau vorm krijgt zal dan ook nader overleg vereisen. Daarvoor zijn verschillende mogelijkheden van formele koppeling aan moederdepartementen of DG Rijk tot een regulerende rol vanuit de Manifestgroep. Deze varianten sluiten elkaar ook niet uit; stelselverantwoordelijkheid is er hoe dan ook voor het Rijk

Het idee is om de programmering en samenwerking in afstemming met die van het Rijk te doen vormgeven in nauw overleg met CIP en Manifestgroep.

De Baseline Informatiebeveiliging

Voor ZBO's en agentschappen geldt dat zij de daar belegde uitvoeringstaak in principe zelfstandig uitvoeren; echter binnen de kaders die daaromtrent door departementen zijn gesteld. In een aantal gevallen betekent dit dat uitvoeringsorganisaties zich moeten houden aan de BIR. Voor anderen geldt dat een dergelijke verplichting minder dwingend is; echter gegeven het feit dat ook zij gehouden zijn aan de 'pas toe of leg uit' lijst van het Forum standaardisatie, zijn ook zij gehouden aan de NEN norm 27002. Het wordt ons duidelijk dat de toepassing van deze norm mogelijk niet overal is doorgevoerd. De implementatie zal dan ook afhangen van de specifieke situatie per ZBO/uitvoeringsorganisatie.

Programmering taskforce

De programmering van de taskforce zal zich in eerste instantie richten op die ZBO's die niet direct aangesloten zijn op het ICCIO overleg. De aangesloten ZBO's volgens de richtlijn die geldt voor departementen. Voor niet aangesloten ZBO's is het van belang dat zij werk maken van de implementatie van de NEN richtlijn of de daarvan afgeleide BIR. Een dergelijk inventarisatie en stimulering kan samen met het CIP worden opgepakt.

Verankering per organisatie

Ook hier geldt dat verankering van de richtlijn uiteindelijk wordt aangetoond vanuit een daarop gerichte visitatie. Er is echter sprake van een groot aantal ZBO's met een diverse opdracht. De organisatie van audits/ self-assessments of peerreviews gericht op verankering is complexer dan de min of meer gelijkvormig te vormen groepen van de overige onderdelen van het overheidsdomein. Dit geldt ook voor de mogelijkheden om de normen die gelden voor de audits, te harmoniseren.

Programmering taskforce

De taksforce zal stimuleren dat de voor het departementale niveau ontwikkelde normenkader en daarvan afgeleide systematiek van audits/self-assessmentss worden vertaald naar een voor de Manifestgroep hanteerbare gereedschapskist. De vormgeving van normenkader/auditsystematiek voor specifieke ZBO's is echter maatwerk en niet vergelijkbaar met de activiteiten voor beleidsdepartementen; gemeenten, provincies en waterschappen. Gegeven de daar meer eenduidige organisatiedoelstelling is het daar beter mogelijk harmonisatie na te streven.

De verankering in het domein

Samen met de grote uitvoeringsorganisaties van het Rijk is vanuit het programma compacte Rijksdienst het CIP opgericht als kennisorganisatie, een soort shared servicecentrum, dat ook als aanspreekpunt voor het NCSC kan dienen en dat nu onder de Manifestgroep functioneert. Het kan een zelfde rol vervullen als SIO/CIBO bij provincies of waterschaphuis bij waterschappen.
De opzet van het CIP is echter gericht op een bottum-up en vrijwillige bijdrage van een veelheid van deelnemers (ook niet Manifestgroepdeelnemers). Een deel van de kennisinbreng wordt geleverd vanuit marktpartijen.

Programmering taskforce

Verheldering van de verhoudingen tussen CIP; NCSC en manifestpartijen staan op de respectievelijke agenda's. De rol van de taskforce kan hooguit zijn om de ontwikkeling te monitoren en waar nodig te stimuleren.

De verankering in ketens

Voor de ZBO's is de ketenpositie wezenlijk; veel ZBO's functioneren in ketens. Het Rijk is daarvan de regisseur. Op veel van die ketens is nog geen coördinerende verantwoordelijkheid voor informatieveiligheid geregeld. Wel zijn stukken van informatieveiligheid geregeld in allerlei auditverplichtingen. Dit leidt tot een bont geheel van verplichtingen voor keten (netwerk)partners.

Programmering en taskforce

Het gaan werken aan keten informatieveiligheid heeft een hoge prioriteit. Samen met de taskforce is inrichting van een ketenregime op een aantal prioritaire ketens, samen met andere domeinen een voor de hand liggende die nu onvoldoende tot stand komt. Er loopt onderzoek naar de eisen te stellen aan de SUWI keten; daarop wachten is niet noodzakelijk. De resultaten zullen liggen in termen van welke eisen te stellen aan een keten.

Gebruik landelijke voorzieningen

Het NCSC vult de rol van CERT (Cyber emergency en response team) in. Zij monitort constant bedreigingen op de informatievoorziening, geeft waar nodig aanwijzingen om de betreffende bedreigingen te weerstaan en is in het uiterste geval verantwoordelijk voor het opschalen van een crisisorganisatie. In die zin versterkt het NCSC de weerbaarheid van de departementale overheid rond informatiebeveiliging. Wil het CIP echter kunnen optreden als ketenpartij in de emergency en

respons keten onder aansturing van het NCSC, dan is het noodzakelijk dat minder vrijblijvende afspraken tussen manifestpartijen; het CIP en NCSC gemaakt worden.

Programmering taskforce

Een voor de taskforce belangrijke rol in dit domein is om de inmiddels door het CIP opgedane ervaringen rond kennisdeling adequaat kan inzetten bij de andere in de programmering betrokken partijen. Dit is uiteraard een proces van halen en brengen. Het CIP kan ook in de positie gebracht worden om kennis en ervaring uit andere sectoren in te brengen bij de aan CIP verbonden partijen. De taksforce kan dit proces actief stimuleren.

Leren

Er is Rijksbreed aandacht geweest voor 'awareness' van het topmanagement ook bij de ZBO's die moeten voldoen aan de departementale richtlijnen voor informatiebeveiliging. In gesprekken komt erkenning van het belang duidelijk tot uitdrukking. De mate waarin die awareness ook duurzaam is en leidt tot een actieve gerichtheid op informatieveiligheid verschilt mede afhankelijk van de mate waarin risico's aanwezig zijn. Daar waar die risico's groter zijn en meer ervaren worden is de actieve gerichtheid op informatieveiligheid intenser volgens een aantal gesprekspartners

Het lijkt dat de managementlaag niet algemeen voldoende aandacht besteedt aan risicoanalyse die samenhangt met het gebruik van gedigitaliseerde informatie. Het onderwerp leeft onvoldoende op DG/SG niveau. Dit geldt ook voor de aandacht die aan informatiebeveiliging wordt gesteld bij het initiëren van vernieuwingsprojecten. Bij het versterken van opdrachten daartoe vindt volgens de gesprekspartners niet altijd voldoende risicoanalyse plaats.

De aandacht voor informatiekundige vraagstukken voor de departementale managementlaag belegd binnen ABD APP. In deze opleidingen komen de PIOFAH aspecten aan bod. Relatief gezien lijkt de aandacht voor informatiekundige onderwerpen beperkt te zijn. Een module die zich richt op risicomanagement en informatiebeveiliging ontbreekt.

Binnen het departement BZK wordt geëxperimenteerd met een digivaardigheidsbewijs. Het betreft een korte training van eindgebruikers door middel van een e-learning omgeving. De training wordt bij positief resultaat afgesloten met een certificaat. Het experiment is overgenomen van de Rabobank waar al langer met een dergelijk instrument getracht wordt informatiebeveiligingsbewustzijn te vergroten.

Programmering en taskforce

De rol van de taskforce zou zich kunnen richten op het in samenwerking met ABD APP ontwikkelen van een leermodule voor management dat zich specifiek richt op risicomanagement en informatiebeveiliging en die ook bruikbaar is voor managementlagen bij ZBO's en uitvoeringsorganisaties.

In het uitbouwen van haar rol ontwikkelt NCSC producten op het gebied van security awareness. De taskforce zal tussen ADB APP en NCSC een coördinerende rol vervullen bij het identificeren van noodzakelijk opleidings- en trainingsmateriaal, de inhoud daarvan en tenslotte zorg dragen dat deze

relevante inhoud breed binnen de overheid verspreid en gebruikt kan worden. Waar nodig kan de taskforce inzetten op de ontwikkeling van materiaal.

Ook het CIP beschikt gegeven haar doelstelling over de mogelijkheden om leervraagstukken vorm te geven. Vanuit haar doelstelling organiseert zij conferenties en ronde tafels rond diverse met beveiliging samenhangende vraagstukken. De taskforce kan stimuleren dat activiteiten van CIP, NCSC en ABD APP in samenhang worden gericht. Waar mogelijk kan zij actief relevant materiaal of conferenties organiseren aanvullend op de hier beschreven activiteiten.

Voortgang verandertraject

Het idee is om de programmering en samenwerking in afstemming met die van het Rijk te doen vormgeven in nauw overleg met CIP en Manifestgroep.

Recapitulerend Rijk en ZBO en Taskforce

In termen van het model van leren en verankeren is wat betreft het verankeren in de organisaties in toenemende mate sprake van eerste orde verandering. Met name het leren kan nog wel een tand dieper. Op domein niveau is sprake van tweede orde leren vanuit voorstel van externe visitatie en daar ook oordelen mee verbinden.

De concrete acties van de taskforce richten zich dan op:

- Gesprek organiseren over verschillende BIR/ZBO baseline op verschillende terreinen gericht op aandacht voor kolom primair proces en ontwikkeling.
- Bij het vormgeven van een relevant stelsel van audit; self-assessement en peer-review kan de taskforce een goede bijdrage leveren aan zelfregulering binnen departementen.
- Externe visitaties bijdragen aan leveren.
- Prioritaire ketenregimes ontwikkelen.
- Met het opleidingsprogramma ABD APP rond risicoanalyse en informatiebeveiliging module ontwikkelen.
- Selectie van 'goede voorbeelden" van verandertraject naar beheersing.
- Het stimuleren van hergebruik van opleiding, zelfregulering en implementatie van BIG bij medeoverheden.
- Aparte aandacht voor situatie zelfregulering ZBO.

Een en ander kan resulteren in de volgende producten waar de Taskforce een bijdrage aan levert. Let wel, dit is slechts een proeve die nadrukkelijk uitwerking behoeft met ICCIO.

Producten programmering departementen en ZBO's

Bijdrage taskforce aan programmering	Activiteiten taskforce; steeds gaat het om in

	afstemming met ICCIO leveren van 'bijdragen aan'; ICCIO heeft normaliter 'the lead'.
Gesprek organiseren over verschillende BIR/ZBO baseline op verschillende terreinen gericht op aandacht voor kolom primair proces en ontwikkeling	• Ontwikkelen modellen departementale implementatieplannen • Ontwikkelen van gerichte communicatie rond implementatie baseline • Ontwikkeling monitoringsystematiek om voortgang implementaties te meten en op departementaal niveau inzichtelijk te maken • Stimuleren van het hergebruik van deze monitoringssystematiek voor ZBO's in samenwerking met manifestgroep
Bij het vormgeven van een relevant stelsel van audit; selfassessement en peer-review kan de taskforce een goede bijdrage leveren aan zelfregulering binnen departementen. Speficiek aandacht besteden aan situatie bij ZBO's	• In kaart brengen vigerende audit systematieken en bijbehorende normenstelsels\ • Auditsystematiek in lijn brengen met basisrichtlijn • Ontwikkelen van een voor departementen en ZBO's relevante systematiek van peer-reviewing en self-assessments
Bijdragen leveren aan Externe visitaties	• Ontwerpen van visitatiesystematiek gebaseerd op BIR; Auditsystematiek en monitoring voortgang implementatie
Prioritaire ketenregimes ontwikkelen	• In kaart brengen/actualiseren van relevante ketens • Identificatie van ketenverantwoordelijke • In samenspraak met ICCIO beleggen van ketenverantwoordelijkheid • Doorzetten en vertalen van keteninzichten naar mede overheden • Organiseren van relevante verantwoordelijkheden van mede overheden en monitoring daarvan in samenwerking met IPO; Waterschapshuis; IBD en NCSC
Met het opleidingsprogramma ABD APP rond risicoanalyse en informatiebeveiliging module ontwikkelen	• Opleidings- en communicatiemateriaal verzorgen • Relatie leggen met beschikbare kennis bij CIP en NCSC • Het stimuleren van hergebruik van opleiding, zelfregulering en implementatie van BIG bij medeoverheden.
Selectie van 'goede voorbeelden'' van verandertraject naar beheersing	• Organiseren van slimme communicatie rond voortgang implementatietrajecten BIR • Organisatie van departementale 'Piet Hein sessies' Wat gaat goed; waarom gaat het goed; wat zijn de lessons learned

10. Nader ontwikkelen en uitvoeren van de programmering

De geschetste programmering is een opzet die een start per 1 januari mogelijk maakt en die door de Taskforce in samenwerking met de verschillende organisaties per domein nadere uitwerking behoeft. Daarbij is niet alleen sprake van nadere uitwerking maar ook van een nadere taakverdeling. Die is als volgt te schetsen.

Interbestuurlijk

Het verdient nogmaals nadruk dat de taskforce interbestuurlijk van karakter is en dienstbaar aan de ontwikkeling per domein. Dit betekent dat:

- De taskforce zal ondersteunen, signaleren en adviseren, maar niet toezicht houden. Uiteindelijk moet dat uitmonden in de mogelijkheid per organisatie analyses als bovenstaand te maken.
- Zij zal deze taak moeten afstemmen met de domein specifieke instanties en werkwijzen zoals bijvoorbeeld de informatiebeveiligingsdienst in het gemeentelijk domein.
- Deze opzet zal alleen slagen als vanaf de start sterk in overleg met de organisaties in de domeinen zelf aan de programmering wordt gewerkt in aansluiting wat binnen die domeinen al loopt aan acties.

Samenwerking en taakverdeling bij de uitvoering

De minister verwoordt het als volgt:

'Met de taskforce zal ik tevens aansluiten bij de initiatieven die binnen de Rijksoverheid, maar ook binnen de medeoverheden opstarten of gestart zijn waar het gaat om informatiebeveiliging. Binnen de Rijksoverheid wordt de invoering van de Baseline informatiebeveiliging Rijk op korte termijn voorzien. Deze algemene Baseline treedt in de plaats van een groot aantal bestaande baselines; het betreft departementale baselines en een aantal specifieke interdepartementale baselines. Hierdoor wordt het basisbeveiligingsniveau bij de Rijksdienst gelijk getrokken en ontstaat eenduidigheid over dit basisniveau. Bij zowel de VNG als de Manifestpartijen zijn er initiatieven voor het instellen van informatiebeveiligingssteunpunten. Binnen de VNG/KING samenwerking bevindt de gemeentelijke Informatiebeveiligingsdienst (IBD) zich in de kwartiermakerfase. Vanuit BZK en VNG wordt de ontwikkeling van deze dienst actief verwelkomd. Met de IBD wordt invulling gegeven aan de eigen verantwoordelijkheid van gemeenten. Het ligt in lijn met het vanuit het NCSC geïnitieerde Programma Nationaal Response Netwerk. Het doel van dit programma is het vergroten van de weerbaarheid van de Nederlandse samenleving door het creëren en stimuleren van een netwerk van responseorganisaties binnen Nederland. Hiermee wordt een belangrijke stap gezet in de landelijke ontwikkeling van sectorale capaciteiten op het gebied van ICT-response. Deze ontwikkeling geeft een impuls aan de verbintenis tussen het NCSC en partijenbuiten de primaire doelgroep (Rijksoverheid en vitale sectoren) van het NCSC. Niet alleen kunnen langs deze weg verschillende sectoren binnen de eigenverantwoordelijkheid zelfstandig digitale weerbaarheid vergroten, ook wordt hiermee de uitrol van een effectief landelijk netwerk van sectorale informatiebeveiligingsdiensten gestimuleerd. De taskforce zal ook aansluiting zoeken bij bestaande, meer algemene, initiatieven, zoals het al genoemde ABD Topclass programma.'

Van bijzonder belang, zoals benadrukt is de vorming van relevante netwerken die de diffusie van het gedachtengoed van informatieveiligheid bevorderen.

In ieder doemen is er dus een organiserend aanspreekpunt waar vanuit landelijk oogpunt opzet van samenwerking mee mogelijk is. In die zin kan de taskforce zich faciliterend voor de domeinen en die samenwerking opstellen door organisatie van het netwerk, bijdragen aan de producten, organisatie van de programmering. Steeds echter complementair aan dat organiserend aanspreekpunt per domein en aan de samenwerking met de landelijke instellingen die tot stand moet komen.

<table>
<tr><td>Organis. per de domein / stelselorg.</td><td>CIO Rijk/DG Rijk</td><td>CIP/Manifestgroep</td><td>ICT strategisch overleg/IPO</td><td>IBD/VNG</td><td>Unie, Waterschapshuis,</td><td>netwerken</td></tr>
<tr><td>DGOB coördinerend</td><td colspan="5" rowspan="5">Vormgeving aan programmering; faciliterende rol van de taskforce, maar wel verantwoordelijk voor tot stand komen onder aansturing van BRG</td><td>CIO's</td></tr>
<tr><td>NCSC</td><td>Topmanagement</td></tr>
<tr><td>Logius</td><td>Bestuurders ICT</td></tr>
<tr><td>OPta</td><td>Kennis/deskundigen</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Overlegorganen</td><td>BRG</td><td>DB informatieveiligheid</td><td>Interbestuurlijke taskforce</td><td></td><td></td><td></td></tr>
</table>

11. Notitie Ira Helsloot

Notitie

Over doelstellingen en bijpassende leerstrategieën voor

de Taskforce Informatiebeveiliging

Oktober 2012

Ira Helsloot

Gerard van Staalduinen

David de Vries

Inhoudsopgave

1. Abstract

De Taskforce 'Bestuur en veilige ICT dienstverlening' (werknaam) wil bestuurders binnen het Nederlands openbaar bestuur adequaat toerusten voor hun verantwoordelijkheid voor een voldoende niveau van informatieveiligheid. Deze notitie gaat in op de daarvoor noodzakelijk leerstrategieën. Voor de Taskforce is de eerste stap om te komen tot een leerstrategie het benoemen van het 'wat': welk niveau van informatieveiligheid is (realistisch en) voldoende. Uit een vergelijk met de huidige situatie volgt dan de realistische veranderopgave voor het lokaal bestuur. Deze veranderopgave valt uiteen in een eerste orde component (aanpassingen binnen bestaande structuren) en een tweede orde component (fundamentele verandering van bestaande structuren is noodzakelijk). Bij de twee veranderopgaven horen eigen verschillende leerstrategieën passend bij de niveaus 'bestuur', 'bestuurlijke omgeving' en 'organisatie'. Deze notitie beschrijft de twee bestuurlijke leerstrategieën passend bij een eerste orde en een tweede orde veranderopgave, en gaat daarbij in op de typische strategie die bij het leren over veiligheid hoort. De verschillende elementen van de veiligheidsketen staan daarin centraal. Onderscheid wordt bovendien gemaakt tussen vier leerstappen: intuïtie, interpretatie, integratie en institutionalisatie. In het daadwerkelijke leerproces vergen deze stappen verschillende werkvormen.

2. Inleiding

De 'Taskforce Bestuur en veilige ICT dienstverlening' (werknaam) wordt ingesteld om bestuurders binnen het Nederlands openbaar bestuur adequaat toe te rusten voor hun verantwoordelijkheid voor een voldoende niveau van informatieveiligheid. Die toerusting dient te bestaan uit het bewerkstelligen van een actieve gerichtheid op bestuurlijk en hoger managementniveau op de aanpak van de informatiebeveiliging. Zoals hieronder aan de orde komt gaat het daarbij als eerste invalshoek niet alleen om de technische aspecten, maar met name ook om de maatschappelijke en politieke risico's die met deze technische aspecten verbonden zijn. Wij zullen daarom deze notitie telkens naar de Taskforce verwijzen als Taskforce Informatieveiligheid om het onderscheid met de techniek van informatiebeveiliging te benadrukken.

Directe aanleiding rapport Onderzoeksraad

De Onderzoeksraad voor Veiligheid spreekt in haar Diginotar rapport over 'gebrekkig zicht op risico's bij bestuurders en ambtelijke opdrachtgevers' en daardoor over 'bestuurlijk onvermogen tot het nemen van verantwoordelijkheid'.

Voor het opstellen van het plan van aanpak voor de Taskforce Informatieveiligheid is de hoofdvraag hoe de gewenste actieve gerichtheid op het behalen van een voldoende niveau van informatieveiligheid kan worden behaald. Bewustwording is daar een onderdeel van maar ook ondersteuning daarvan door het aanbieden van handreikingen, adviseren over processen en procedures gericht op een veranderde organisatorische omgang en het verankeren van de resultaten in de betrokken organisaties. Deze doelstellingen vragen om beantwoording van de volgende hoofdvraag als basis voor het plan van aanpak:

Door welke leerstrategie kan de Taskforce Informatieveiligheid de actieve gerichtheid binnen het Nederlands openbaar bestuur op een adequate aanpak van informatieveiligheidsvraagstukken op de lange termijn nader bevorderen?

In deze notitie geven wij onze visie op deze leerstrategie.

De notitie bestaat uit twee gedeeltes. Het eerste deel formuleert de 'wat'-opgave die de Taskforce heeft ten behoeve van het tweede 'hoe'-deel dat de eigenlijke leerstrategie beschrijft.

Als preambule opmerking mag gelden dat de probleemstelling en de daarop gebaseerde doelstellingen van de Taskforce nog concreet moeten worden uitgewerkt in het strategische concept voor het project. Uiteindelijk zal uit de uitwerking af te leiden moeten zijn dat de doelstellingen bestuurlijk, realistisch, haalbaar en meetbaar zijn. Vooralsnog presenteren wij een aanpak die strategisch richting kan geven aan die uitwerking en waarbij de invulling ook afhankelijk is van beschikbare middelen en nadere analyse van de uitgangssituatie. Tot op zekere hoogte zal ook 'gedurende de rit' nadere invulkling plaats moeten vinden.

3. Van het 'wat' naar het 'hoe': de eerste opgave van de Taskforce

De 'wat'-vraag die aan de orde is betreft het vaststellen door de Taskforce van *wat* het voldoende niveau van informatieveiligheid is en *wat* een adequate én realistische aanpak is.

Informatieveiligheid

Zoals al gezegd gebruiken we het woord informatieveiligheid in plaats van het woord informatiebeveiliging omdat dat laatste begrip vooral een technische connotatie heeft. Informatieveiligheid is echter ook echt breder dan alleen het nemen van technische beveiligingsmaatregelen. De maatschappelijke risico's van onvoldoende beveiligingsmaatregelen maken een bredere oriëntatie noodzakelijk op alle facetten van informatieveiligheid. Het gaat ook om zaken als risico's, impactanalyses, (digitale)

weerbaarheid, verwachtingenmanagement, contractmanagement en crisismanagement. Als referentiekader kan de informatie-veiligheidsketen behulpzaam zijn[4]:

- pro-actie: vaststellen van het beleids- en uitvoeringskader door (wettelijke) regels en voorschriften voor informatieveiligheid;
- preventie: risicoanalyse en volgens de regels en voorschriften realiseren van adequate beveiligingsmaatregelen;
- preparatie: (planmatig) opbouwen van weerbaarheid van de organisatie tegen kwetsbaarheden in het systeem van de informatieveiligheid;
- respons: alertheid en vermogen van de organisatie om snel en adequaat op kwetsbaarheden en incidenten te kunnen reageren en de betrouwbaarheid en continuïteit van de informatievoorziening te waarborgen;
- nazorg en herstel: vermogen van de organisatie om na incidenten de informatiefunctie te kunnen herstellen.

Om van deze 'wat'-vraag naar de 'hoe'-vraag te komen zijn op voorhand diverse 'besturingsuitgangspunten' voor de Taskforce benoemd. De Taskforce

- gaat uit van zelfregulering binnen de bekende staatsrechtelijke kaders;
- sluit aan bij voorgenomen en in uitvoering zijnde initiatieven ter verbetering van de informatieveiligheid;
- gaat niet uit van een centrale aanpak, maar van een ontwikkeling per domein, sector en organisatie;
- treedt niet in de taken en verantwoordelijkheden van het bevoegd gezag, ofwel het eigenaarschap van de informatiebeheerder;
- verspreidt ontwikkelde kennis, expertise en ervaringen;
- stimuleert, stuurt, coördineert en faciliteert het leerproces;
- rapporteert, evalueert en communiceert de bevindingen.

Samenvattend dient de Taskforce te fungeren als 'buitenboordmotor'. Dat wil zeggen als aanjager op maat van het leer- en ontwikkelproces van informatiebeveiliging.

Concrete, bekende 'hoe'-activiteiten zijn daarmee:

- inventarisering en verspreiding van 'best practices'
- inrichting van een platform waar uitwisseling van kennis en praktijkervaringen kan plaatsvinden.

Een diepere vraag die echter eerst beantwoord moet worden voordat tot beantwoording van de 'hoe'-vraag kan worden gekomen is de analyse van de veranderopgave die samenhangt met

[4] Op basis van: Ministerie van Binnenlandse Zaken (1993). *Integrale Veiligheidsrapportage.*

het bereiken van de centrale doelstelling van het project. Welke veranderingen moeten de betrokken organisaties doormaken om tot een voldoende informatieveiligheidsniveau te komen?

In onze optiek gaat de 'wat'-vraag in op de veranderdoelstelling: de opgave wat verandert moet worden en waarom (visie en bewustwording). De 'hoe' vraag gaat in op de wijze waarop de verandering plaats vindt en tot stand komt: het veranderproces. Bij veranderingen moet een onderscheid worden gemaakt tussen twee typen veranderingen:

- Eerste orde veranderingen zijn beperkte aanpassingen *binnen* de bestaande structuren en werkwijzen(organisaties, procedures, middelenstromen etc.)
- Tweede orde veranderingen zijn fundamentele veranderingen *van* de bestaande structuren en werkwijze in een nieuwe aanpak.

Op basis van de rapportage van de Onderzoeksraad voor Veiligheid (OVV) kan voor de noodzakelijke verbetering van de informatieveiligheid worden ingeschat dat niet volstaan kan worden met eerste orde veranderingen alleen voor alle partijen in het openbaar bestuur. Met andere woorden er zullen zeker (ingrijpende) tweede orde oplossingen noodzakelijk blijken. Dit impliceert dat in de aanpak van de Taskforce het eerste en tweede orde leren en veranderen een plaats moeten krijgen.

Voorbeelden eerste en tweede orde veranderingen

We geven enkele tentatieve voorbeelden van denkbare eerste en tweede orde veranderingen relevant voor informatieveiligheid. Op deze plaats dienen deze voorbeelden slechts als illustratie niet als aanbeveling!

Eerste orde verandering:

- Invoeren en verplichten van opleidingen informatieveiligheid voor een relevante groep medewerkers
- expliciet benoemen van informatieveiligheid in portefeuille lid college van B en W
- verplicht stellen van paragraaf 'informatieveiligheid' in (gemeentelijke) begroting en jaarverslag
- het houden van informatieveiligheidsoefeningen.

Tweede orde verandering:

- instellen van functie Chief Information Officer met de juiste bevoegdheden
- inrichten nieuwe functie 'audit dienst informatieveiligheid' bij Rijk, VNG of elders
- wettelijke normering voor niveau informatieveiligheid.

Bedacht moet worden dat tweede orde veranderingen veel meer energie vergen dan eerste orde veranderingen. Dit zal straks zichtbaar worden in de verschillende passende leerstrategieën. Wanneer derhalve kan worden volstaan met de 'kracht van incrementele verandering' verdient dat de voorkeur. Voor de Taskforce ligt daarom een opgave om per aspect van de informatieveiligheidszorg te kijken of volstaan kan worden met eerste orde veranderingen of dat tweede orde veranderingen aan de orde zijn. De Taskforce zal de lopende veranderingen als uitgangspunt kiezen en op basis daarvan concluderen of deze ver genoeg gaan om de noodzakelijk geachte gerichtheid op informatieveiligheid blijvend te ondersteunen. De verankering van beveiligingsmaatregelen in het geheel van de genoemde veiligheidsketen omvat in ieder geval vraagstukken die qua aansturing en uitwerking op het niveau van twee orde veranderingen zijn gepositioneerd.

De geschiedenis van een Taskforce als illustratie

Nadat in 2005 onderzocht was dat de voorbereiding van Nederland op de gevolgen van overstromingen zwak was, werd besloten tot het instellen van de Taskforce Management Overstromingen.[5] Deze Taskforce is met enthousiasme, maar met een beperkte analyse van haar takenpakket aan de gang gegaan. Startpunt was het creëren van bestuurlijke bewustwording door onder andere bestuurlijke bijeenkomsten en het maken van simulaties van de effecten van overstromingen. De opbrengst van deze activiteit leek geslaagd in de zin dat bestuurders vaak zeer onder de indruk waren van de effecten van overstromingen die zij niet eerder zo onderkend hadden. Het zetten van een volgende stap bleek echter lastig: het treffen van werkelijk effectieve maatregelen om de enorme materiële schade te voorkomen was zeer, zeer kostbaar en voor een groot deel de discretie van externe partijen. Een complicerende factor was verder dat de verantwoordelijk staatssecretaris om politieke redenen niet kon meegaan met het bevorderen van de zelfredzaamheid van burgers, die noodzakelijk is om mensenlevens effectief te redden; in haar beleving was het aan de overheid om voor veiligheid van haar burgers zorg te dragen. Er was met andere woorden niet tijdig onderkend dat voor het slagen van het project essentieel tweede orde veranderingen moesten worden doorgevoerd zoals verandering van de bouwwijze van vitale infrastructuur in Nederland en een paradigmashift van de rampenbestrijding waarbij zelfredzaamheid de basis zou moeten worden. Omdat geen draagvlak was bij de opdrachtgevers op rijksniveau voor deze twee orde veranderingen had de Taskforce een onmogelijke opdracht om deze wel elders binnen het openbaar bestuur te bewerkstelligen. Uiteindelijk werd halverwege de looptijd van de Taskforce impliciet besloten tot het bijstellen van de doelstelling: het eindresultaat was niet meer een betere voorbereiding maar het opleveren van overheidsplannen en een eindoefening passend bij de bestaande rampenbestrijdingsorgansatie. Het eindresultaat was met andere woorden teruggebracht tot een eerste orde veranderopgave. De plannen en de eindoefening zijn opgeleverd, maar tot een werkelijke verbetering van de voorbereiding op overstromingen

[5]Horst, G. ter & Huizinga-Heringa, J.C., (3 juni 2009). *Kabinetsreactie Taskforce Management Overstromingen.*

heeft de Taskforce niet kunnen bijdragen. Het tweede orde niveau van veranderen is niet bereikt omdat de direct betrokken organisaties weliswaar meer inzicht hebben gekregen in de overstromingsrisico's en maatregelen, maar deze kennis en ervaring niet hebben verwerkt in een nieuwe aanpak en werkwijze. Na de Taskforce zijn deze organisaties weer overgegaan tot de gebruikelijke 'orde van de dag', ofwel de werkwijze die voor deze Taskforce van toepassing was.

Ten behoeve van het kunnen ontwikkelen van een leerstrategie als onderdeel van de 'hoe'-vraag is het tenslotte noodzakelijk onderscheid te maken tussen de drie niveaus die betrokken zijn bij de veranderopgave op het terrein van de informatieveiligheid:

- Bestuurders: eindverantwoordelijk
- Bestuurlijke omgeving: collega bestuurders
- Organisatie.

Als voorbeeld: eerste orde veranderopgaven vergen vaak een kleinere bestuurlijke component. Het zal dan veelal voldoende zijn om het hoger management in de bestuurlijke omgeving te adresseren. Significante veranderingen die tot stand moeten komen in interactie met de directe omgeving en afstemming met andere partners, belanghebbenden en direct betrokkenen vragen meer om bestuurlijke aansturing van het tweede orde veranderproces.

De 'van wat naar hoe'-opgave in beeld

We vatten ons beeld van de 'van wat naar hoe'-opgave van de Taskforce in onderstaande figuur samen:

Figuur 1:*De Taskforce fungeert, weergegeven in de bovenste rode pijl en eerder al kort aangegeven, als 'buitenboordmotor' van het leerproces. Dit uit zich in een rol bij zowel de interpretatie als de integratie van nieuwe kennis binnen de organisatie. Bestuurders (en hoger management) vormen de doelgroep van de Taskforce Informatiebeveiliging. Zij zijn de actoren waar de Taskforce zich primair op richt, wat niet wegneemt dat ook anderen een rol spelen om de uiteindelijke doelen te bereiken. Eerst is het – via de rode pijl vanuit de Taskforce naar de bestuurders toe – in het geval van een tweede orde leerproces van belang de intuïtie van de bestuurders te benaderen. Zij dienen zich bewust te worden van het probleem en van wat er speelt. Vervolgens wordt overgegaan op het creëren van een bepaalde awareness naar de omgeving, een fase die plaatsvindt door beïnvloeding vanuit de Taskforce. Dit komt tot uiting in de kromme rode pijl, tussen bestuurders en de bestuurlijke omgeving. In de praktijk kan hier worden gedacht aan het presenteren van voorbeelden over informatieveiligheid, het bieden van 'best practices'. Alleen kennis is*

echter niet voldoende; deze moet overdragen worden en vervolgens begrepen worden door de rest van de bestuurlijke omgeving. In de taal van de organisatieleer gaat het hier om teams, de delen die samen de totale organisatie vormen. Op het moment dat kennis is geland in de bestuurlijke omgeving, dient deze verder uit te worden gerold in de organisatie. Van de bestuurlijke component vindt hier de koppeling met de operationele actoren plaats. In dit betreffende geval naar hen die uiteindelijk in de praktijk voor de informatiebeveiliging zullen moeten zorgen. Opdrachten worden door de bestuurders gegeven – vandaar de blauw kromme pijl rechtsboven – maar de Taskforce begeleidt deze integratie. Op het moment dat de hele organisatie – en dus de verschillende ter zaken doende individuen – zich bewust en op de hoogte is van de geïnitieerde kennis, dient deze verankerd te worden in de structuur. In de praktijk vindt dit onder meer plaats door het maken van werkafspraken en het vaststellen van organisatienormen. De Taskforce begeleidt deze verankering en rapporteert over de mate waarin niet alleen de kennis, maar ook de organisatie zelf op het gebied van de informatiebeveiliging verandert, maar is wel minder prominent aanwezig dan bij eerdere stappen. Dit wordt in de figuur zichtbaar in de twee rode stippellijnen. Bij de terugkoppeling is zowel de organisatie als de Taskforce betrokken. Dit is weergegeven in de blauwrood geblokte pijl, onderaan in de figuur.

4. Leerstrategieën passend bij verschillende veranderopgaven

Twee leerstrategieën

In dit deel van de notitie beschrijven we de leerstrategieën (als onderdeel van het veranderproces) passend bij eerste en tweede orde veranderopgaven op bestuurlijk niveau.

> *Een leerstrategie omvat de visie op welke wijze en met welke middelen de geformuleerde leerdoelstellingen worden bereikt.*

Het bijpassende onderscheid dat wij op deze plaats maken is dat tussen 'lower order learning' en 'higher order learning':

- 'Lower order learning' wordt ook wel 'single-loop learning' genoemd. Het gaat hier over activiteiten die iets toevoegen aan kennis, competenties of routines zonder daarbij de fundamentele natuur van de organisatie te veranderen. Mason (1996)[6] noemt deze vorm van organisatieleer ook wel non-strategic learning, waarmee bedoeld wordt dat deze leer meer aan de oppervlakte blijft en niet de strategie van een organisatie aanpast.
- 'Higher order learning' wordt ook wel 'double-loop learning' genoemd. Hier gaat het om de situatie waarin, naast het detecteren en corrigeren van fouten, de organisatie wordt betrokken bij het ter discussie stellen van bestaande normen, procedures, beleid en doelen. Mason (1996) noemt dit: strategic learning.

---

[6] Mason, D. (1996). *Leading and managing the expressive dimension: Harnessing the hidden power source of the nonprofit sector.* San Francisco: Jossey-Bass.

Het ideaalbeeldbeeld van higher orde leren

In veel theoretische beschrijvingen wordt aan higher order learning een hogere waarde toegekend dan lower order learning. Zo'n positieve insteek over higher-order learning zien we terug in Bloom's Taxonomie.[7][8]Hij wist op een onderscheid tussen verschillende leervormen. Sommige vormen – die op het lagere niveau – vereisen meer cognitieve processen. Maar het maken van analyses, het creëren van nieuwe kennis en het evolueren van een organisatie, is in zijn ogen van een andere orde dan enkel het aanleren van feiten en concepten. Higher order thinking kost, zo stelt Bloom, meer moeite, vereist meer competenties, maar is uiteindelijk wel waardevoller omdat de capaciteiten die daarmee worden aangeleerd beter van pas komen in nieuwe situaties. Het stelt individuen én organisaties beter in staat zich aan te passen aan veranderende situaties. Maar, daartegenover staat dat het in de harde werkelijkheid wel noodzakelijk is om telkens de vraag te stellen of de energie die moet worden gemobiliseerd voor higher orde leren wel noodzakelijk is om de geformuleerde doelstellingen te bereiken. Er zijn veel situaties denkbaar waarin voor bepaalde doelgroepen volstaan kan worden met een eerste orde leerproces..

Leerstrategieën specifiek voor het informatieveiligheidsdomein

Het standpunt 'Het is hier veilig, mij kan niets gebeuren, ik voldoe aan het veiligheidsvoorschriften' is één van de grootste valkuilen van het veiligheidsbeleid. Zeker op het terrein van de informatieveiligheid waarin niet de natuurwetten maar de inventiviteit van criminelen de gang van zaken over risico's, gevaren en passende maatregelen bepalen. In algemene zin is uniek voor 'veiligheidsleren' dat de dagelijkse werkpraktijk geen of niet voldoende prikkels bevat die de noodzaak van het leren duidelijk maken. Veiligheidsrisico's zijn immers verborgen. Voorschriften leveren wel een bijdrage aan de veiligheid, maar kunnen (zeker op de langere termijn) niet waarborgen dat er geen onveilige situaties ontstaan. Veiligheid start met het te onderhouden besef welke risico's en gevaren er zijn, het zien en onderkennen hoe gevaarlijke situaties kunnen ontstaan, welke omstandigheden niet gewenste ontwikkelingen beïnvloeden en hoe moet worden opgetreden om de gewenste condities te kunnen beheersen. Criminelen zijn slim, de informatieveiligheid moet nog slimmer zijn. Veiligheid impliceert daarmee kennis en inzicht in de aanwezige omstandigheden en het vermogen om zelfstandig en adequaat in deze omgeving te kunnen ingrijpen. Voorschriften en instructies als zodanig kunnen en doen dat niet. Ze kunnen er wel voor zorgen dat iemand begrijpt en zich er bewust van is (of wordt) welke handelingen in bepaalde omstandigheden noodzakelijk zijn om een gewenste veilige situatie te bereiken. Het bewustzijn van risico's en gevaren en het begrijpen van de maatregelen waarmee een gewenste situatie kan worden

---

[7] Bloom, B.S. e.a. (1956). *Taxonomy of educational objectives: the classification of educational goals; Handbook I: Cognitive Domain.* New York: Longman.

[8] Anderson, L. & Krathwohl, D.A. (2001). *Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Eductional Objectives.* New York: Longman.

gerealiseerd, zijn de basisvoorwaarden voor een adequate inrichting van een veilige omgeving. Uiteraard moet uiteindelijk e.e.a gedocumenteerd worden in handleidingen en richtlijnen.

De Taskforce dient derhalve ten behoeve van tweede orde leren als eerste in te zetten op het ontdekken en activeren van dit basisbesef en verdiepend inzicht. Niet op het aanleren van richtlijnen voor bestuurlijk handelen dus, maar wel op een confrontatie met omgevingen waarin risico's en gevaren zich manifesteren en waarin bestuurders keuzes moeten maken welke oplossingen een bijdrage leveren aan de doelstellingen die zij voor het eigen veiligheidsbeleid hebben geformuleerd. Simpele problemen en oplossingen staan niet op het menu. Om de waakzaamheid en weerbaarheid voor risico's en gevaren te vergroten dient de doelgroep als eerste *geconfronteerd* te worden met complexe en unieke situaties, waarin meerde oplossingsperspectieven mogelijk zijn. In discussies en debatten moeten vervolgens een dieper inzicht in de informatieveiligheidsproblematiek worden verkregen, bepalen analyses de oplossingsrichtingen, moeten besluiten worden gemotiveerd en maatregelen worden verdedigd. In een tijd dat de cybercriminaliteit zich sterker dan ooit ontwikkelt moet de bestuurder het debat aan hoe zijn organisatie adequaat weerstand tegen deze ontwikkelingen kan en moet bieden. Het verwijzen naar voorschriften zal daarbij niet in alle omstandigheden de meest passende oplossing zijn. Er zal meer moeten gebeuren.

Inhoudselementen van de veiligheidsleerstrategie

Inhoudelijk stellen wij voor om in welke leerstrategie ook gekozen wordt de veiligheidsketen centraal te stellen. In het veiligheidsmanagement gaat het, als bij alle management, om een proces van besluitvorming, sturen en regelen gericht op het bereiken van de geformuleerde veiligheidsdoelstellingen. Kern van die aanpak is voor informatieveiligheid is dat prognoses worden gemaakt van de verwachte dreigingsontwikkelingen in de omgeving en dat op basis van scenarioanalyses handelingsperspectieven worden ontworpen om situaties en omstandigheden te kunnen beheersen.

.

Inhoudelijke elementen zijn daarmee:

- het uitvoeren van risico inventarisaties en risicoanalyses om het niveau van de preventieve beveiligingsmaatregelen te bepalen: voor de bouw, de inrichting en het gebruik van systemen (beheersmaatregelen);
- het toetsen en beoordelen van situaties en omstandigheden aan vigerende veiligheidsregels en voorschriften;
- het scenario denken d.w.z. uitgaan van het optreden van een incident om te bepalen hoe een incident zich, in tijd en ruimte, kan ontwikkelen en met welke responsmaatregelen de ongewenste gevolgen (impact analyses) kunnen worden voorkomen, beperkt en aangepakt;

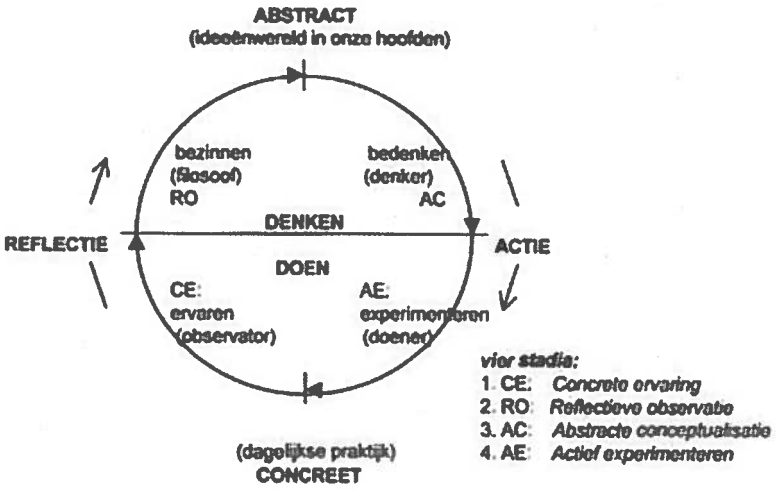
- het opstellen van plannen en procedures voor beheers- en responsmaatregelen (preparatie en planvorming);
- opleiding en training (individueel en met organisatorische eenheden) voor het kunnen toepassen van beheers- en responsmaatregelen (waaronder crisisbesluitvorming, crisismanagement en crisiscommunicatie);
- rapportage, analyse, beoordeling en evaluaties met adviezen en voorstellen voor het verbeteren van de beheers- en responsmaatregelen van de organisatie.

De sterkte van een gehele keten wordt aangeduid als een veiligheidsniveau. Het leerproces gaat vooral in op de onderlinge betekenis en verbanden tussen de verschillende elementen van de veiligheidsketen. De integraliteit en samenhang van de elementen staat centraal. Het belangrijkste is dat het eindresultaat wordt bewaakt en dat het inzicht groeit in de verschillende accenten die in de keten kunnen worden gelegd. Voor elk veiligheidsniveau gelden minimale eisen die aan de verschillende elementen worden gesteld. Om over het eindresultaat (het vastgestelde veiligheidsdoel) te kunnen oordelen moet er minimale inhoudelijke kennis zijn van het doel, de functie en de mogelijkheden van alle afzonderlijke onderdelen.

Vier leerstappen

Bij elk van de twee leerstrategieën maken we onderscheid in vier leerstappen, te weten intuïtie, interpretatie, integratie en institutionalisatie.[9] Niet op elke stap zal de Taskforce een even grote invloed (willen en kunnen) uitoefenen. De vier stappen staan hieronder uitgebreid beschreven. Aan het slot van elke leerstap wordt kort aangegeven hoe hier tegenaan moet worden gekeken wanneer het eerder gemaakte verschil tussen hogere en lagere orde denken/leren in ogenschouw wordt genomen.

[9] Lawrence, T., Mauws, M., Dyck, B., & Kleysen, R. (2005). *The politics of organizational learning. In Academy of Management Review. 30*(1), p. 180-191.



Figuur 2:*De klassieke leercirkel van Kolb*[10]

- Intuïtie: concrete ervaring als startpunt (CE)

De literatuur gaat uit van intuïtie als eerste stap in het leerproces van de organisatie. Het is een fase die zich bij personen in het voorbewustzijn bevindt. Intuïtie kan dan ook niet worden aangebracht, maar alleen worden geprikkeld en gestimuleerd. Leren begint met het ervaren van een probleem of een vraag vanuit de alledaagse praktijk.Dit gebeurt door nieuwe ervaringen en externe prikkels. Als een individu iets heeft meegemaakt, koppelt zijn intuïtie dit aan nieuwe gebeurtenissen. Wanneer een individuele actor, met invloed of (doorzettings)macht tot een bepaald inzicht komt, kan het zijn dat hij de rest van de organisatie daarin mee wil krijgen. In het geval van de Taskforce kunnen bestuurders in deze eerste stap bewust worden gemaakt van het belang van informatiebeveiliging. De actie van de Taskforce zit in het prikkelen van de intuïtie. Wanneer het over leren in de eerste orde gaat, zal dit niet tot nauwelijks nodig zijn. Pas als ook echt de structuur van en de denkpatronen binnen de organisatie moeten worden aangepast, moet van buitenaf worden ingespeeld op de intuïtie. Dit kan bijvoorbeeld worden gedaan door het organiseren van serious games of peergroepen van elkaar te laten leren. Dit eerste stadium wordt ook wel het stadium van de beeldvorming genoemd.

- Interpretatie: nadenken over onze ervaringen (RO)

---

[10]Kolb, D., (1981). Learning styles and disciplinary differences. In A. Chickering. The Modern American College (pp. 232-255). San Francisco: Jossey-Bass Inc.

Als het vereiste inzicht is geland bij de bestuurders, de doelgroep van de Taskforce, gaat deze groep zich bezinnen op de situatie. Het gaat hier om reflecteren , dat wil zeggen het nadenken over wat er is waargenomen en wat er moet gebeuren. In dat denken kijken de deelnemers terug op de situatie en interpreteren deze door deze informatie te confronteren men wat men al over de situatie weet.(herinnering). Dit is de fase van interpretatie waarin de oordeelsvorming plaats vindt Crossan e.a. (1999)[11]: 'Het interpreteren is het uitleggen, door woorden en/of acties, van een inzicht of een idee aan zichzelf of anderen.' In de praktijk vindt dit plaats door conversaties en dialogen. Wat bij een individu begint, belandt uiteindelijk binnen een groter geheel. Belangrijk om hierbij op te merken is dat lang niet alle ideeën die via intuïtie opkomen geschikt zijn om de stap van de interpretatie (en laat staan verdere stappen) te bereiken. Essentieel hierin, zo zegt de literatuur, is de macht en (politieke) positie om een idee over te brengen. Dit zou meer bepalend zijn voor de overlevingskans dan de kwalitatieve kracht of de waarde van de gedachte. (NB: in dat kader is het een goede keus om bestuurders de doelgroep van de Taskforce te laten zijn, aangezien zij deze invloed vaak wel bezitten.) Deze fase vergt overigens van beide partijen inzet. De bestuurder zal de kennis moeten overbrengen, de verstaander zal de kennis moeten begrijpen. In de lijn van de eerdere initiatie moet ook in deze fase 'beïnvloeding' plaatsvinden. Inzicht moet worden vergroot. Bijvoorbeeld door voorbeelden te tonen waarin het belang van informatiebeveiliging wordt laten zien, kan de Taskforce het interpretatieproces beïnvloeden. Net zoals in de leerstap intuïtie bestaat ook hier verschil tussen eerste en tweede orde leren. Wanneer het niet nodig is de organisatie grondig te vernieuwen, zal het aandragen van kennis voor de interpretatie al gauw voldoende zijn. Indien eerst ook begrip en bewustzijn moet worden aangebracht, zijn interactieve sessies als workshops, debatten en discussies echter een veel betere manier om het gewenste doel te bereiken.

De eerste twee stadia van de ontwikkelcyclus abstraheren de praktijkervaringen tot nieuwe ervaringskennis.

- *Integratie: bedenken van oplossingen (AC)*

Waar het er in de vorige fase om draaide de directe omgeving van de bestuurder bewust te maken van het belang van de kennis, is dat niet voldoende. Het is van groot belang dat de leidinggevenden achter het leertraject staan, maar zonder operationele steun zal het daadwerkelijke effect miniem zijn. In deze casus is dat niet anders. Het bewust maken van de organisatie als geheel heet het integratieproces. In het stadium van het denken richten de activiteiten zich op het ontwikkelen van een antwoord of een plan om het probleem op te lossen (planvormingsfase). Om dat te bewerkstelligen gaat het om het bedenken van alternatieve oplossingen en het maken van keuzes. Kennis wordt omgezet in handelingen, instructies en opdrachten. Het integreren gaat over het ontwikkelen van een gezamenlijk, gemeenschappelijk begrip tussen individuen. Alternatieve oplossingen die worden bedacht,

---

[11] Crossan, M., Lane, H. & White, R. (1999). *An organizational learning framework: From institution to institution. In Academy of Management Review. 24*(3), p.522-537

worden geconfronteerd met bestaande kennis (geabstraheerde conclusies uit eerdere ervaringen). Uiteindelijk ligt de focus op het creëren van nieuwe situaties en coherente en gezamenlijke acties, bijvoorbeeld uitgevoerd door de individuen in de organisatie. Bij het bedenken onstaan nieuwe ideeën , concepten en plannen, die verandering moeten brengen in de bestaande situatie. Dit zal over het algemeen gemakkelijker gaan in het eerste orde leren dan in het tweede orde leren. Waar andere actoren binnen de organisatie bij de simpelste variant met workshops en discussies kunnen worden geactiveerd, zal bij het tweede orde leren dieper op de aard van de organisatie moeten worden ingegaan. Zoals bij 'intuïtie' het bewustzijn van de bestuurders moest worden geprikkeld, gebeurt dat hier bij de andere actoren. Het is echter de bedoeling dat de rol van de Taskforce, in dit stadium van het leerproces, een stuk minder prominent is dan in de eerste fases, waarin de bestuurders nog met het onderwerp in aanraking moesten worden gebracht. Vanaf de stap integratie zal de organisatie, zowel bij eerste orde als bij tweede orde leren, veel zelf moeten invullen.

- *Institutionalisatie: actie ondernemen (AE)*

Op het moment dat aan de eisen van de integratiefase is voldaan, is de hele organisatie bewust gemaakt van het belang van de kennis. De eerste confrontatie is daarmee voltooid, iedere medewerker en elk team dat op de hoogte moet zijn, is ook daadwerkelijk op de hoogte. Vervolgens moeten de ontwikkelde plannen wordt getest en uitgevoerd (doen). Er is een nieuwe situatie gecreëerd waarmee de geconstateerde problemen naar verwachting zijn opgelost. De cirkel is daarmee rond. Zolang er echter geen sprake is van verankering in de organisatie, is de verandering niet gewaarborgd voor de toekomst. Tijdens de institutionalisatie wordt de door individuen en groepen geleerde kennis verankerd in 'systemen, structuren, procedures en strategie' (Crossan, 1999). Deze vierde stap onderscheidt zich van het individuele of groepsleren doordat er instituties binnen de organisatie ontstaan die uiteindelijk ook voor alle nieuwe leden van de organisatie van toepassing zijn. Indien individuen vervolgens binnen die organisatie, vanuit hun intuïtie, tot nieuwe ideeën of gedachten komen, begint de weergegeven leercirkel eigenlijk weer van voren af aan. De hoofdrol in deze stap wordt door de organisatie gespeeld. Een Taskforce kan hier eigenlijk alleen nog fungeren als een ondersteunende actor. De 'buitenboordmotor' moet bij de institutionalisatie veel minder krachtig opereren dan in de eerste fases van het proces.

Over de relatie tussen bestuurlijk en individueel leren

De Taskforce gaat uit van de gedachte dat het creëren van draagvlak voor nieuwe kennis bij bestuurders essentieel is om de rest van de organisatie mee te krijgen in de gewenste richting.

Dit idee wordt onderstreept door bestuurskundig onderzoek van Eva M. Witesman en Charles R. Wise (2012).[12] Trainingen op het gebied van democratische processen, zo blijkt uit de daarop gerichte studie, hebben pas echt effect en rendement als bestuurders dit proces ondersteunen en medewerkers (lees: ambtenaren) voor die trainingen motiveren. Overigens heeft het niet alleen met motivatie te maken. Ook geld speelt hierin een rol. Het zijn, zo bleek al uit onderzoek van Kettl et al (1996)[13] en Wise et al (2007)[14], de bestuurders in het openbaar bestuur die verantwoordelijk zijn voor het maken van belangrijke beslissingen over 'trainingsprioriteiten' die gefinancierd, geïnitieerd of aangemoedigd worden. Zonder de trainingen of opleidingen van medewerkers (individueel leren) is echte verandering niet haalbaar, zo schrijven Witesman en Wise in hun artikel (pagina 711): 'Training van ambtenaren is een noodzakelijke voorwaarde om een effectieve overheidshervorming te bewerkstelligen'.

Samengevat is de leercyclus in de eerste stap begonnen met het ervaren van een probleem of vraagstuk, dat opgelost moest worden (intuïtie). Tijdens de tweede stap is het probleem geïnterpreteerd en is over de situatie nagedacht (interpretatie). Als derde stap zijn vervolgens oplossingen bedacht (integratie). Tot slot is in de vierde stap de nieuwe situatie gerealiseerd en is ervaren en waargenomen of het beoogde resultaat is bereikt (institutionalisering). De organisatie kan zich vervolgens opnieuw bezinnen op de nieuwe waarnemingen en opnieuw conclusies trekken of de situatie aan de gestelde doelstellingen betantwoord. Leren en ontwikkelen is in deze benadering een oneindig doorgaand en zich voortdurend herhalend proces. De cyclus blijft zich in de praktijk herhalen. De Tasforce zet in op een eenmalige activering van dit proces in de verwachting dat daarmee de nu gesignaleerde problemen voortvarend worden opgepakt.

5. Werkvormen bij de leerstrategiën

De specifieke leerstrategie die past bij vraagstukken waarin een relatief kleine kans op risico's maar een potentieel groot effect centraal staan, vergt een aantal specifieke werkmethodes van de Taskforce.

---

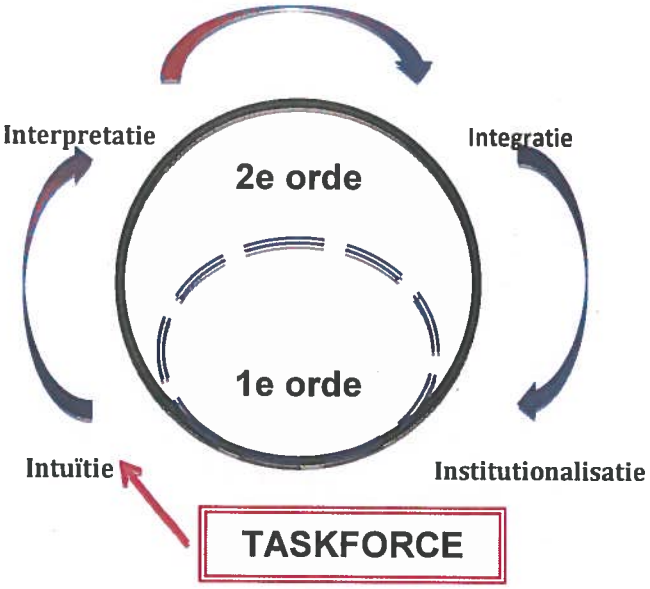
[12] Witesman, E., Wise, C. (2012). *The Reformer's Spirit: How Public Administration Fuel Training in the Skills of Good Governance.* In Public Administration Review 72(5). pp. 710-720.

[13] Kettl, D., Ingraham, P., Sanders, R. & Horner, C. (1996). *Civil Service Reform: Building a Government That Works.* Washington DC: Brookings Institution Press.

[14] Wise, C. et al (2007). *Strategic Assessment of the Present State of Public Administration Education and Training in Ukraine and Prospects for Launching a Capacity Building Institution for Public Officials* (http.glennschool.osu.edu/faculty/brown/home/FinalReport.pdf (accessed June 15, 2012).

In de onderscheiden vier leerstappen zijn deze werkmethodes:

- Leerstap 1 (intuïtie): concrete ervaring (CE) ➔ leermethode: ervaren, observatie, divergeren met als werkvormen simulatie, brainstormen, open opdrachten, meerdere uitkomsten, verzorgen presentatie, samenvatting opstellen, vragen bedenken;
- Leerstap 2 (interpretatie): reflectieve observatie (RO) ➔leermethode: bezinnen, abstraheren met als werkvormen kernwoordenspel, incidentmethode, film/videoband bekijken, observatie opdrachten, uitwisselen van praktijkervaringen in groepsgesprekken;
- Leerstap 3 (integratie): abstractie conceptualisatie (AC) ➔leermethode: bedenken, convergeren met als werkvormen revisie-werkvorm, leergesprek, forum en doceren;
- Leerstap 4 (institutionalisering): actief experimenteren (AE) ➔leermethode: experimenten, doen, concretiseren met als werkvormen gevalsbespreking, logboek verzorgen, toepassingsopdrachten, experimenteren met behulp van de theorie;



Figuur 3:*De vier leerstappen voor eerste en tweede orde leren*

In onderstaande tabel staan de werkvormen per leerstap benoemd, waarbij onderscheid is gemaakt tussen het hogere en lagere orde leren. Net zoals eerder in de figuur met de afgebeelde 'wat'-opgave van de Taskforce zijn ook hier de activiteiten van de Taskforce rood gekleurd en de stappen voor de organisatie zelf in het blauw.

Werkvormen behorende bij de vier leerstappen		
Leerstap	**Eerste orde leren (lower level learning)**	**Tweede orde leren (higher level learning)**
INTUÏTIE Het herkennen en erkennen van het belang van informatieveiligheid voor de organisatie.		- Voorbeeldconfrontatie - Serious gaming - Peer to peer - Analyse van voorbeelden - Uitvoeren QuickScan
INTERPRETATIE Het betekenis geven aan de intuïtie over informatieveiligheid; dit gebeurt binnen de omgeving van de bestuurder.	- Conferentie (presentatie en uitwerking) - Handleidingen - Uitvoeren onderzoek op hoofdlijnen	- Interactieve workshops - Themagerichte analyses - Debat en discussie - Starten risico-inventarisatie - Bepalen en vaststellen aanwezig en gewenst veiligheidsniveau
INTEGRATIE Het borgen van de aangeleerde kennis over informatieveiligheid naar andere onderdelen en medewerkers binnen de organisatie.	- Workshops voor het koppelen van thema's - Discussie en debat voor rest organisatie - Inventarisatie en beoordeling situaties en oplossingen	- Interactieve conferentie - Confrontaties met situaties en oplossingen - Praktijksimulaties en dilemmatraining - Uitwerking opdrachten voor presentatie - Inventarisatie van maatregelen per schakel van de veiligheidsketen
INSTITUTIONALISATIE Het organiseren van institutionalisatie van de informatieveiligheid binnen de organisatie.	- Conferentie, toelichten werkwijze voor stappen organisatie - Uitvoeren audits, praktijksimulaties en oefeningen	- Bieden van handleidingen en ondersteuning - Collegiale consultatie met uitwisselen van kennis en ervaringen

Bijlage 6 Organisatieboek: governance en organisatie

Op 1 januari aanstaande gaat de Taskforce Bestuur en veilige dienstverlening van start. De taskforce heeft tot doel om de bewustwording rond informatieveiligheid bij bestuurders en medewerkers van overheidsorganisaties te verbeteren. Daarnaast streeft zij een aantoonbare verankering van dit verbeterde bewustzijn na.

De taskforce signaleert, stimuleert en monitort noodzakelijke verbeteringen in het veiligheidsbewustzijn. Zij richt zich met name op de ontwikkeling van het leervermogen van overheidsorganisaties op dit terrein en monitort de wijze waarop het geleerde bij deze organisaties wordt verankerd.

De uitvoering van werkzaamheden laat zij waar mogelijk uitvoeren door bestaande (stelsel) partijen. In die zin werkt de taskforce nauw samen met NCSC, de IBD en het CIP. Het spreekt voor zich dat de taskforce waar nodig actief relaties legt met ander organisaties binnen en buiten het overheidsdomein voorzover dat voor de realisatie van de doelen van de taskforce noodzakelijk is.

De taskforce wordt opgezet voor een periode van twee jaar. Daarna worden de geboekte resultaten geëvalueerd en worden werkzaamheden waar nodig belegd binnen de overheid.

Deze notitie behandelt de besturings- en inrichtingsaspecten van de taskforce.

De taskforce is organisatorisch gepositioneerd bij ICTU. Daartoe is een programmaovereenkomst gesloten. De programmaovereenkomst behelst een facilitering van de PIOFAH- taken en de daarvoor binnen ICTU geldende regels. De verdere hiërarchische en inhoudelijke aansturing geschiedt vanuit de Directie B en I en de geschetste governancestructuur.

1. Governance van de taskforce

Sturing en organisatie

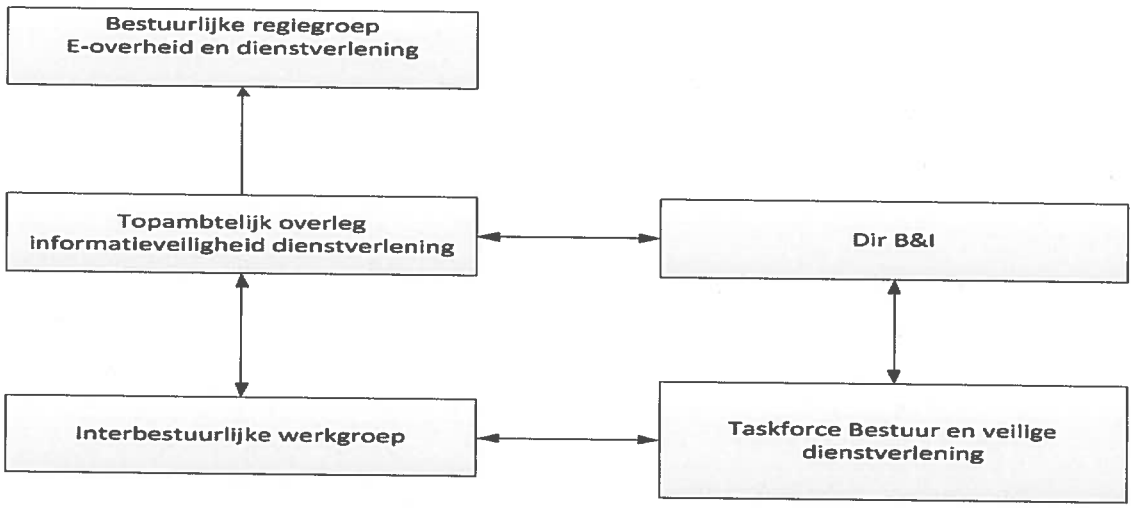
De voorstellen voor sturing en organisatie zijn gebaseerd op de volgende uitgangspunten.

- Het huidige stelsel van bevoegdheden en verantwoordelijkheden rond informatieveiligheid is uitgangspunt.
- Iedere overheidsorganisatie blijft zelf verantwoordelijk voor realisatie eigen informatieveiligheid
- Coördinatie op bestaande initiatieven is een noodzaak om overheidsbrede informatieveiligheid te verbeteren
- De taskforce kent een Interbestuurlijke aanpak; collegiaal en in vertrouwen

- De taskforce wordt klein en wendbaar opgezet zodanig dat hij in een netwerk van organisaties stimulerend werkt
- De Governance van de taskforce sluit aan de bestaande bestuurlijke regiegroep e overheid en dienstverlening.

Governance

Uit de gesprekken blijkt een tweeledige behoefte. Ten eerste geen aparte nieuwe overlegstructuren Ten tweede een geconcentreerde, aparte aandacht voor het vraagstuk van informatieveiligheid met de mogelijkheid tot interbestuurlijke coördinatie, gegeven de verantwoordelijkheid van de verschillende betrokken organisaties. Het voorstel is als volgt om de daarmee samenhangende governance als volgt vorm te geven.



De bestuurlijke regiegroep e- overheid en dienstverlening is een goed forum voor overleg en coördinatie informatieveiligheid. Vanuit V en J is aangegeven een dergelijke afstemming gewenst te vinden en kan gevraagd worden om aan de regiegroep deel te nemen. Voor een snelle en krachtige besluitvorming in het netwerk van de geschetste vierhoek is een topambtelijk overleg van de vijf domeinen[15] gewenst. De dir B&I van BZK is met name ook opgenomen vanwege de taak inzake stelselverantwoordelijkheid en coördinatie. De programmaraad 'Follow up DigiNotar' vindt een opvolger in de interbestuurlijke werkgroep 'Informatieveiligheid dienstverlening' .

[15] Rijksoverheid; ZBO's en agentschappen', Provincies, Waterschappen en Gemeenten.

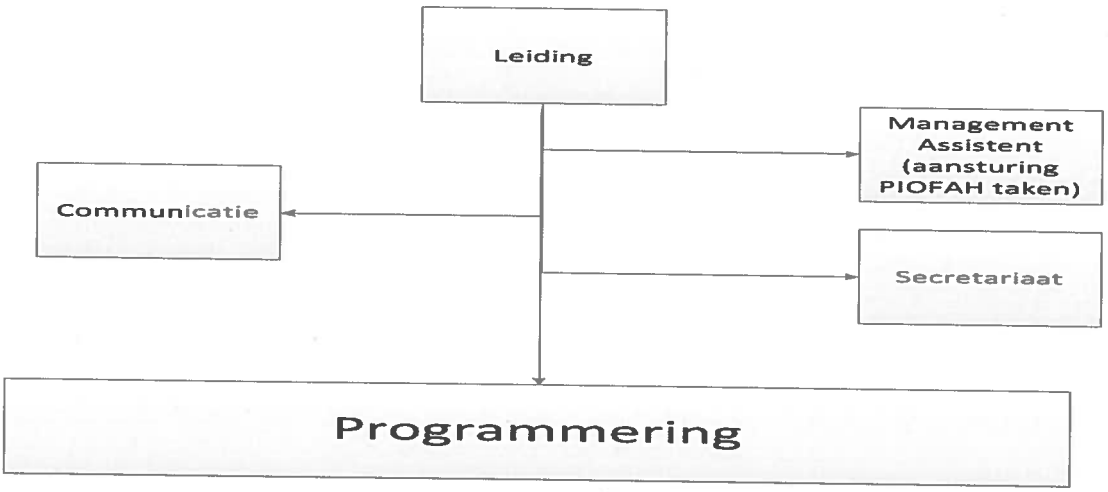
2. Deleiding van de taskforce

De leiding behoeft een tweeledige set van competenties die lastig te verenigen is. Ten eerste toegang hebben tot bestuurlijk en top managerial arena's en mede vanuit de resultaten van het overleg daarin aansturen van de taskforce. Ten tweede een creatieve, hoogwaardige vormgeving aan de programmering en het 'hands on' dagelijks leiding geven daaraan. Het advies is de leiding in te richten door aanstelling van een eindverantwoordelijk interbestuurlijk ervaren manager/ex-bestuurder, die met gemiddeld 0,4 fte wel 'echt' leiding geeft aan de taskforce.In die taak wordt hij ondersteund door eendagelijks programmanager voor 0,8 fte.

Functieprofielen van de leiding van de taskforce zijn opgenomen in de bijlage. De wervingsprocedure is in volle gang. Het streven is om op 19 december de leiding van de taskforce voor te stellen aan de bestuurlijke regiegroep.

3. Organisatie en formatie

De taskforce is een eenheid van beperkte omvang, gepositioneerd binnen ICTU. De PIOFAH taken verzorgt ICTU conform een programma overeenkomst. Hiërarchische aansturing geschiedt door de directeur B&I; zie bij governance.



In de taskforce is kennis en vaardigheid aanwezig inzake communicatie, informatieveiligheid, leerprocessen, organisatie en sturing (verankering) en kennisprocessen. Uiteraard is er ondersteuning gericht op een krachtige programmering. De verschillende functionarissen verzorgen het accountmanagement voor de verschillende domeinen. Zie onderstaande tabel.

Taskforce opzet	Fte	Schaal
Leiding	1,2	
Directeur	0,4	contract
Programmamanager	0,8	15
Ondersteuning	**2**	
Secretaresse	1	6
Communicatiemedewerker	1	12
Programmering	**7**	
Beleidsmederwerker Leren	1	13
Beleidsmedewerker Verankeren	1	12
Beleidsmedewerker informatieveiligheid	1	13
Beleidsmedewerker onderzoek/monitoren	1	12
Junior beleidsmedewerkers	3	10/11
Totaal formatie	**10,2**	

- In dit overzicht ontbreken de functie van managementassistent en de invulling van de PIOFAH functies.
- Deze functies worden via een overeenkomst afgenomen bij ICTU

Het streven is de formatie mede in te vullen met medewerkers vanuit de andere overheden. Een zogenaamde romptaskforce waarmee het mogelijk is de werkzaamheden te starten bestaat in ieder geval uit de leiding, ondersteuning, een overeenkomst met ICTU en twee beleidsmedewerkers. De werving van de romptaskforce is op de beleidsfuncties informeel gestart. Over de invulling van de leiding moet uiteraard nauw overleg plaats vinden met de departementale top en voor zover gewenst interbestuurlijk. Dir B&I heeft de leiding van deze wervingsacties.

In de bijlage zijn de functieprofielen van de diverse functionarissen opgenomen. De wervingsprocedure is in volle gang.

4. Planning en control

De planning en controlcyclus wordt ingericht op basis van de bestaande werkwijzen en procedures zoals die bij ICTU zijn geoperationaliseerd. De uitwerking daarvan en daarmee samenhangende mandaatregeling zijn als bijlage bij deze rapportage gevoegd.

Het budget voor de taskforce bedraagt in 2013 € 5 mln. Daarnaast is een budget voor stelsel gerelateerde activiteiten rond informatiebeveiliging beschikbaar voor de directeur B&I. Dit budget is echter niet voor doelstellingen van de taskforce gealloceerd.

5. PIOFAH Taken

Met ICTU is een overeenkomst afgesloten rond de invulling van de PIOFAH taken. De overeenkomst en de diverse uitgewerkte procedures zijn opgenomen als bijlage bij dit document. Het betreft respectievelijk:

- De mandaatregeling op basis waarvan de leiding van de taskforce verplichtingen kan aangaan
- Een korte beschrijving van de planning en controlcyclus die voor de taskforce van belang is. Onderliggend aan deze procedure is bij ICTU een daartoe passende administratieve organisatie ingericht. Een gedeelte van de managment-assistent functie wordt door een projectsecretaris

van ICTU vervuld. Deze functionaris draagt zorg voor correcte vulling van de onderliggende administratieve systemen.

- De medewerkers van de taskforce worden gehuisvest bij ICTU. Werkplekken en standaard ICT voorzieningen zijn voor medewerkers van de taskforce beschikbaar. De medewerkers van de taskforce krijgen (wel/niet) beschikking over een internetdomein 'taskforcebid' en bijbehorende mailaccounts. Een beschrjiving van de voor de taskforce relevante voorziening is als bijlage opgenomen.

6. Functieprofielen

In deze bijlage zijn de functieprofielen van de voorziene formatie opgenomen. De werving van medewerkers van de taskforce wordt ondersteund door ICTU. In deze paragraaf zijn eerst de algemene teksten opgenomen die in elke vacature zijn vermeld. Vervolgens zijn per functie de relevante beschrijvingen opgenomen.

7. Sollicitatie en functies

Op 1 januari aanstaande gaat de interbestuurlijke Taskforce Bestuur en veilige dienstverlening van start. De taskforce heeft tot doel de binnen de overheid de gerichtheid van bestuur en top management op informatieveiligheid blijvend te versterken en door bevorderen van bewustwording van de maatschappelijke risico's, van kennis en inzichten van informatieveiligheidsstrategie en van de verankering van informatieveiligheid in de organisatie- en stelselprocessen. Daarnaast heeft de taskforce tot taak de coördinatie van het informatieveiligheidsbeleid overheidsbreed te bevorderen en daarover indien opportuun te adviseren. De taskforce is opgericht als vervolg op aanbevelingen van de Onderzoeksraad voor veiligheid naar DigiNotar en Lektober.

De taskforce signaleert, stimuleert en monitort noodzakelijke verbeteringen in het veiligheidsbewustzijn. Zij richt zich met name op de ontwikkeling van het leervermogen van overheidsorganisaties op dit terrein en monitort de wijze waarop het geleerde bij deze organisaties wordt verankerd.

De uitvoering van werkzaamheden laat zij waar mogelijk uitvoeren door bestaande (stelsel) partijen. In die zin werkt de taskforce bijvoorbeeld nauw samen met NCSC, de IBD en het CIP en met de bestaande koepelorganisaties. Het spreekt voor zich dat de taskforce waar nodig actief relaties legt met andere organisaties binnen en buiten het overheidsdomein voor zover dat voor de realisatie van de doelen van de taskforce noodzakelijk is.

De taskforce wordt ingesteld voor een periode van twee jaar. Mede op basis van de evaluatie van geboekte resultaten worden werkzaamheden waar nodig belegd binnen de overheid. Aansturing van de taskforce vindt plaats door een interbestuurlijke regiegroep onder voorzitterschap van de Minister van Binnenlandse Zaken. De directeur Burgerschap en Informatie treedt op als gedelegeerd opdrachtgever en stuurt de taskforce hiërarchisch aan. De taskforce is organisatorisch gepositioneerd binnen ICTU.

Meer informatie over de vacature en over de sollicitatieprocedure:

De sollicitatieprocedure voor deze functie wordt uitgevoerd door ICTU.

Naam: Jaap van Hoek (SC Human Resources)

Telefoonnummer: 0621137497

E-mailadres: solliciteren@ictu.nl

Over ICTU

ICTU is van en voor de overheid. ICTU wil overheden helpen beter te presteren met slim gebruik van ICT.

Velen gebruiken producten die bij ICTU zijn gerealiseerd. Denk aan DigiD, DigiD Machtigen, Overheid.nl, Staatscourant online, het 14+netnummer en het Burger Service Nummer.

ICTU is een projectenorganisatie. Om kwaliteit en flexibiliteit te kunnen garanderen werkt ICTU met een kern van vaste medewerkers en een schil van medewerkers met een tijdelijke aanstelling, gedetacheerden en externen. Momenteel werkt ICTU met ruim 300 medewerkers in meer dan 20 projecten op verschillende domeinen in opdracht van verschillende overheden. ICTU-medewerkers hebben hart voor de publieke zaak en kennen de overheid. Het resultaat staat steeds voorop.

Medewerkers werken aan projecten, vanuit expertteams binnen Relatiemanagement, Deliverymanagement of het Shared Service Centrum. Zij werken op basis van principes en standaarden die voor alle projecten gelden.
Voor meer informatie over ICTU en verhalen van ICTU-medewerkers, zie www.ictu.nl.

Vacature: programmaleider Taskforce Bestuur en veilige dienstverlening.

Functie-omschrijving:

De programmaleider is verantwoordelijk voor de realisatie van de doelstellingen van de taskforce Bestuur en veilige dienstverlening.. Hij/zij rapporteert daarover aan de Bestuurlijke regiegroep E-overheid en dienstverlening en aan de directeur Burgerschap en Informatie

Functie-eisen:

- Is ervaren eindverantwoordelijk manager/ex-bestuurder
- Ervaren in het regisseren van interbestuurlijke processen
- Thuis in thema's informatieveiligheid en leer- en verankeringsprocessen
- Heeft (bestuurlijk) leidinggevende ervaring
- Verbinder van het netwerk
- Kan accountmanagement inrichten
- Kan een voor de taskforce relevant ambassadeursnetwerk organiseren
- ruime ervaring in omvangrijke (complexe) projecten / programmaportfolio's in meerdere projectmanagementrollen

- Ruime ervaring als leidinggevende en daarin succesvol

Vereiste competenties:

De projectdirecteur beschikt over de volgende competenties. Hij toont deze aan door middel van zijn CV en korte motivatie voor deze functie.

- Bestuurssensitiviteit
- Organisatiegericht aansturen
- Omgevingsbewustzijn
- Netwerkvaardigheid
- Samenbindend leiderschap
- Innovatief handelen

Werk-/denkniveau: WO

Opleidingsniveau: WO

Arbeidsvoorwaarden

Arbeidsvoorwaarden met betrekking tot het salaris.

Minimum salaris: € XXX bruto per maand

Maximum salaris: € XXX bruto per maand

Indicatie: Het genoemde salaris is gebaseerd op een volledige werkweek.

Dienstverband: (tijdelijke)aanstelling

Contractduur: tenminste 12 maanden met optie op verlenging /vaste aanstelling

Maximaal aantal uren per week: 36

Standplaats:

Den Haag

Vacature: Programmamanager Taskforce Bestuur en veilige dienstverlening.

Functie-omschrijving:

De programmamanager is verantwoordelijk voor de dagelijkse aansturing van de taskforce. Hij/zij vertaalt de programmering van de taskforce in haalbare doelstelling en resultaten. In die rol stuurt hij zowel de beleidsmedewerkers van de taskforce en heeft contacten met de voor programmering relevante partijen in het netwerk.amen met de programmaleider draagt hij op die wijze zorg voor de realisatie van de doelstellingen van de taskforce.

Functie-eisen:

- Kan leer- en verankeringsprocessen organiseren
- Kan leiding geven aan een programmatisch opgezette taskforce
- Kan netwerk betrekken bij uitvoering
- Is een gesprekspartner op diverse bestuurslagen
- Kan snel schakelen tussen bestuurs- en uitvoeringslagen

Vereiste competenties:

De projectmanager beschikt over de volgende competenties. Hij toont deze aan door middel van zijn CV en korte motivatie voor deze functie.

- Bestuurssensitiviteit
- Anticiperen
- Netwerkvaardigheid
- Organisatiegericht aansturen
- Innovatief handelen
- Omgevingsbewustzijn
- Samenwerken
- Resultaatgericht

Werk-/denkniveau: WO

Opleidingsniveau: WO

Salarisomschrijving:

Salarisschaal 14 t/m 15 afhankelijk van niveau en ervaring

Dienstverband: detachering vanuit de overheid

Periode: tenminste 12maandenmet optie tot verlenging

Maximaal aantal uren per week: 36

Standplaats:

Den Haag

Vacature: Senior beleidsmedewerker/ adviseur 'bestuurlijke en organisatorische procesvoering'Taskforce Bestuur en veilige dienstverlening.

Functie-omschrijving:

De senior beleidsmedewerker "bestuurlijk en organisatorische procesvoering' verantwoordelijk voor de activiteiten die gericht zijn op de blijvende bestuurlijke en organisatorische verankering van de informatieveiligheid,in wisselwerking met het programma van leren inzake informatieveiligheid. Als resultaat levert hij concrete bijdragen aan versterking van de planning en control cyclus in organisaties, ontwikkeling en functioneren van een visitatiestelsel etc. Hij/zij geeft deze activiteiten en producten vorm in nauwe samenwerking met diverse overheden, koepels en stelselpartijen. De senior beleidsmedewerker geeft daarnaast in nauw overleg met de programmaleiding vorm en inhoud aan het accountmanagement van één of meerdere voor de taskforce relevante overheidsdomeinen.

Functie-eisen:

Van senior beleidsmedewerker 'bestuurlijk en organisatorische procesvoering' wordt verwacht dat hij/zij aantoonbare, recente en relevante ervaring heeft met inrichten en verbeteren van planning en control, kwaliteit beleid, ook op het niveau van stelsels. Het is niet noodzakelijk dat deze ervaring is opgedaan bij de overheid. Relevante opleiding en/of werkervaring op het thema 'veiligheid van informatievoorziening' is een pré.

Vereiste competenties:

De senior beleidsmedewerker/ adviseur beschikt over de volgende competenties. Hij toont deze aan door middel van zijn CV en motivatie voor deze functie.

- Analyserend vermogen
- Overtuigingskracht
- Organisatiesensitiviteit
- Flexibiliteit
- Netwerkvaardigheid
- Plannen en Organiseren
- Innovatief handelen
- Omgevingsbewustzijn
- Samenwerken
- Resultaatgericht

Salarisomschrijving:

Salarisschaal 13 (afhankelijk van niveau en ervaring)

Dienstverband: detachering vanuit de overheid

Periode: tenminste 12maandenmet optie tot verlenging

Maximaal aantal uren per week: 36

Standplaats:

Den Haag

Vacature: Senior beleidsmedewerker/ adviseur 'Onderzoek en monitoring' Taskforce Bestuur en veilige dienstverlening.

Functie-omschrijving:

De senior beleidsmedewerker/ adviseur 'Onderzoek en monitoring' is binnen het programma van de Tarskforce verantwoordelijk voor het opzetten en begeleid van kennisprocessen. Het betreft onder meer onderzoek op het gebied van informatieveiligheid binnen de overheid en daarmee samenhangende wet en regelgeving. Daarnaast geeft hij/zij vorm en inhoud aan de opzet en uitvoering van een monitoringsystematiek. De onderzoeks- en monitoringsactiviteiten worden in nauw overleg met relevante stelselpartijen (NCNSC, IBD, CIP etc) opgezet en uitgevoerd. Daarnaast geeft hij/zij in nauw overleg met de programmaleiding vorm en inhoud aan het accountmanagement van één of meerdere voor de taskforce relevante overheidsdomeinen.

Functie-eisen:

Van de senior beleidsmedewerker Onderzoek en Monitoring wordt verwacht dat hij/zij beschikt over aantoonbare, recente en relevante ervaring met het inrichten van het uitvoeren van onderzoek en monitoring. Het is niet noodzakelijk dat deze ervaring is opgedaan bij de overheid. Relevante opleiding en/of werkervaring op het thema 'veiligheid van informatievoorziening' is een pré.

Vereiste competenties:

De senior beleidsmedewerker/ adviseur beschikt over de volgende competenties. Hij toont deze aan door middel van zijn CV en motivatie voor deze functie.

- Analyserend vermogen
- Overtuigingskracht
- Organisatiesensitiviteit
- Flexibiliteit
- Netwerkvaardigheid
- Plannen en Organiseren
- Innovatief handelen
- Omgevingsbewustzijn
- Samenwerken
- Resultaatgericht

Werk-/denkniveau: WO

Opleidingsniveau: WO

Salarisomschrijving:

Salarisschaal 12/ 13 afhankelijk van niveau en ervaring

Dienstverband: detachering vanuit de overheid

Periode: tenminste 12maandenmet optie tot verlenging

Maximaal aantal uren per week: 36

Standplaats:

Den Haag

Vacature: Senior beleidsmedewerker/ adviseur 'Leren' Taskforce Bestuur en veilige dienstverlening.

Functie-omschrijving:

De senior beleidsmedewerker/ adviseur 'Leren' is binnen het programma is verantwoordelijk voor het opzetten van activiteiten die gericht zijn op bewustwording, kennis en inzicht van informatieveiligheid(s)strategie binnen de overheid. De organisatie van bijvoorbeeld awarenessconferenties en de ontwikkeling van relevante leerproducten- en omgevingen behoren tot zijn takenpakket. Hij/zij geeft deze activiteiten vorm in nauwe samenwerking met diverse overheden, koepels en stelselpartijen. De senior beleidsmedewerker/ adviseur wordt hierin ondersteund door een kleine pool van medewerkers. Daarnaast geeft de senior beleidsmedewerker in nauw overleg met de programmaleiding vorm en inhoud aan het accountmanagement van één of meerdere voor de taskforce relevante overheidsdomeinen.

Functie-eisen:

De senior beleidsmedewerker beschikt over aantoonbare, recente en relevante ervaring op het inrichten van leerprocessen. Het is niet noodzakelijk dat deze ervaring is opgedaan bij de overheid. Relevante opleiding en/of werkervaring op het thema 'veiligheid van informatievoorziening' is een pré..

Vereiste competenties:

De senior beleidsmedewerker/ adviseur beschikt over de volgende competenties. Hij toont deze aan door middel van zijn CV en motivatie voor deze functie.

- Analyserend vermogen
- Overtuigingskracht
- Organisatiesensitiviteit

- Flexibiliteit
- Netwerkvaardigheid
- Plannen en Organiseren
- Innovatief handelen
- Omgevingsbewustzijn
- Samenwerken
- Resultaatgericht

Werk-/denkniveau: WO

Opleidingsniveau: WO

Salarisomschrijving:

Salarisschaal 13 (afhankelijk van niveau en ervaring)

Dienstverband: detachering vanuit de overheid

Periode: tenminste 12maandenmet optie tot verlenging

Maximaal aantal uren per week: 36

Standplaats:

Den Haag

Vacature: Senior beleidsmedewerker/ adviseur 'Informatiebeveiliging ' Taskforce Bestuur en veilige dienstverlening.

Functie-omschrijving:

De senior beleidsmedewerker/ adviseur Informatiebeveiliging is verantwoordelijk voor de hoogwaardige inbreng binnen het programma van leren, onderzoeken en verankeren van informatieveiligheid. Hij vertaalt strategische vraagstukken rond informatieveiligheid in de uitwerking van de producten 'leren, verankeren en monitoring'. In het bijzonder is hij/zij belast met bevordering van de overheidsbrede coördinatie en de advisering inzake informatieveiligheid binnen het werkgebied van de taskforce. In die zin onderhoudt hij de relatie met onder meer IBD en NCSC. De senior beleidsmedewerker geeft daarnaast in nauw overleg met de programmaleiding vorm en inhoud aan het accountmanagement van één of meerdere voor de taskforce relevante overheidsdomeinen

Functie-eisen:

De senior beleidsmedewerker beschikt over aantoonbare, recente en relevante ervaring op het beleidsterrein van informatieveiligheid. Het is niet noodzakelijk dat deze ervaring is opgedaan bij de overheid. Uiteraard is de goed thuis in het thema 'veiligheid van informatievoorziening' en kan dit aantonen vanuit relevante opleiding en/of werkervaring.

Vereiste competenties:

De senior beleidsmedewerker/ adviseur beschikt over de volgende competenties. Hij toont deze aan door middel van zijn CV en motivatie voor deze functie.

- Analyserend vermogen
- Overtuigingskracht
- Organisatiesensitiviteit
- Flexibiliteit
- Netwerkvaardigheid
- Plannen en Organiseren
- Innovatief handelen
- Omgevingsbewustzijn
- Samenwerken
- Resultaatgericht

Werk-/denkniveau: WO

Opleidingsniveau: WO

Salarisomschrijving:

Salarisschaal 12/ 13 afhankelijk van niveau en ervaring

Dienstverband: detachering vanuit de overheid

Periode: tenminste 12maandenmet optie tot verlenging

Maximaal aantal uren per week: 36

Standplaats:

Den Haag

Vacature: (drie maal) Beleidsmedewerker/ Medewerker Advisering Taskforce Bestuur en veilige dienstverlening

Functie-omschrijving:

De beleidsmedewerker draagt bij aan de ontwikkeling en inrichting van het programma van de taskforce in nauwe samenwerking met de senior beleidsmedewerkers/ adviseurs. De beleidsmedewerker geeft mede vorm en inhoud aan de inrichting en uitvoering van het programma door bijvoorbeeld het opleveren van beleidsnotities, door de opzet en organisatie van conferenties; werkbijeenkomsten etc. Beleidsmedewerkers kunnen worden ingezet op alle aandachtsgebieden

van de taksforce. De beleidsmedewerkers geven samen met de senior beleidsmedewerkers/ adviseurs invulling aan accountmanagementtaken van de taskforce

Functie-eisen:

De beleidsmedewerker beschikt over expertise op het gebied van informatiebeveiliging en/of leerprocessen, onderzoek en monitoring en/of processen van organisatieverbetering. Hetzij door relevante opleiding; hetzij door relevante recente werkervaring. De beleidsmedewerkers weten van aanpakken en zijn resultaatgerichte doeners.

Vereiste competenties:

De beleidsmedewerker/ medewerker advisering beschikt over de volgende competenties. Hij toont deze aan door middel van zijn CV en motivatie voor deze functie.

- Klantgerichtheid
- Analyserend vermogen
- Plannen en organiseren\
- Leervermogen
- Innovatief handelen
- Omgevingsbewustzijn
- Samenwerken
- Resultaatgericht

Werk-/denkniveau: WO

Opleidingsniveau: WO

Arbeidsvoorwaarden

Salarisschaal 10 t/m 11 afhankelijk van niveau en ervaring

Dienstverband: detachering vanuit de overheid

Periode: tenminste 12maanden met optie tot verlenging

Maximaal aantal uren per week: 36

Standplaats:

Den Haag

Vacature: (Senior) Adviseur Communicatie Taskforce Bestuur en veilige dienstverlening.

Functie-omschrijving:

De adviseur communicatie geeft vorm en inhoud aan de communicatiestrategie van de taskforce. De adviseur weet deze strategie te operationaliseren door het ontwikkelen en inzetten van diverse communicatie-instrumenten.

Functie-eisen:

De (senior) adviseur communicatie beschikt over expertise op het gebied van communicatiestrategie en de operationalisering daarvan. De adviseur communicatie heeft affiniteit met leer- of verankeringsstrategie. Ervaring met communiceren over informatieveiligheid is een pré.

Vereiste competenties:

De (senior) adviseur communicatie beschikt over de volgende competenties. Hij toont deze aan door middel van zijn CV en motivatie voor deze functie.

- Analyserend vermogen
- Overtuigingskracht
- Organisatiesensitiviteit
- Flexibiliteit
- Netwerkvaardigheid
- Plannen en Organiseren
- Innovatief handelen
- Omgevingsbewustzijn
- Samenwerken
- Resultaatgericht

Werk-/denkniveau: WO/HBO

Opleidingsniveau: WO/HBO

Salarisomschrijving:

Salarisschaal 11 t/m 12 afhankelijk van niveau en ervaring

Dienstverband: detachering vanuit de overheid

Periode: tenminste 12maanden met optie tot verlenging

Maximaal aantal uren per week: 36

Standplaats:

Den Haag

8. Planning en controlcyclus

Bijgaand PDF bestand beschrijft de inrichting van de standaard P&C cyclus van ICTU.
Detailuitwerking vindt plaats bij de start van de taskforce.

Tekenbevoegdheid Project- en teammanagers

Binnen het inkoopproces heeft de teammanager mandaat om tot bepaalde drempelbedragen inkoopcontracten/-brieven te tekenen. Dit mandaat krijgt de teammanager van de directeur, die dit op haar beurt van het Bestuur heeft gekregen.

Boven de hieronder genoemde drempelbedragen, heeft de teammanager geen mandaat meer en tekent de directeur de genoemde documenten.

Voor het bepalen van de drempelbedragen geldt de raming van de kosten bij de aanbesteding. Dat wil zeggen: de initiële contractwaarde plus alle te verwachten uitbreidingen.

Het mandaat van de teammanager op het gebied van inkoop luidt – beknopt – als volgt:

Raamovereenkomsten	Onbeperkt mandaat.
Dynamisch Aankoopsysteem	Mandaat tot € 30.000 incl. BTW.
Enkelvoudig onderhands aanbesteden	Mandaat tot € 30.000 incl. BTW. N.B. Enkelvoudig onderhands aanbesteden is mogelijk tot € 50.000 incl. BTW. Wanneer de raming van de opdrachtwaarde meer dan € 30.000 en minder dan € 50.000 incl. BTW bedraagt, heeft de teammanager geen mandaat.
Meervoudig onderhands aanbesteden	Mandaat tot € 30.000 incl. BTW, wanneer gekozen wordt om de opdracht met die raming meervoudig onderhands aan te besteden, in plaats van enkelvoudig onderhands.
Europees aanbesteden	Geen mandaat.

9. Mandaatregeling
De navolgende tabel wordt gevuld in overleg met dir B&I. De tabel wordt beheerd door ICTU

FUNCTIE	NAAM	HANDTEKENING / D.D.	PARAAF / D.D.
Budgeteigenaar			
Plaatsvervangend budgeteigenaar Tot een maximum van			
Budgetbeheerder			
Plaatsvervangend budgetbeheerder			

Voor het aangaan van verplichtingen is wordt gebruik gemaakt van bestaande raamcontracten zoals die zijn afgesloten door ICTU. Het bestaande stappenplan van ICTU is leidend bij het aangaan van overeenkomsten met derden. Dit stappenplan is als pdf bestand bijgevoegd.

10. Huisvesting en werkplekken

ICTU draagt zorg voor de inrichting van een tiental werkplekken. Een huisvestingsplan is onderhanden en is medio december gereed. Werkplekken zijn beschikbaar vanaf 1 januari.

Het huisvestingsplan wordt toegevoegd aan deze bijlage

TASKFORCE

Bestuur & Informatieveiligheid Dienstverlening

Taskforce Bestuur en Informatieveiligheid Dienstverlening

Programmaplan

3 juni 2013

Versie 1.1

Rijksoverheid VNG Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Inhoudsopgave

versie	datum	wijziging
1.0	9 april 2013	initieel document t.b.v. IBWG 12 april 2013
1.1	3 juni 2013	Tekstuele aanpassingen en verplaatsing overheidslaag specifieke programmering naar losse bijlage.

1. Inleiding

Na de inbraak bij DigiNotar, in september 2011, hebben de ministers van BZK en V&J aan de Onderzoeksraad voor de Veiligheid verzocht om een onderzoek uit te voeren naar het belang van digitale veiligheid en naar de bijzondere verantwoordelijkheid die de overheid heeft in het waarborgen daarvan.

Op 28 juni 2012 heeft de Onderzoeksraad een rapport uitgebracht waarin staat dat overheidsorganisaties hun digitale veiligheid niet in alle gevallen op orde hebben en daarom die veiligheid niet kunnen waarborgen.

Voorts concludeert de Onderzoeksraad dat bestuurders van veel overheidsorganisaties er onvoldoende in slagen om sturing te geven aan een goede digitale veiligheidszorg. Dat komt ondermeer doordat zij zich te weinig bewust zijn van de dreigingen in het digitale domein en de gevolgen daarvan op de digitale dienstverlening.

De overheid moet zich bewust zijn van die risico's en daar ook actief naar handelen. Daarbij gaat het om het actief voeren van risicomanagement op het domein van digitale veiligheid. Bestuurders van overheidsorganisaties ontbreekt het vaak aan de kennis die zij nodig hebben om hun organisaties op dit terrein aan te sturen. Zij slagen er beter in sturing te geven aan digitale veiligheid, wanneer zij zich ervan bewust zijn dat dit een voorwaarde is voor de continuïteit van hun dienstverlening.

Op 13 februari 2013 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) formeel ingesteld en komt hiermee tegemoet aan de aanbeveling van de Onderzoeksraad voor de Veiligheid: 'daartoe moet u een programma ontwikkelen dat bestuurders van overheidsorganisaties doordringt van het belang van digitale veiligheid en hen te voorzien van voldoende inzicht en vaardigheden om hen in staat te stellen actief sturing te geven aan de beheersing van digitale veiligheid in hun organisatie'.

2. Samenvatting programmering: doelen

		2013				2014			
		1e	2e	3e	4e	1e	2e	3e	4e
1	1e (0-)meting na 1 jaar								
2	2e meting na 1,5 jaar								
3.	3e meting na 2 jaar								
4.	Adequate gerichtheid/bewustzijn op Informatieveiligheid overheidsorganisaties								
	• Gerichtheid op uitvoering Risico Analyse								
	• Gerichtheid op ontwikkeling informatieveiligheidsbeleid								
	• Gerichtheid op het uitvoering informatieveiligheidsbeleid								
	• Gerichtheid op verantwoordiging, control & toezicht								
	• Gerichtheid op verandering & bijstelling								
5.	Adequate verankering informatie-veiligheid in organisatie en overheidslaag								
	• Verankerde Risico Analyse								
	• Verankerde informatieveiligheidsbeleid								
	• Verankerde uitvoering informatie-beveiligheidsbeleid								
	• Verankerde systematiek van verantwoording controle en toezicht								
	• Verankerde systematiek van verandering & bijstelling								
6..	Adequate gerichtheid informatieveiligheid in ketens tussen overheidsorganisaties								
7.	Adequate verankering informatieveiligheid in ketens tussen overheidsorganisaties								
	Externe sturing								
	• Adequate ontwikkelde monitorings- • Systematiek								
	• Uitgevoerde gewenst onderzoek								
	• Uitgevoerde communicatie mbt gerichtheid en verankering								

3. Opdracht

De opdracht aan de is als volgt:

1. De bewustwording te versterken van bestuur en managementtop van de eisen aan informatie-veiligheid, met name ook vanuit maatschappelijke en politieke risico's.
2. Een leerstrategie uit te voeren voor een actieve gerichtheid van bestuur en ambtelijke top op adequate aanpak informatieveiligheid dienstverlening.
3. De lange termijn verankering van informatieveiligheid en gerichtheid daarop in de reguliere processen en informatieketens te versterken, waarbij gerichtheid op weerbaarheid en herstel deel zijn van die verankering. Een verplichtende vorm van zelfregulering per domein is het beoogde einddoel van die verankering.
4. De overheidsbrede coördinatie rond het stelsel van informatiebeveiliging te bevorderen en te adviseren over dit stelsel.
5. Voor zover nodig aanvullend onderzoek te doen verrichten.

De uiteindelijke invoering van de bovengenoemde opdracht is de de verantwoordelijkheid van de overheidslaag zelf. De Taskforce zal zich inspannen om waar nodig specifiek voor de verschillende overheidslagen de invoering van bovenstaande zaken op te zetten en uit te werken in een programmaering. De Taskforce acht zich verantwoordelijk voor het realiseren van het noodzakelijke proces om te komen tot de in punt drie genoemde 'verplichtende zelfregulering'.

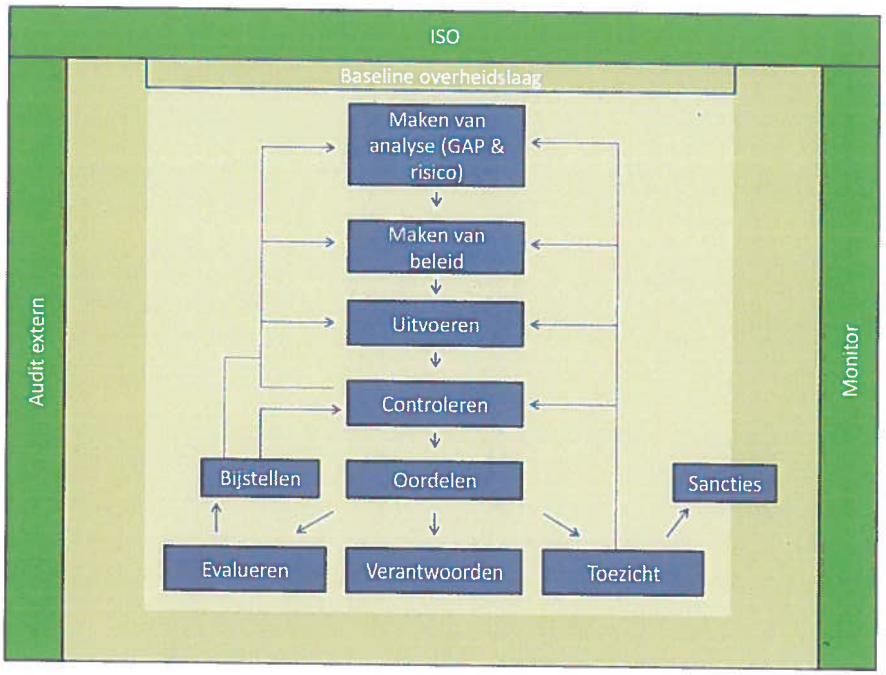
De Taskforce heeft op dringend verzoek van de betrokken overheden ook tot taak om de overheidsbrede coördinatie rond het stelsel van informatieveiligheid te bevorderen en waar nodig over het gehele beleid nader te adviseren.

4. Zelfregulering en leerstrategie

De minister van BZK heeft aangegeven na twee jaar de afweging te maken of wetgeving noodzakelijk is of niet. Een alternatief voor wetgeving is verplichtende zelfregulering per domein, waarvan de werking transparant is en die de minister in staat stelt zich over de werking van dit stelsel naar de Tweede Kamer te verantwoorden.

Verplichtende zelfregulering houdt in dat een bestuur of overheid vraagt om in bepaalde mate van zelf verantwoordelijk te zijn voor het bereiken van een met meerdere besturen of overheden afgesproken doel en daarbij zelf verantwoordelijk is voor benodigde invoering van wet- en/of regelgeving. Hierbij maakt het bestuur of de overheid zelf beleid. Daarbij wijst ze een externe partij aan die monitort. Een externe partij neemt waar nodig stappen om effectiviteit te waarborgen.

De opdracht van de Taskforce is geoperationaliseerd naar een strategie die moet uitmonden in stelsel van zelfregulering per organisatie en overheidslaag.



Figuur 1: Verplichtende zelfregulering bij informatieveiligheid

Verplichtende zelfregulering betekent in de praktijk dat in iedere overheidslaag en bijbehorende overheidsorganisaties beleid, afspraken en eventuele wet- en regelgeving wordt vastgelegd om informatieveiligheid te verbeteren, op een bepaald niveau te brengen, op de agenda van bestuurders te houden en te borgen. Zo moet een jaarlijkse cyclus worden geborgd, waarin ambtelijke en bestuurlijke oordeelsvorming over informatieveiligheid plaatsvindt. Daarin is bovendien een verbeteraanpak neergelegd. In deze cyclus van analyseren, plannen, uitvoeren, controleren en bijstellen wordt in eerste instantie een risicoanalyse opgesteld. Op basis van deze analyse kan beleid worden geformuleerd in een beleidsplan èn een implementatieplan. In dit beleid worden de normen voor de organisatie toegepast. Er wordt gericht op dit beleid en deze normen gestuurd, waarbij gebruik wordt gemaakt van een eenduidige meldingsystematiek. Met regelmaat wordt het beleid geëvalueerd door middel van controle, verantwoording en toezicht op beleid en de uitvoering daarvan.

De organisatie doet dat zelf, maar een externe vorm van toetsing gericht op blijvende scherpte is eveneens onderdeel. Daar waar nodig zal het beleid moeten worden bijgesteld.

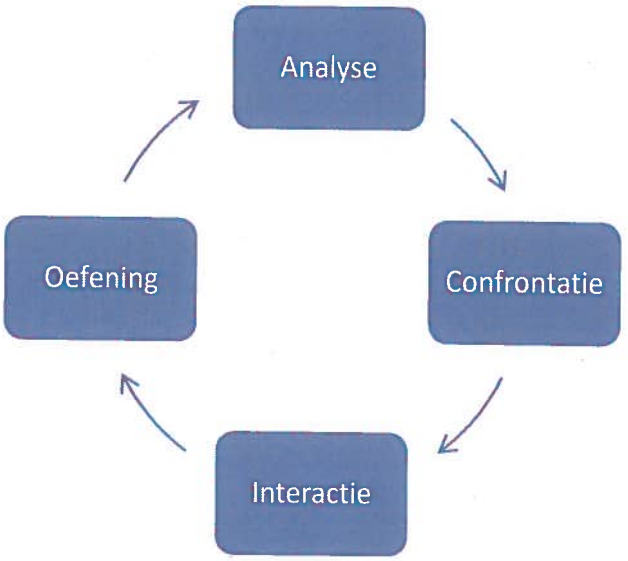
Uitgangspunten:

1. Een normatieve basis per organisatie en per overheidslaag (ISO 27001 en ISO 27002).
2. Een verankering van deze normatiek,ook als basis voor risicoanalyse. Elke betrokken organisatie regelt de informatieveiligheid op adequaat niveau. Op het niveau van de overheidslagen is er een stelsel van afspraken over de verantwoordelijkheid hierbij van koepelorganisaties. Op landelijk niveau belegde en daarvoor ingerichte voorzieningen faciliteren deze zelfregulering.
3. Een door de overheidslaag zelf opgelegde auditing is hierbij een belangrijk instrument. De ontwikkeling van een stelsel van single audit is een stimulerende factor voor zelfregulering . Single audit betekent dat de verschillende audits waaraan de organisatie onderworpen is en die zich richt op hetzelfde object, zoals informatie(beveiliging), zoveel mogelijk tot één audit worden samengevoegd om dubbeling en onnodige administratieve last te voorkomen. Dit streven vindt zo veel als mogelijk plaats.
4. Elke organisatie, nader ondersteund per overheidslaag, traint regulier op een actieve gerichtheid van bestuur, management, ICT-functionarissen en andere medewerkers op informatieveiligheid.
5. Voor elke organisatie en elke overheidslaag is een probleemanalyse en veranderplan opgesteld dat uiteindelijk leidt tot een verplichtende zelfregulering van informatieveiligheid.

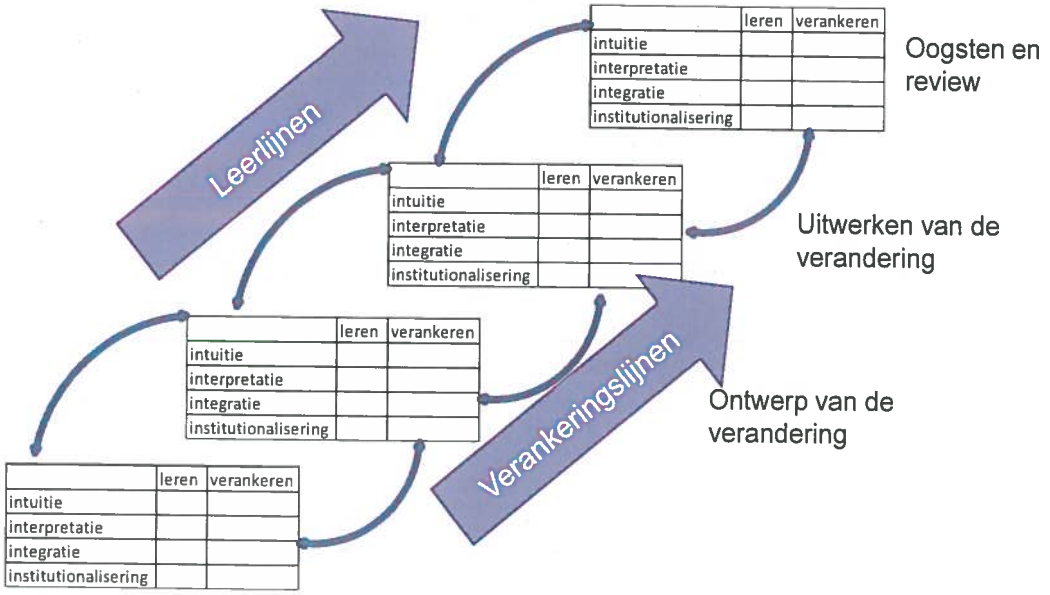
Leerstrategie

Het einddoel van de Taskforce is dus om per overheidslaag en organisatie te komen tot wat genoemd is 'verplichtende zelfregulering van de informatieveiligheid'. De verandercyclus om dit te bereiken loopt van nadruk op bewustwording en het verkrijgen van inzicht en kennis, naar verankering. De Taskforce ontwikkelt daartoe een leerstrategie en biedt deze aan de overheden en overheidsorganisaties aan. De leerstrategie biedt een proces van bewustwording tot verankering aan.

Verandercyclus



De zelfregulering komt de komende twee jaar tot stand door een iteratief proces van 'leren' en 'het verankeren' daarvan in de organisatie en het overheidslaag.



Figuur 3: leren en verankeren

Doelgroepen

In de uitwerking van de leerstrategie is het wenselijk een onderscheid te maken naar verschillende doelgroepen, die een verschillende benadering vragen:

- Bestuurders
- Topmanagement zoals gemeentesecretaris en directeuren
- CIO en ICT-management
- ICT-professionals
- Alle medewerkers; eventueel nadere specificatie

Eindproducten

- Een vastgesteld en geaccepteerd geharmoniseerd normenkader gebaseerd op NEN 27001 en 27002 per overheidslaag.
- De implementatie daarvan binnen de overheidslagen is gaande in alle organisaties
- Per overheidslaag een werkende en geaccepteerde systematiek om de voortgang van de implementatie te meten en inzichtelijk te maken, en zichtbaar gebruik hiervan, zodat inzicht bestaat over de stand van zaken op ieder moment.
- In de ieder overheidsorganisatie is toetsing op informatieveiligheid onderdeel van het jaarlijkse auditing proces.

- Daartoe is er een geharmoniseerd maar per domein specifiek ontwikkelde systematiek voor peer-reviewing en self-assessments, alsook eventueel andere vormen van externe auditing. Een voor elke organisatie uitgevoerde visitatie gericht op het vaststellen van de verplichtende zelfregulering kan daar deel van uit maken.
- Een overdrachtsrapportage van de Taskforce waarin per overheidslaag de bereikte resultaten worden geduid en geaccepteerde voorstellen zijn opgenomen over hoe het bereikte resultaat regulier wordt verankerd.

De missie van de Taskforce is na twee jaar geslaagd wanneer alle overheidslagen en overheidsorganisaties gezamenlijk een solide basis hebben gelegd voor deze zelfregulering op het domein informatieveiligheid. In iedere organisatie moet een jaarlijkse cyclus zijn geborgd waarin ambtelijke en bestuurlijke oordeelsvorming over de informatieveiligheid en de aanpak van verbeterpunten plaats vindt. Er moet sprake zijn van een continu leerproces, mede gebaseerd op risicomanagement.

5. Werkwijze Taskforce en rol Taskforce

Op basis van de geformuleerde uitgangspunten uit hoofdstuk 3 dient een programmering tot stand te komen per overheidslaag die uiteindelijk leidt tot de beoogde zelfregulering voor die overheidslaag. Bij het opstellen van de programmeringen zijn de overheidslagen zelf verantwoordelijk en zijn derhalve ook de trekker. De programmering is niet 'iets van de Taskforce'. Wel zal de Taskforce met de betrokken partijen in de overheidslagen in gesprek gaan om zo spoedig mogelijk tot een concrete programmering en uitvoering te komen.

De Taskforce bouwt hierbij voort op de huidige initiatieven op informatieveiligheidsvlak van elk van de overheidslagen vanuit een intensieve samenwerking met de koepelorganisaties. Betrokken (koepel)organisaties zijn de Unie van Waterschappen, het IPO, de VNG, de Manifestgroep, en de Interdepartementale Commissie Chief Information Officers. Bovendien wordt nauw samengewerkt met betrokken organisaties op informatieveiligheidsvlak, zoals het Nationaal Cyber Security Centrum (NCSC),het Centrum Informatiebeveiliging en Privacybescherming (CIP), de Informatiebeveiligingsdienst voor gemeenten (IBD), het Waterschapshuis en Logius, het Agentschap van het Ministerie van BZK.

Rol van de Taskforce

De rol van de Taskforce is dus complementair aan die van de ontwikkelingen in de overheidslagen zelf, uitgaande van de programmering van de overheidslagen zelf naar zelfregulering. De Taskforce, met de leerstrategie als uitgangspunt, zal zich profileren als het interbestuurlijke voertuig (symbool en drager) van die ontwikkeling naar zelfregulering. Die positionering behelst twee rollen:

1. *Hulp bieden bij de ontwikkeling naar zelfregulering*

De Taskforce stelt zich tot doel het veiligheidsbewustzijn te bevorderen, met verplichtende zelf-regulering als eindbeeld, aanvullend op de initiatieven die door bestaande partijen zijn ontplooid. De Taskforce organiseert activiteiten die de betreffende ontwikkeling stimuleren. Het betreft onder andere:

- het afstemmen van activiteiten van deze partijen in de diverse overheidslagen;
- het stimuleren van hergebruik van ontwikkeld materiaal dat zich richt op de bevordering van bewustzijn over informatiemanagement (richtlijnen, formats, trainingen, conferenties, etc.);
- het identificeren van witte vlekken in de ontwikkeling van informatieveiligheid binnen de domeinen en in samenwerking met genoemde partijen in te zetten op invulling daarvan;
- het helpen om ontwikkelde producten en systemen voor zelfregulering uiteindelijk te beleggen binnen de bestaande lijnorganisaties;
- het waar nodig (doen) ontwikkelen van leer- en verankeringsactiviteiten in aanvulling op en in samenwerking met bestaande organisaties;
- het organiseren van congressen; workshops; peer-to-peer-sessies die de ontwikkeling van informatieveiligheid in het overheidsdomein bevorderen;
- het stroomlijnen van bestaande normen- en auditstelsels rond informatieveiligheid.

2. *Monitoren, signaleren en dialoog voeren over voortgang*

De tweede rol is dat de Taskforce bijdraagt aan het niet-vrijblijvende karakter van de ontwikkeling naar zelfregulering. De Taskforce gaat dan ook overleggen met de betreffende instanties over het tot stand komen van een programmering, het monitoren van de voortgang van de ontwikkeling naar zelfregulering en daarover de dialoog te voeren.

6. Generieke programmering

De Taskforce BID heeft als opdracht informatieveiligheid en de gerichtheid daarop in de reguliere processen en informatieketens te verankeren. Een verplichtende vorm van zelfregulering per domein is het beoogde einddoel van die verankering. Omwille van eenduidigheid en efficiëntie zet de Taskforce in op een generieke programmering op die ze vervolgens vertaalt naar de specifieke situatie van elke overheidslaag. De generieke programmering werkt aan twee sporen: adequate gerichtheid op informatieveiligheid en adequate verankering van informatieveiligheid.

Voor iedere overheidslaag wordt een accountmanager aangewezen vanuit de Taskforce. Deze bekijkt samen met de overheidslaag wat de huidige situatie is in die overheidslaag en welke doelstellingen bereikt moeten worden om te komen tot het gezamenlijk vastgestelde noodzakelijke niveau van bewustzijn en informatieveiligheid. De generieke programmering geeft de ideale volgorde in behalen van doelstellingen en inzet van instrumenten aan.

Ontwikkeling van een aantal instrumenten en workshops gebeurt overheidslaag overstijgend. Andere instrumenten en workshops worden aangepast aan de overheidslaag en de daar geldende norm.

Samen bekijken accountmanager en overheidslaag welke bestaande netwerken/gremia en initiatieven gebruikt kunnen worden als platform voor workshops, bewustwordingpresentaties en lancering van producten binnen een overheidslaag.

Uitgangspunten specifieke programmering

1. Programmering is specifiek voor de verantwoordelijkheid van een overheidslaag;
2. Programmering start daar waar er al energie of beweging is (projecten, initiatieven, bestuurlijke thema's) binnen een overheidslaag;
3. Programmering is zoveel mogelijk gericht op bestaande netwerken en gremia (conferenties, opleidingen, vergaderingen, vakbladen, nieuwsbrieven) binnen een overheidslaag;
4. Programmering neemt norm als uitgangspunt, overheidslaag is verantwoordelijk voor implementatie;
5. Programmering richt zich op co-creatie met pioniers en faciliteren van beginners.

Leerproces

Samen met een groep pioniers en een groep beginners zal in elke overheidslaag via pilots het opleidingsaanbod en de verankeringsinstrumenten. Via learn and share bijeenkomsten tussen overheidslagen stimuleert de Taskforce BID het wederzijds leren, afkijken en het hergebruik.

Format Generieke programmering t.b.v. domeinspecifieke invulling

Maak een analyse van de huidige situatie van de overheidslaag (Fase 0)

Is er een cyclus van informatiebeveiliging? Ja → Welke stappen heeft de overheidslaag al gezet?

Nee ↓ Van risicoanalyse tot bijstellen

Kies bijbehorende faciliteiten vanuit

Start bij Fase 1 Taskforce volgens volgend format

Beschrijving fasen

Fase 0:

Gerichtheid:
- dialoog over verplichtende zelfregulering binnen overheidslaag

Verankeren:
- analyse van huidige stand van zaken, rollen en verantwoordelijkheden,

Fase 1:

Gerichtheid:
- bewustzijn over belang normatieve basis en zelfregulering
- eerste bewustzijn rondom belang van een actieve rol bestuurders

Verankeren:
- Baseline (term als eindproduct is nu: geharmoniseerd normenkader)
- meldingssystematiek voor overheidslaag beschikbaar
- besluitvorming over verplichtende zelfregulering binnen overheidslaag
- DigiD assessment ingepland

Fase 2:

Gerichtheid:
- Vaardigheden om te sturen op totstandkoming van risico-analyse en beleidsplan
- Vaardigheden voor melden aan koepelorganisatie en stelselpartijen
- Bewustzijn van belang controlemechanismen

Verankeren:
- Toegepaste risico-analyse
- (Aangepast) Beleid op gebied van informatieveiligheid
- Overheidslaag meldt incidenten en crises bij juiste instantie
- DigiD assessment afgerond

Fase 3:

Gerichtheid:
- Vaardigheden om te sturen op implementatie van de norm
- Vaardigheden om te sturen op controlemechanismen

Verankeren:
- Eerste 5 bedrijfsprocessen voldoen aan norm (implementatie norm)
- Self-assessment op deze 5 bedrijfsprocessen
- Calamiteitenoefening op deze 5 bedrijfsprocessen

Fase 4:

Gerichtheid:
- Vaardigheden om te sturen op incidentenmanagement
- Vaardigheden om integraal te sturen op leren van incidenten en bijstelling

Verankeren:
- Eerste 10 bedrijfsprocessen voldoen aan norm
- Peer reviews op deze 10 bedrijfsprocessen
- Calamiteitenoefening op deze 10 bedrijfsprocessen (implementatie norm)
- (Aangepast) Incidentenmanagement en responsbeleid
- Check interne auditor

Fase 5:

Gerichtheid:
- Bewustzijn en bekwaamheid rondom informatieveiligheid bij bestuurders en topmanagers
- Bijstellingsproces en –plan rondom integraal leren
- Trainingsplan voor organisatie

Verankeren:
- Solide basis voor zelfregulering in verplichtende vorm
  a. Geïmplementeerde baseline
  b. Toegepaste systematiek controlemechanismen
  c. Toegepaste systematiek voor bijstellen
  d. Jaarlijkse audit
  e. Externe visitatie gepland

Doelstellingen per fase

Fase	Gerichtheid	Verankeren
Fase 0	• Belangenorganisatie/koepel voelt zich verantwoordelijk voor verplichtende zelfregulering in haar overheidslaag	• Belangenorganisatie/koepel ondersteunt overheidslaag bij op pijl houden van de informatieveiligheid (via handreikingen, etc.)
Fase 1	• Bestuurders en topmanagers weten wat informatieveiligheid in de breedte inhoud • Bestuurders en topmanagers (h)erkennen het belang van informatieveiligheid • Bestuurders en topmanagers (h)erkennen het belang van zelfregulering • Bestuurders en topmanagers melden incidenten bij de juiste instanties • Bestuurders en topmanagers (h)erkennen de noodzaak tot sturen • Bestuurders en topmanagers zien het belang van een actieve rol bij informatieveiligheid • Bestuurders en topmanagers (h)erkennen problemen/risico's binnen eigen organisatie	• Belangenorganisatie/koepelorganisatie stelt voorstel voor invulling verplichtende zelfregulering vast binnen overheidslaag • Bestuurders en topmanagers kunnen incidenten melden bij de juiste instanties • Bestuurders en topmanagers stellen de juiste stuurvragen bij incidenten of calamiteiten • Bestuurders en topmanagers spelen een actieve rol binnen de organisatie bij informatieveiligheid • Bestuurders en topmanagers sturen op het maken van een risicoanalyse binnen eigen organisatie
Fase 2	• Bestuurders en topmanagers weten welke stuurvragen ze kunnen stellen voor optimale informatieveiligheid • Bestuurders en topmanagers zien het belang van een normatieve basis • Bestuurders en topmanagers (h)erkennen het belang van een werkend stelsel van informatieveiligheid • Bestuurders en topmanagers willen rapporteren aan domein en stelsel • Bestuurders en topmanagers kunnen rapporteren aan domein en stelsel	• Bestuurders en topmanagers stellen de juiste stuurvragen voor optimale informatieveiligheid • Bestuurders en topmanagers hebben handreikingen om te sturen op optimaliseren van beleidsplan Informatieveiligheid • Belangenorganisatie/koepel rapporteert elk half jaar aan het Stelsel over het niveau van informatieveiligheid en verplichtende zelfregulering • Bestuurders en topmanagers melden incidenten bij de daarvoor ingestelde instanties

Fase 3	• Bestuurders en topmanagers kunnen sturen op implementatie en uitvoering van een norm • Bestuurders en topmanagers kennen de verantwoordelijken voor informatieveiligheid in de uitvoering • Bestuurders en topmanagers kunnen sturen op het aanscherpen van uitvoeringsprocessen op informatieveiligheid • Bestuurders en topmanagers zien het belang van controlemechanismen	• Bestuurders en topmanagers sturen op implementatie en naleving van het normenkader • Bestuurders en topmanagers hebben maandelijks contact met de verantwoordelijken voor informatieveiligheid in de uitvoering • Bestuurders en topmanagers sturen op het aanscherpen van uitvoeringsprocessen op informatieveiligheid • Overheden hebben incidentmanagement en responsbeleid op gebied van informatieveiligheid • Bestuurders en topmanagers stellen de juiste stuurvragen bij incidenten of calamiteiten • Belangenorganisatie/koepel rapporteert elk half jaar aan het Stelsel over het niveau van informatieveiligheid en verplichtende zelfregulering
Fase 4	• Bestuurders en topmanagers kunnen integraal sturen op leren van incidenten en bijstelling • Bestuurders en topmanagers kunnen sturen op implementatie en uitvoering van een norm • Bestuurders en topmanagers kunnen sturen op het aanscherpen van uitvoeringsprocessen op informatieveiligheid • Bestuurders en topmanagers zien het belang van controlemechanismen	• Overheden houden elk jaar een calamiteitenoefening op gebied van informatieveiligheid • Overheden hebben incidentmanagement en responsbeleid op gebied van informatieveiligheid • Overheden hebben een continuïteitsplan rondom informatieveiligheid • Overheden zetten elk half jaar een controlemechanisme als interne check in • Overheden evalueren voor elke kwartaalrapportage de zelfregulering en het niveau van informatieveiligheid en stellen waar nodig bij • Overheden zorgen elke 5 jaar voor een externe visitatie op gebied van informatieveiligheid • Overheden hebben het onderwerp informatieveiligheid ingebed in al hun procedures.
Fase 5	• Overheden trainen periodiek op informatieveiligheid • Bestuurders en topmanagers gaan periodiek in dialoog over innovatie op gebied van informatieveiligheid met CISO/informatiebeveiligers.	• Overheden hebben solide basis voor verplichtende zelfregulering

7.Opleidingsaanbod en instrumenten

De Taskforce heeft als opdracht informatieveiligheid en de gerichtheid daarop in de reguliere processen en informatieketens te verankeren. Hiervoor zet de Taskforce een generieke programmering met generieke middelen in die ze vervolgens vertaalt naar de specifieke situatie van elke overheidslaag.

Het middelen aanbod van de Taskforce bestaat uit bestaande middelen, zoals opleidingen of best practices, en nieuw aanbod. De Taskforce heeft haar aanbod samengesteld op basis van opgehaalde behoeften op grond van het concept verplichtende zelfregulering, bestaande normenkaders en gesprekken binnen overheidslagen.

Behoeften binnen overheid

Uit gesprekken met verschillende doelgroepen binnen de overheidslagen kwam de volgende behoefte naar voren:

- Uniformering van normenkaders
- Meer kunnen sturen vanuit risicobewustzijn en risico-omgang
- Hulp bij bedenken en formuleren stuurvragen informatieveiligheid
- Gat dichten tussen bestuur en techniek: zelfde taal leren spreken
- Aansluiten bij huidige bestuurlijke thema's en projecten
- Focus op continuïteit en kwaliteit
- Samenwerking intern en extern stimuleren
- Hergebruik van aanpakken en opleidingen

Randvoorwaarden voor verandering

Betekenisgeving binnen organisatie
- besef van en inzicht in breedte van informatieveiligheid
- besef van en inzicht in belangen bij informatieveiligheid
- besef van en inzicht in risico's en sterktes
- stimuleren en waarderen van gewenst gedrag

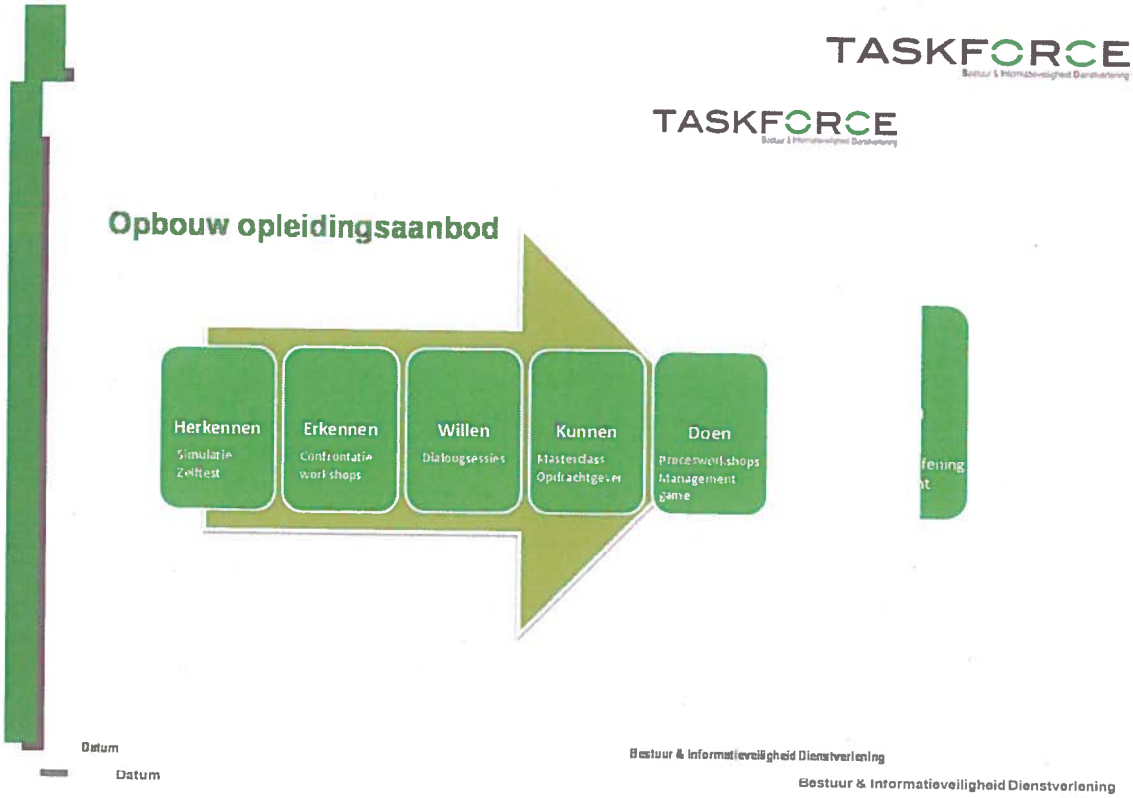
Inbedding in organisatie
- nadrukkelijke (voorbeeld)rol van bestuur en topmanagement
- vanuit eigen organisatiedoelen en -structuren veranderen
- samenwerken binnen organisatie
- wederzijds willen afkijken, ook van andere terreinen

Aanbod

Het aanbod van middelen bestaat uit twee delen:
- opleidingaanbod;
- verankeringinstrumenten.

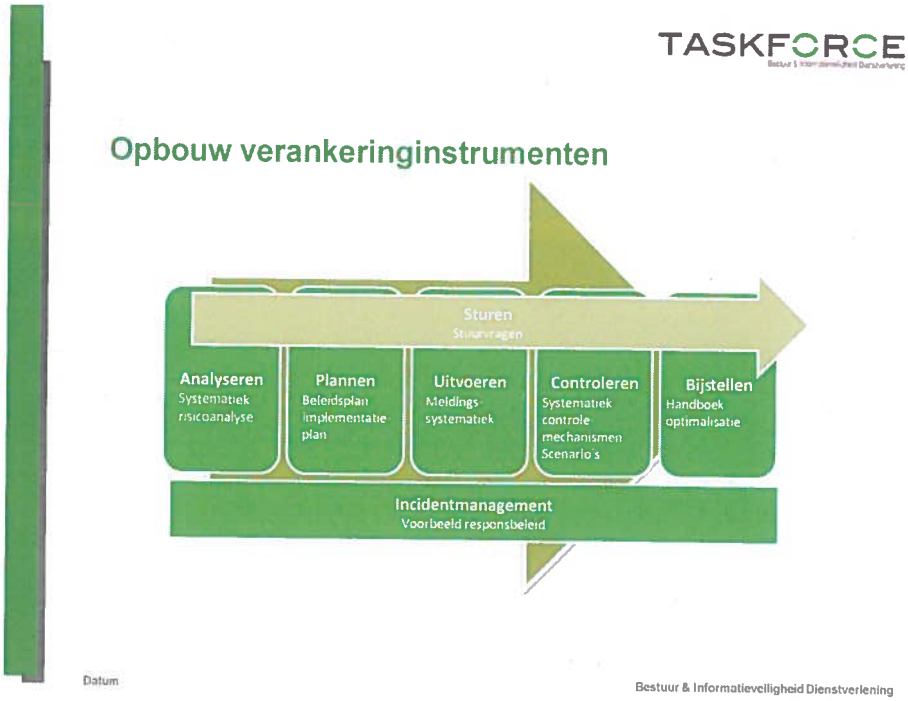
Opleidingsaanbod:

- Simulatie (NCSC)
- Zelftest (iBOB)
- Confrontatieworkshop
- Dialoogsessie bestuur/topmanagement – CISO
- Risicobewustzijn sessie
- Procesworkshops
- Verankersessie
- Management game (oefening)



Verankeringinstrumenten:

- Best practices:
  - Systematiek voor risicoanalyse
  - Beleidsplannen informatieveiligheid
  - Ingericht Incendent Responsmanagement
  - Implementatieplan informatieveiligheid
- Handreikingen:
  - Handboek optimalisatie processen en procedures
  - Top 10 stuurvragen voor informatieveiligheid
  - Top 10 stuurvragen bij incidenten en calamiteiten
  - Oefenscenario's calamiteiten en incidenten
- Meldingssystematiek incidenten (Stelsel breed)
- Systematiek voor controlemechanismen
- Systematiek voor veranderen en bijstellen



Pilots

Het opleidingsaanbod en een aantal verankeringinstrumenten zullen getoetst worden in een zestal pilots. In de pilots bekijken de Taskforce en overheidslagen of het aanbod genoeg aansluit bij de dagelijkse praktijk en welke mix wanneer het meest effectief is. Tijdens de pilots delen de deelnemende overheidslagen hun ervaringen via blogs en interviews.

Planning 2013

2013	april	mei	juni	juli	augustus	sept	okt	nov	dec
Ontwikkelen zelftest, confrontatieworkshops en dialoogsessies, risicobwustzijn sessie									
Ontwikkelen systematiek risicoanalyse, meldingssystematiek, format beleidsplan, implementieplan									
Pilots									
Toepassing aanbod									
Ontwikkelen handreikingen, systematiek voor controlemechanismen									
Ontwikkelen procesworkshop, verankersessie									
Pilots									
Toepassing									

8.Monitoring voortgang naar verplichtende zelfregulering

Taskforce en monitoring

De Taskforce heeft als opdracht informatieveiligheid en de gerichtheid van bestuur en topmanagement daarop in de reguliere processen en informatieketens van hun organisatie te verankeren. Een verplichtende vorm van zelfregulering voor elke overheidslaag (Rijk, Provincies, Gemeenten, ZBO's en Waterschappen) is het beoogde einddoel van die verankering. Dat is geen vrijblijvende doelstelling. Gedurende de looptijd van de taskforce (2013-2015) dienen organisaties en overheidslagen voldoende voortgang van naar "verplichtende zelfregulering" geboekt te hebben, anders zal de stelselverantwoordelijke (minister van BZK) zich nader beraden over de invoering van wet- en regelgeving.

Doelstelling

Het doel van het monitoringonderzoek is tweeledig:

1. Explorerend: inzicht krijgen in het niveau van en de voortgang van organisaties en overheidslagen in het realiseren van verplichtende zelfregulering op het thema informatieveiligheid
2. Informerend: de resultaten van het onderzoek dienen gerapporteerd te worden aan de stelselverantwoordelijke, overheidsorganisaties en koepelorganisaties binnen de verschillende overheidslagen.

Vraagstelling

De centrale vraagstelling in dit onderzoek luidt:

"Wat is het niveau en de voortgang van organisaties en overheidslagen naar verplichtende zelfregulering omtrent het waarborgen van informatieveiligheid?"

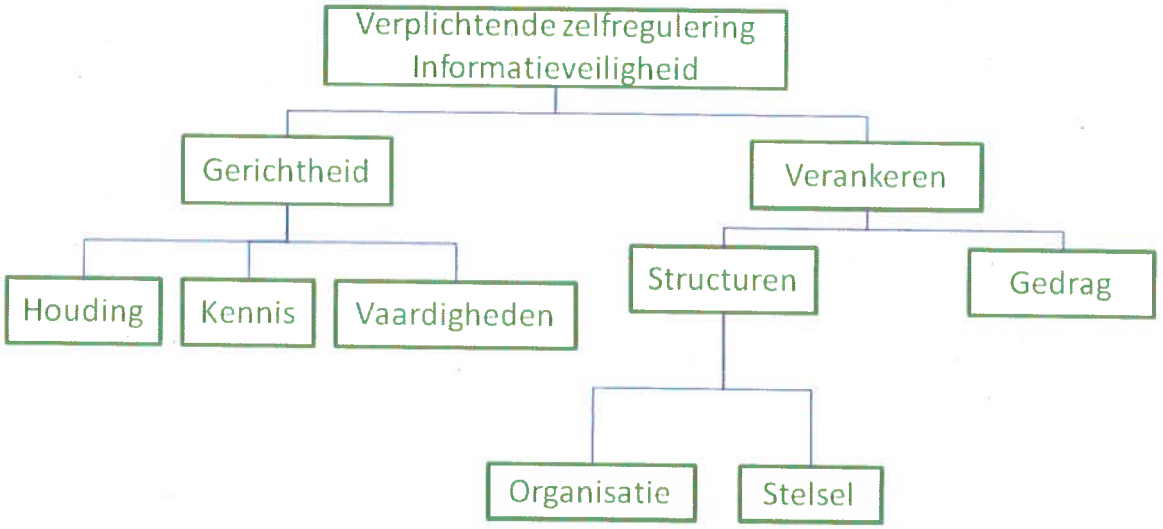
Conform de programmering van de Taskforce onderscheidt het onderzoek naar de voortgang naar verplichtende zelfregulering twee sporen van ontwikkeling: 1)gerichtheid van bestuurders en topmanagement op en 2) de verankering van informatieveiligheid in een organisatie op strategisch en tactisch niveau. Een belangrijk onderdeel van de programmering vormt de ontwikkeling en implementatie van een overheidslaag specifieke norm (BIR, BIG, etc) op het gebied van informatiebeveiliging. De vraagstelling is nader te concretiseren in 3 onderzoeksvragen:

- Is er gedurende de periode van 2013-2015, sprake van een verbetering van gerichtheid op het thema informatieveiligheid, door bestuurders en topmanagent van overheidsorganisaties in de overheidslagen (Rijk, Provincies, Gemeenten, ZBO's en Waterschappen)?
- Is informatieveiligheid sterker verankerd op strategisch en tactisch besturingsniveau binnen overheidsorganisaties in de overheidslagen (Rijk, Provincies, Gemeenten, ZBO's en Waterschappen) gedurende de periode van 2013-2015?
- Hebben overheidsorganisaties en overheidslagen(Rijk, Provincies, Gemeenten, ZBO's en Waterschappen) voortgang geboekt in het implementeren van een overheidslaag specifieke norm voor informatiebeveiliging gedurende de periode van 2013-2015?

Onderzoeksopzet

Dit monitoringsonderzoek beoogd het zelfregulerend vermogen van overheidsorganisaties op het gebied van informatieveiligheid, of de ontwikkeling daarvan, te meten in de periode 2013-2015.De Taskforce BID gaat er vanuit dat een adequate gerichtheid en verankering een vereiste zijn voor het slagen van zelfregulering door organisaties. De mate van gerichtheid blijkt uit de houding ten opzichte van informatieveiligheid en het bestaan van kennis en het beschikken over vaardigheden om hierop te kunnen sturen. De mate van verankering blijkt uit de realisatie van structuren in de organisatie en het stelsel en het gedrag van bestuurders inzake het borgen van informatieveiligheid. Een schematische weergave van de operationalisatie is te zien in de figuur hieronder.

Aansluitend op de programmering onderscheiden we in de ontwikkeling naar zelfregulering 5



volwassenheidsfasen van gerichtheid en verankering. De volwassenheid op gerichtheid en verankering geven samen de volwassenheid van het zelfregulerend vermogen van organisaties weer. De tabel hieronder geeft de conceptuele gedachte van dit groeimodel weer.

Overheidslaag	**Sporen**	**Volwassenheidsfasen**					
		Fase 0	Fase 1	Fase 2	Fase 3	Fase 4	Fase 5
Rijk	Gerichtheid						
	Verankering						
ZBO	Gerichtheid						
	Verankering						
Provincies	Gerichtheid						
	Verankering						
Gemeenten	Gerichtheid						
	Verankering						
Waterschappen	Gerichtheid						
	Verankering						

Vragenlijst

Op basis van de bovenstaande operationalisaties wordt door de Taskforce BID een vragenlijst ontwikkeld en uitgezet onder de doelgroep. In lijn met generieke programmering, beperkt de vragenlijst zich tot het meten van:

- De gerichtheid van bestuurders en topmanagement op informatieveiligheid
- De verankering van informatieveiligheid in organisaties op tactisch en strategisch besturingsniveau.
- De implementatie van een overheidslaagspecifieke norm op het gebied van informatieveiligheid

Om de antwoorden van organisaties te kunnen beoordelen en vertalen naar een objectieve en vergelijkbare meetresultaten, wordt tevens een score model ontwikkeld wat verschillende niveaus van zelfregulering onderscheidt. Om te kunnen rapporteren over de *voortgang* van organisaties naar verplichtende zelfregulering, dienen gedurende de looptijd van de Taskforce BID minimaal twee metingen uitgevoerd te worden bij elke organisatie.

Voordat de vragenlijst onder alle organisaties uit de doelgroep verspreid wordt , wordt eerst een pilot studie uitgevoerd onder enkele organisaties uit verschillende overheidslagen om de voor dit onderzoek ontwikkelde vragenlijst te testen.De inhoud van de vragenlijst en planning van het monitoringonderzoek zullen worden afgestemd worden met de bestuurslagen.

Planning

De onderstaande tabel geeft de werkzaamheden van het monitoringonderzoek weer.

	apr	mei	juni	juli	aug	sep	okt	nov	dec
Ontwikkelen vragenlijst									
Ontwikkelen scoremodel									
Afstemmen monitor IBR									
Afstemmen bestuurslagen									
Uitvoeren pilot									
Inzet monitoring instrument									
Rapportage									

	jan	feb	mrt	apr	mei	juni	juli	aug	sep	okt	nov	dec
Ontwikkelen vragenlijst												
Ontwikkelen scoremodel												
Afstemmen monitor IBR												
Afstemmen bestuurslagen												
Uitvoeren pilot												
Inzet monitoring instrument												
Rapportage												

9.Ketensturing

Alle overheidslagen zijn betrokken in ketens. . De interbestuurlijke werkgroep heeft een ketenwerkgroep ingesteld die wordt gefaciliteerd vanuit de Taskforce BID. Doel van die werkgroep is om te bewerkstelligen dat een vorm van coördinatie op informatieveiligheid in ketens tot stand komt. Deze lichte vorm van coördinatie wordt dan ingericht op basis van de principes van de verplichtende zelfregulering. De eerste bijeenkomst van de werkgroep Ketens heeft op 19 maart plaatsgevonden.

Het blijkt dat ketenvraagstukken vanuit meerdere invalshoeken worden benaderd. In ieder geval wordt vanuit NORA gewerkt aan een katern dat zich specifiek richt op de 'governance' van ketens. Logius; CWI, TNO en RUG werken samen in het TTISC onderzoek. Dit onderzoeksproject richt werkt aan een assurance-raamwerk voor ICT-ketenbeheersing, besturing en –control; een methodiek om zekerheid aan gebruik van ICT-ketens te kunnen verschaffen.

Naar aanleiding van discussie in de eerste werkgroepbijeenkomst stellen we de volgende opdrachtformulering op hoofdlijnen voor.

- Breng lopende initiatieven rond de 'governance' en informatieveiligheid van ketens in kaart
- Identificeer de top 10 kritische ketens op het gebied van dienstverlening en informatieveiligheid
- Breng per keten in kaart op welke wijze wordt voldaan aan de principes van verplichtende zelfregulering
- Formuleer een interbestuurlijke ketenprogrammering voor bestuurders.

De komende weken staan in het licht van het afstemming en verdere verdieping van deze opdrachtformulering met deelnemers aan deze werkgroep en vertaling daarvan in een plan van aanpak van een ketenprogrammering.

Deze programmering wordt afgestemd met de programmering rond verplichtende zelfregulering in de overige overheidslagen. Het is de ambitie van de Taskforce om waar mogelijk gebruik te maken van reeds ontwikkelde bruikbare producten. Denk daarbij aan onder andere het NORA katern; het TTISC onderzoek en de CIP groep ketens.

Wie zijn betrokken

Onderstaande organisaties nemen deel aan de werkgroep ketens.

- BZK (BK -B& I),
- BZK (OBR),
- Waterschappen,
- VNG,
- KING,
- BKWI,
- Logius,
- NCSC,
- Taskforce BID

De Taskforce is in gesprek met NORA om te bezien op welke wijze zij betrokken kan zijn bij de uitvoering van de aan de ketenwerkgroep verstrekte opdracht. Met CIP is nader overleg nodig over de invulling van haar vertegenwoordiging. Vanuit het provinciaal domein is nog geen vertegenwoordiging in de werkgroep afgevaardigd.

Wat wordt opgeleverd?

- Een plan van aanpak (eind mei)
- Een overzicht van de toepasbaarheid van lopende initatiatieven op het gebied van ketenbesturing voor het realiseren van verplichtende zelfregulering (medio juli)
- Een uitgewerkte programmering gericht op bestuurders waarin risicomanagement rond ketens centraal staat (november 2013) inclusief de uitvoering daarvan (april 2014)
- Een overzicht van de door de werkgroep aangegeven belangrijkste (dienstverleningsketens (juli 2013) voorzien van een analyse van de daarin optredende knelpunten op het gebied van risicomanagement en governance (december 2013)
- De inrichting van de per keten gewenste 'lichte coordinatie' (2014)

Wat is de timing

In onderstaande tabel is de timing van de werkzaamheden van de werkgroep weergegeven. Deze timing wordt verder uitgewerkt in het plan van aanpak dat uiterlijk 28 mei wordt opgeleverd ter besluitvorming. De nadere uitwerking van de programmering in activiteiten die zich richten op 'gerichtheid' en 'verankeren' zal in eerste aanleg in dat plan van aanpak zichtbaar zijn. Verdere detaillering vindt plaats binnen de activiteit 'ontwikkeling ketenprogrammering'.

	apr	mei	juni	juli	aug	sep	okt	nov	dec	jan	feb	mrt
Uitwerken plan van aanpak												
In kaart brengen lopende intiatieven												
Identificatie ketens												
Uitwerking verplichtende zelfregulering per keten												
Ontwikkeling ketenprogrammering												
Uitvoering keten programmering												
Inrichting 'lichte coordinatie'												

10.Single audit

Inleiding

Als normatieve basis voor de inrichting van en oordelen over de informatieveiligheid, geldt een van de ISO 27001/27002 afgeleide Baseline Informatieveiligheid per bestuurslaag . Elke betrokken organisatie kent op basis daarvan een reguliere (jaarlijkse) auditing van de kwaliteit van de informatieveiligheid. Op dit moment bestaan al voor de verschillende domeinen en ketens verschillende auditverplichtingen en er lijken er meer te volgen. De aanname is dat doormiddel van een 'single audit' systematiek de met de auditverplichtingen samenhangende (administratieve) lasten voor overheidsorganisaties beperkt kunnen worden. In het inrichtingsplan van de Taskforce is geadviseerd de auditverplichtingen te inventariseren en overheidslagen te faciliteren in het toe te werken naar een 'single audit' systematiek. In deze rapportage schetsen we een beeld van onze bevindingen rondom 'single audit' tot nu toe.

Single audit

Het belang van een efficiënte inrichting van het auditproces is voor alle overheidslagen van belang. De mate waarin de behoefte door de overheidslagen wordt gevoeld verschilt. Gemeenten geven aan een grote auditdruk te kennen. Vanuit departementen, waterschappen en provincies wordt deze auditdruk niet met dezelfde 'zwaarte' ervaren. Onderstaand schetsen we enkele ontwikkelingen die we in onze inventarisatieronde tot nu toe hebben opgehaald.

Gemeenten
Naast de reguliere audits die zich richten op financiële verantwoording bestaan voor gemeenten ook auditverplichtingen in het kader van BAG, GBA en DIGID. Het grootste bezwaar van gemeenten is dat het normenkader voor deze typen audit steeds is afgeleid vanuit eenzelfde normenstelsel, maar dat de accenten in de audit net anders zijn belegd. De organisatie van informatievoorziening wordt daardoor steeds opnieuw in de audit betrokken, maar dan net vanuit dat andere perspectief. Gemeenten pleiten er sterk voor om, gebaseerd op de BIG, te streven naar een single audit systematiek. Dat kan ook omdat de BIG ook normen bevat die de voortvloeien uit de auditbehoefte vanuit BAG en GBA.

BPR
BPR is verantwoordelijk voor het beheer van stelselvoorzieningen die samenhangen met persoonsregistraties. BPR monitort de uitvoering van GBA –audit bij gemeenten. . De audit is verplicht gesteld in de wet GBA. Deze wet wordt vernieuwd onder de naam wet BRP. Daarmee wordt ook de audit vernieuwd. Na invoering van de nieuwe wet BPR worden gemeenten wordt de bestaande audit vervangen door een systematiek van zelfevaluatie, die onder de huidige wet GBA al beproefd is. Vooruitlopend op de invoering van de wet op BRP is dit evaluatie-instrument al op de website beschikbaar.

Uitvoeringsinstellingen
De uitvoeringsinstellingen onderzoeken de mogelijkheid om bestaande normenkaders beter op elkaar af te stemmen. De CIP-domeingroep Normen ontwikkelt daartoe een model voor een uniforme, gestructureerde opbouw van normenkaders. Dit gebeurt door over het gehele landschap heen gelijke objecten te voorzien van standaard normeringen in een binnen alle kavels herkenbare structuur en in één syntax. Deze structuur en syntax zijn (her)bruikbaar voor elk te normeren object.

Het model richt zich niet meer op normenkaders voor kavels, maar op normenkaders voor objecten (waarvan kavels gebruik maken). Databases en webservices komen vaak in meerdere kavels voor; daar hoef je maar één keer uitgangspunten en normen voor te bepalen. De objecten van de NCSC-webrichtlijnen zijn in een eerste concept gereed. De eerste resultaten van deze domeingroep worden gepresenteerd op de CIP conferentie van 6 juni.

TTIC onderzoek
Daarnaast loopt een onderzoek naar beheersing van risico's en controls in ICT-ketens. Dit TTIC onderzoek wordt uitgevoerd door TNO en de Rijksuniversiteit Groningen in opdracht van Logius. Het onderzoek doet aanbevelingen op het gebied van de inrichting van governance en een daarbij passende assurance systematiek.

SISA systematiek
Gemeenten kennen sinds 2006 een kader voor financiële verslaggeving die zowel inzicht geeft in de gehele bedrijfsvoering als in specifieke departementale geldstromen. Beide onderwerpen worden in het jaarverslag van gemeenten opgenomen en zijn onderworpen aan accountantscontrole. De controle vindt in één procesgang plaats door de extern accountant van de gemeente. De daarop afgegeven verklaring geldt vervolgens als voldoende Assurance voor ook de departementale geldstromen. Deze regeling staat bekend als de SISA regeling. De auditdienst rijk (ADR) ziet toe op een correcte uitvoering van deze praktijk door extern accountants. Voordat deze regeling in werking trad was het voor gemeente noodzakelijk om voor elke departementale geldstroom een aparte accountantsverklaring te overleggen. De SISA regeling heeft dan ook bijgedragen aan een vermindering van de auditlast bij gemeenten en departementen. Een belangrijke onderliggende randvoorwaarde is geweest dat de stelselverantwoordelijkheid van respectievelijk de ministers van BZK, Financiën en overige departementen goed zijn belegd. Daarnaast is de coördinerende rol van de ADR een randvoorwaarde voor het goed functioneren van deze systematiek.

Wat nu te doen?

Het in gang gezette onderzoek door CIP geeft handvatten voor een gestroomlijnd normenkader. Het onderzoek van het TICC wordt ondermeer onderzocht hoe assurance binnen ketens vormgegeven kan worden. Dat deze initiatieven kunnen bijdragen aan het verlagen van de auditlast ligt voor de hand. We hebben daar echter nog geen eenduidig beeld van. Ook de ontwikkeling van de BIG draagt bij aan vereenvoudiging van het auditkader in het gemeentelijk domein. Kritisch is daar wel het tempo waarmee dit normenkader kan worden geïmplementeerd. Dit geldt ook voor de ontwikkeling en implementatie van vergelijkbare normenkaders in de overige domeinen (departementen; waterschappen; provincies). Hoe precies de ontwikkeling van normenkaders CIP gelijke tred (kan) houdt(en) met de ontwikkeling en implementatie van de BIR, BIG etc hebben we nog niet helder voor ogen.

Of en in hoeverre het haalbaar is om toe te werken naar een op SISA gelijkende single audit systematiek voor vraagstukken rond informatieveiligheid en de principes van verplichtende zelfregulering vergt nader onderzoek. Niet alleen onderzoek omtrent de afstemming van de normenkaders en audit verplichtingen, maar zeker ook naar afstemming op het bestuurlijke vlak en met stakeholders.

Zo dient er nagedacht te worden wie de opdrachtgever en opdrachtnemer zijn bij het ontwikkelen van een single audit systematiek voor informatieveiligheid en welke rol Taskforce BID vervult. De rol van de Taskforce BID is in principe faciliteiterend, maar zij zou een voorstel kunnen doen voor een aanpak van de single audit systematiek, een pilot uitvoeren, of kunnen bijdragen aan het ontwikkelen van een best practice.

Het realiseren van een op SISA gelijkend framework kan overigens tot gevolg hebben dat de met name de kleinere externe accountantskantoren niet goed in staat zijn om invulling te geven. Vanuit de ADR is opgemerkt dat dit aspect in verder onderzoek meegewogen moet gaan worden in overleg met de betreffende beroepsorganisaties.

- **Op te leveren producten**
- Een plan van aanpak single audit
- Een verdieping van bestaande initiatieven die zich richten op het verminderen van auditlast'
- Een beschrijving van de raakvlakken van die initiatieven
- Een uitgewerkt auditframework dat de auditlast binnen de overheid daadwerkelijk verminderent
- De resultaten van de uitvoering van een pilot met dit auditframework
- Daadwerkelijke implemenatie van dit framework

11.Communicatie

De uitdaging voor de Taskforce Bestuur en Informatieveiligheid Dienstverlening op communicatievlak is ervoor te zorgen dat bestuur en het topmanagement van de organisaties binnen de verschillende overheidslagen zich openstellen voor het onderwerp informatieveiligheid en de rol van de Taskforce BID daarbinnen. Om dit te bereiken dienen de koepelorganisaties van de vijf overheidslagen, en de gerelateerde partijen die hun kernverantwoordelijkheid hebben op informatieveiligheidsvlak, eenzelfde openheid te hebben en de verantwoordelijkheid van de Taskforce BID, evenals de eigen verantwoordelijkheid op dit vlak te (h)erkennen. Mede ook om een gezonde bodem te creëren voor de samenwerking en de gezamenlijke verantwoordelijkheid ook concreet handvatten te geven.

Kortom, het is belangrijk om de identiteit (herkomst/vertrouwen), de autoriteit (de opdracht), de mentaliteit (de inspirator gericht op 'samen') en de verantwoordelijkheid (de eindproducten) van de Taskforce BID eenduidig en krachtig neer te zetten richting haar doelgroepen. Dit uiteraard gerelateerd aan het onderwerp informatieveiligheid.

Dat betekent dat er een tweetal lagen van communicatie gaat ontstaan:

- *Generieke communicatie*
  Dat wil zeggen, de communicatie door de Taskforce BID zelf richting haar doelgroepen (koepelorganisaties, gerelateerde organisaties op informatieveiligheidsvlak, primaire ambassadeurs, directe collega's en pers)
- *Specifieke communicatie*
  Dat wil zeggen de communicatie door de Taskforce BID in nauwe samenwerking met de koepelorganisatie binnen elke overheidslaag. Deze communicatie is gericht op de specifieke doelgroepen binnen elke overheidslaag en heeft als doel verplichtende zelfregulering per overheidslaag mogelijk te maken.

Om kennis, houding en gedrag van de betrokken doelgroepen optimaal te stimuleren, leert ervaring dat het zinvol is om de hiertoe in te zetten communicatie-aanpak en bijbehorende middelen op drie pijlers te baseren: informeren, involveren en inspireren. Het is hierbij uiteraard belangrijk dat de toon, vorm en uitstraling van de communicatie naar de verschillende doelgroepen aansluit bij de opdracht (autoriteit) van de Taskforce BID. Een eigen logo en huisstijl zijn dan ook randvoorwaardelijk. Naast autoriteit dient de nadruk evenzeer te liggen op actieve verbinding/samenwerking door bijvoorbeeld de zichtbaarheid van de logo's van de koepelorganisaties. Dit vergroot niet alleen de herkenbaarheid, maar ook de acceptatie onder de doelgroepen.

Om de start van de Taskforce BID te markeren, haar positionering eenduidig neer te zetten en haar doelen op een succesvolle manier te delen, is gestart met de eerste communicatielaag; de inzet van generieke communicatie. Deze communicatie wordt, ook op middelenvlak, specifieker verdiept per overheidslaag (de hiervoor genoemde specifieke communicatie). In de separate communicatieplannen ten behoeve van de vijf afzonderlijke overheidslagen (rijksoverheid, zelfstandige bestuursorganen, provincies, waterschappen en gemeenten) worden deze specifieke middelen apart benoemd.

Voor meer informatie zie de bijgevoegde documenten :
- *Communicatieplan Taskforce Bestuur en Informatieveiligheid Dienstverlening*
- *Communicatiekalender Taskforce Bestuur en Informatieveiligheid Dienstverlening*

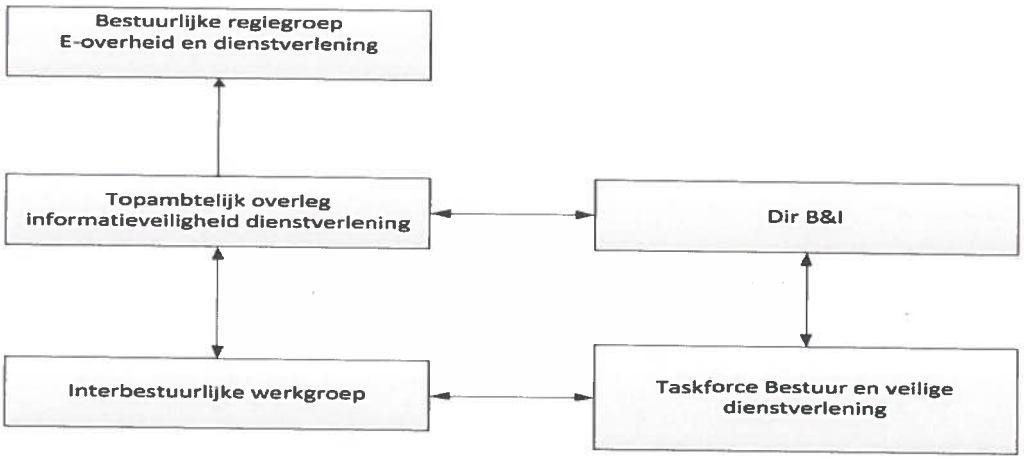
Bijlage 1: Governance

Sturing en organisatie

De voor sturing en organisatie zijn gebaseerd op de volgende uitgangspunten.

- Het huidige stelsel van bevoegdheden en verantwoordelijkheden rond informatieveiligheid is uitgangspunt.
- Elke overheidsorganisatie blijft zelf verantwoordelijk voor realisatie eigen informatieveiligheid
- Coördinatie op bestaande initiatieven is een noodzaak om overheidsbrede informatieveiligheid te verbeteren
- De Taskforce kent een Interbestuurlijke aanpak; collegiaal en in vertrouwen
- De Taskforce wordt klein en wendbaar opgezet zodanig dat hij in een netwerk van organisaties stimulerend werkt
- De Governance van de Taskforce sluit aan de bestaande bestuurlijke regiegroep e overheid en dienstverlening.

Bij de vormgeving aan de governance is huidige stelsel van bevoegdheden en verantwoordelijkheden rond informatieveiligheid uitgangspunt. Interbestuurlijke coördinatie op bestaande initiatieven is een noodzaak om overheidsbrede informatieveiligheid te verbeteren. De Taskforce wordt klein en wendbaar opgezet zodanig dat zij in een netwerk van organisaties stimulerend werkt. Een en ander kan vorm krijgen door als volgt aan te sluiten bij de bestaande BRG E-overheid en dienstverlening



De BRG E-overheid en Dienstverlening is een goed forum voor overleg en coördinatie van informatieveiligheid. Vanuit VenJ is aangegeven dat een dergelijke afstemming gewenst is en V en J kan aan de regiegroep deelnemen. Voor een snelle en krachtige besluitvorming in het netwerk van de geschetste vierhoek is een topambtelijk overleg van de vijf overheidslagen gewenst. De directie B&I van BZK is met name ook opgenomen vanwege de taak inzake stelselverantwoordelijkheid en coördinatie. De programmaraad 'Follow-up DigiNotar' vindt een opvolger in de interbestuurlijke werkgroep Bestuur en 'Informatieveiligheid Dienstverlening'.

DG BK (dir. B en I) stuurt op de voortgang van het geheel. Deze stelselverantwoordelijkheid laat de specifieke verantwoordelijkheid van rijkspartijen op specifieke terreinen onverlet (NCSC, Logius enz.)

Per overheidslaag zullen op de voortgang aanspreekbare partijen aanwezig moeten zijn op de voortgang van de programmering te bespreken. Steeds is daarbij te onderscheiden naar de bestuurlijk eerstverantwoordelijke en de meer uitvoerend verantwoordelijke.

- Rijk: DG OBR en ICCIO, V&J, I&M en EZ
- Gemeenten: VNG en IBD
- Provincies: IPO en Overleg directeuren bedrijfsvoering met ICT strategisch overleg
- Waterschappen: UVW en Waterschapshuis
- ZBO: in overleg met Rijk, de Manifestgroep en CIP

Speciale verantwoordelijkheden zullen voortkomen uit de ketenprogrammering

Ambtelijk Topoverleg

Samenstelling Ambtelijk Topoverleg	
Na(a)m(en)	Rol
Dg BK	Opdrachtgever namens minister BZK
Dg OBR	Domeinvertegenwoordiger
Directeur VNG	Domeinvertegenwoordiger
Directeur Unie van Waterschappen	Domeinvertegenwoordiger
IPO	Domeinvertegenwoordiger
Directie Cyber Security – VenJ	Adviseur
Hoofd Taskforce BID	Adviseur
Manager Taskforce BID	Adviseur

Interbestuurlijk Werkgroep

Samenstelling Interbestuurlijke Werkgroep
BZK/DGBK/B&I - Voorzitter
BZK/DGBK/B&I - Secretaris
BZK/DGBK/B&I - Projectleider Taskforce BID
Hoofd Taskforce BID
Manager Taskforce BID
Plv. manager Taskforce BID
BZK/DGOBR/DIR – vertegenwoordiger domein
Logius – vertegenwoordiger stelsel
UVW/Waterschapshuis – vertegenwoordiger domein
KING – vertegenwoordiger stelsel
NCSC – vertegenwoordiger stelsel
VNG – vertegenwoordiger domein
IPO – vertegenwoordiger domein
UWV/CIP – vertegenwoordiger stelsel
UVW – vertegenwoordiger domein
EZ - vertegenwoordiger stelsel
V&J – vertegenwoordiger stelsel
I&M – vertegenwoordiger stelsel

Leiding en organisatie/formatie Taskforce BID

In de formatie is een aantal disciplines verankerd dat benodigd is voor de taak van de Taskforce. Het streven is de formatie mede in te vullen met medewerkers vanuit de andere overheden.

Samenstelling Taskforce BID	
Naam	Rol
[redacted]	Hoofd
[redacted]	Manager
[redacted]	Plv. manager / Account Rijk
[redacted]	Programmasecretaris
[redacted]	Account Gemeenten Portfolio Leren & Verankeren
[redacted]	Portfolio monitoring
[redacted]	Account Provincies Account Waterschappen
[redacted]	Communicatie en woordvoering
[redacted]	Communicatie
[redacted]	Account Veiligheidsregio's
[redacted]	Portfolio Audit & monitoring
[redacted]	Account ZBO Portfolio Informatiebeveiliging
[redacted]	Bestuurlijk Beleidsadviseur
[redacted]	Juridisch Beleidsadviseur
[redacted]	Portfolio Leren & Verankeren
[redacted]	Administratieve ondersteuning en facilitering

De precieze inhoudelijke invulling van de rollen en verdeling van de inhoudelijke werkzaamheden kan in de loop van de tijd wijzigen om tot een doelmatige aanpak te kunnen komen.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Stichting ICTU
De heer [redacted]
Postbus 84011
2508 AA DEN HAAG

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
http://www.rijksoverheid.nl

Kenmerk
2015-0000590990

Uw kenmerk

Bijlage(n)

Datum 15 oktober 2015
Betreft bijdragevaststelling en terugvordering

Geachte [redacted]

Op 28 september jl. heb ik de verantwoording voor de door u ontvangen bijdrage van 1 november 2012 t/m 30 maart 2015 ontvangen. Dank daarvoor.

Het inhoudelijke verslag is door mij in goede orde ontvangen. Met het resultaat kan ik instemmen.

Uit de eindafrekening blijkt dat u € 8.264.312,00 voor deze activiteiten hebt uitgegeven. Dat is minder dan de toegekende bijdrage van € 8.583.615,00 waarvan € 8.583.615,00 als voorschot is uitbetaald.

Onder verwijzing naar de bijdrageverlening van <datum, kenmerk>, stel ik het definitieve bijdrage bedrag vast op € 8.264.312.

Dit betekent dat u het bedrag van onderbesteding, te weten (€ 319.303 minus de al terug ontvangen € 250.000) € 69.303,00 dient terug te storten. Hiervoor ontvangt u binnenkort een factuur van ons.

Hoogachtend,
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

[redacted]

Directeur Burgerschap en Informatiebeleid

ICTU

AFSCHRIFT

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Burgerschap en Informatiebeleid
T.a.v. [redacted]
Postbus 20011
2500 EA Den Haag

Betreft
Decharge en eindafrekening project Taskforce BID

Ons kenmerk
C746-05

Uw kenmerk

Contactpersoon
[redacted]

Telefoon
[redacted]

Datum 28 SEP. 2015

Geachte [redacted]

Namens het bestuur van de Stichting ICTU verzoek ik u decharge te verlenen voor het project Taskforce BID, inhoudende dat het project is afgerond en dat ICTU regarderende het project een adequaat financieel en administratief (archief)beheer heeft gevoerd, al zijn verplichtingen jegens opdrachtgever correct is nagekomen en dat daarmee geen verplichtingen meer openstaan.

Het project was gedurende de periode 1 november 2012 tot en met 30 maart 2015 ondergebracht bij de Stichting ICTU, die daartoe op 5 november 2012 een projectovereenkomst 'Faciliteren uitvoering Taskforce BID is aangegaan met de Staat der Nederlanden, vertegenwoordigd door de Minister van Binnenlandse Zaken en Koninkrijksrelaties, en welke namens deze door de (destijds) directeur Burgerschap en Informatiebeleid, mevrouw B. Steenbergen is ondertekend.

De werkzaamheden zijn uitgevoerd met inachtneming van de genoemde projectovereenkomst. Voor de verantwoording verwijs ik u naar de bijlagen, alsmede naar de door ICTU gedurende de looptijd van het project opgeleverde rapportages.

Het project heeft een batig eindresultaat van € 319.303 (zie bijlage 1), waarvan een bedrag van €250.000 reeds op 9 juni 2015 is teruggestort op rekeningnummer van opdrachtgever. In het eerste kwartaal van 2015, de laatste drie maanden van de Taskforce BID, is gestuurd op een batig eindresultaat. Met het vrijvallen van een aantal stelposten, waaronder communicatie en het leer- en verankeraanbod, is dit gunstiger uitgevallen. Het vrijvallen van het Leer- en Verankeraanbod heeft een directe relatie met opstarten van het *onderhoudsprogramma* rondom het Leer- en Verankeraanbod. Eind 2014 is vanuit de Taskforce BID voorgesteld om het batig eindresultaat ten gunste te laten zijn van dit programma, om zo het rendement van de activiteiten

van de Taskforce BID en de koepels verder te optimaliseren. Het advies is om dit voorstel over te nemen. In het OGON tussen BZK en ICTU is uiteindelijk afgesproken dat de onderuitputting retour komt naar BZK

De in bijlage 1 genoemde kosten, zijn inclusief nog niet ontvangen facturen cq. transitorische posten. Indien deze bij afwikkeling van het eindresultaat nog niet zijn ontvangen en/of wanneer de transitorische posten hoger dan wel lager zijn dan de daadwerkelijk ontvangen facturen c.q. kosten, dan zal dit worden verrekend met de opdrachtgever.

Indien na afwikkeling van het eindresultaat nog onverwachte facturen c.q. kosten worden ontvangen, bestemd voor het project Taskforce BID, dan zullen deze door ICTU worden doorgezonden aan opdrachtgever ter betaling.

Ik verzoek u om de Stichting ICTU de gevraagde decharge te verlenen door één exemplaar van dit in tweevoud toegestuurde dechargeverzoek te ondertekenen en door middel van bijgevoegde antwoordenvelop te retourneren aan het projectbureau van Stichting ICTU.

Met vriendelijke groet,

Namens het bestuur van de Stichting ICTU,

directeur

Voor akkoord: 15-10-2015

Namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties, voor deze,

directeur burgerschap en Informatiebeleid

BIJLAGEN
Bijlage 1: Financiële verantwoording
Bijlage 2: Vaste activa
Bijlage 3: Overdracht projectdocumentatie
Bijlage 4: Eindrapportage

Bijlage 1 Financiële verantwoording

Initieel was voor de Taskforce BID tweemaal een bedrag van €6,4M begroot, in totaal €12,8M. In overleg is medio 2013 uiteindelijk besloten om dit terug te brengen tot €8,4M i.v.m. de beperkte beschikbare middelen vanuit BZK enerzijds, en de beperkte afname van het aanbod in het eerste jaar van de Taskforce BID anderszijds i.v.m. de doorlooptijd van het mobilisatietraject binnen de verschillende overheidslagen. Op verzoek van BZK is in het 4e kwartaal van 2014 een bezuiniging doorgevoerd van €125.000 t.b.v. het financieren van het visitatietraject bij gemeenten, wat toen aangevuld is met een even zo groot bedrag vanuit BZK, met als doel dat de VNG dit bedrag van €250.000 in 2014 zou bestemmen. Dit bedrag van €250.000 is reeds teruggestort op 9 juni 2015, daar na overleg besloten is om de financiering hiervoor via BZK te laten verlopen. Hiermee blijft een restbedrag over van €69.303.

De kosten en baten over de verschillende boekjaren zijn als volgt:

Boekjaar	Restant vorig jaar	Baten	Kosten	Restant
2012	-	€ 6.400.000	€ 17.230	€ 6.382.770
2013	€ 6.382.770	€ 1.100.000	€ 3.004.921	€ 4.477.849
2014	€ 4.477.849	€ 1.083.615	€ 4.799.398	€ 762.066
2015	€ 762.066	€ 0	€ 442.763	€ 319.303
Totaal		**€8.583.615**	**€8.264.312**	

Voor een uitsplitsing van de kosten naar de verschillende begrotingsposten, zie volgende bladzijde.

ICTU

Kosten 2012	Mensen	Middelen	Totaal
Kwartiermakersfase	€ 17.230	€ 0	€ 17.230

Kosten 2013	Mensen	Middelen	Totaal
Adequate gerichtheid op informatieveiligheid	€ 377.828	€ 749.933	€ 1.127.761
Adequate verankering informatieveiligheid in organisatie en overheidslaag	€ 135.039	€ 227.153	€ 362.192
Adequate gerichtheid op informatieveiligheid in ketens	€ 126.445	€ 52.234	€ 178.679
Adequate verankering van informatieveiligheid in ketens	€ 31.467	€ 46.314	€ 77.781
Externe sturing Taskforce • Ontwikkelde adequate monitorings-systematiek • Uitgevoerd gewenst onderzoek • uitgevoerde communicatie mbt verankering en gerichtheid	€ 36.821 € 42.457 € 182.038	€ 155.612 € 223.598 € 322.150	€ 192.433 € 266.055 € 504.188
Interne sturing Taskforce	€ 266.364	€ 29.468	€ 295.832
Totaal	€ 1.198.459	€ 1.806.462	€ 3.004.921

Kosten 2014	Mensen	Middelen	Totaal
Gerichtheid	€ 625.506	€ 819.208	€ 1.444.714
Verankering	€ 227.736	€ 732.382	€ 960.118
Stelsel	€ 257.221	€ 523.631	€ 780.852
Dialoog	€ 122.765	€ 360.862	€ 483.627
Communicatie	€ 147.807	€ 514.651	€ 662.458
Bedrijfsvoering	€ 434.125	€ 33.504	€ 467.629
Totaal	€ 1.815.159	€ 2.984.239	€ 4.799.398

N.B. In overleg met de opdrachtgever is de structuur van de posten aangepast t.o.v. 2013.

Kosten 2015	Mensen	Middelen	Totaal
Gerichtheid	€ 50.159	€ 29.951	€ 80.110
Verankering	€ 54.707	€ 67.615	€ 122.322
Stelsel	€ 48.469	€ 14.987	€ 63.456
Dialoog	€ 29.716	€ 0	€ 29.716
Communicatie	€ 30.883	€ 18.462	€ 49.345
Bedrijfsvoering	€ 82.236	€ 15.578	€ 97.814
Totaal	€ 296.170	€ 146.593	€ 442.763

Bijlage 2 Vaste Activa

Voor de uitvoering van het project zijn de volgende vaste activa aangeschaft. Deze activa zijn overgedragen aan het *onderhoudsprogramma*.

Aantal	Omschrijving	Typenummer
2	Tablet	merk ASUS type K00F (ME102A)

Bijlage 3 Overdracht projectdocumentatie

De volledige projectdocumentatie is reeds in digitale vorm overgedragen aan de opdrachtgever, waarbij een onderscheid is gemaakt tussen concept- en definitieve stukken. Niet relevante stukken, of financieel[1]-/privacy-gevoelige stukken, zijn verwijderd. Bovendien zijn de deliverables rondom het Leer- en Verankeraanbod op de sub-site pleio.informatieveiligheid.nl geplaatst en is de volledige projectdocumentatie overgedragen aan het onderhoudsprogramma. In excelvorm is een overzicht aangeleverd van alle uitgevoerde (communicatie)activiteiten alsook de communicatiekalender. Daarnaast is in hardcopy een overzicht geleverd van alle artikelen en overig gepubliceerd materiaal.

[1] o.a. aanbestedingstrajecten

Bijlage 4 Eindrapportage

De opdracht van de minister van BZK aan de Taskforce BID was:

1. De bewustwording te versterken van bestuur en ambtelijke top als het gaat om de eisen aan informatieveiligheid, met name ook vanuit maatschappelijke en politieke risico's.
2. Een leerstrategie uit te voeren voor een actieve gerichtheid van bestuur en ambtelijke top op adequate aanpak informatieveiligheid dienstverlening.
3. De lange termijn verankering van informatieveiligheid en gerichtheid daarop in de reguliere processen en informatieketens te versterken, waarbij gerichtheid op weerbaarheid en herstel deel zijn van die verankering. Een verplichtende vorm van zelfregulering per domein is het beoogde einddoel van die verankering.
4. De overheidsbrede coördinatie rond het stelsel van informatieveiligheid te bevorderen en te adviseren over dit stelsel.
5. Voor zover nodig aanvullend onderzoek te doen verrichten. De uitwerking van bovengenoemde opdracht is en blijft de verantwoordelijkheid van de overheidslagen en overheidsorganisaties zelf.

De Taskforce BID heeft de afgelopen twee jaar gefunctioneerd als aanjager, vliegwiel, facilitator en verbinder. De focus lag op organisaties uit de volgende overheidslagen: Rijk, ZBO's, gemeenten, provincies en waterschappen. In alle gevallen heeft de Taskforce BID zich ten dienste gesteld van BZK en de koepels; zij staan uiteindelijk voor de implementatie en het beheer.

Gekozen is voor een aanpak gebaseerd op organisatieleren, met als inzet om te komen tot verplichtende zelfregulering op informatieveiligheid. Dit is binnen de looptijd van de Taskforce BID voor alle overheidslagen gelukt.

De Taskforce BID heeft samen met de overheidslagen een gericht opleidingsaanbod en concrete verankeringsinstrumenten ontwikkeld en aangeboden ter ondersteuning van de opdracht. Daarbij is ingezet op hergebruik van bestaand en beproefd aanbod en waar nodig aangevuld met nieuw aanbod.

Met de inzet van dit materiaal is een zichtbare en meetbare verandering gerealiseerd bij bestuur en topmanagement op het vlak van informatieveiligheidsbewustzijn en risicobewust handelen. Dit vertaalt zich onder andere in de in control verklaringen op informatieveiligheid, die opgenomen gaan worden in de reguliere PDCA-cyclus. Om te komen tot een goede beeld, is ook ingezet op het ontwikkelingen van een weerbaarheidsbeeld informatieveiligheid overheden. Hiervoor is de basis gelegd, welke overgedragen is aan de BZK en de koepels.

De zelfregulering is niet vrijblijvend en vraagt om een samenhangend stelsel van normen, coördinatie van beleid en afspraken over de naleving en toetsing binnen de interbestuurlijk afgesproken kaders. Hiervoor is in interbestuurlijk verband gewerkt aan de doorontwikkeling van deze kaders voor informatieveiligheid. De (tussen)resultaten hiervan zijn overgedragen aan BZK.

Als laatste is ingezet op het realiseren van een pro-actieve coalitie op informatieveiligheid, waarlangs op bestuurlijk niveau de dialoog gevoerd wordt over dit thema. Het biedt de ruimte om onderwerpen op informatieveiligheid te adresseren die voortkomen uit de vele veranderingen waar bestuurders en topmanagers mee geconfronteerd worden. De basis hiervoor is gelegd en ook overgedragen aan BZK en de koepels

Meer informatie is te vinden in de eindrapportage van de Taskforce BID, welke ook te vinden is op de website www.taskforcebid.nl.

Onze producten

	Weten/herkennen		Erkennen		Willen	Kunnen		Doen	
Product	Zelftest	Masterclass	Confron-tatie workshop	Dialoog-sessie	Risico-bewustzijn-sessie	Proces Workshop	Veranker sessie	Informatie-veiligheids-oefening	App
Doelgroep	Bestuurder	Bestuurder	Manager	Manager IB-er	Bestuurder Manager	Manager IB-er	Manager IB-er	Crisisteam	Hele organisatie
Thema	Kennis	Kennis	Commit-ment	Commit-ment	Risicobesef	Risico-manage-ment	Verant-woordelijk-heden	Weerbaar-heid	Kennis

Weten/herkennen: Zelftest

Test uw kennis
Via een online zelftest krijgt u als bestuurder een beeld van uw kennis en bewustzijn op het gebied van informatieveiligheid. U ontdekt de verschillende aspecten van informatieveiligheid en vooral ook hoe u daarop kunt sturen.

Leerdoelen
- U krijgt inzicht in de breedte en het belang van het onderwerp informatieveiligheid
- U ziet dat informatieveiligheid een integraal deel is van risicomanagement
- U ervaart dat u zelf een actieve rol in de sturing van het onderwerp heeft

Voor wie
Bestuurders en topmanagers

Werkvorm
online test met 10 vragen

Weten/herkennen: Masterclass

Masterclass Informatieveiligheid
Wilt u leren van anderen? Dat kan! In onze masterclasses, exclusief voor bestuurders, neemt u kennis van de visie van een collega-bestuurder, een inhoudelijke visie van een expert en/of een best practice.

Leerdoelen
- U krijgt inzicht in de breedte en het belang van het onderwerp informatieveiligheid
- U ziet dat informatieveiligheid een integraal deel is van risicomanagement
- U krijgt inzicht in innovatie op gebied van informatieveiligheid

Voor wie
Bestuurders

Werkvorm
lezing en dialoog

Erkennen: Confrontatieworkshop

Verken uw rol
In een confrontatieworkshop ontdekt u via confrontatie met een scenario uit de praktijk het belang van een actieve rol van het management bij een incident én het belang van het stellen van de juiste stuurvragen.

Leerdoelen
- U ervaart dat u een eigen actieve rol in de sturing van het onderwerp heeft
- U leert welke stuurvragen u kunt stellen voor een goede informatiepositie
- U verkent welke bestuurlijke besluiten en opdrachten nodig zijn bij crisisbeheersing

Voor wie
Topmanagers

Werkvorm
scenario en dialoog

Erkennen: Dialoogsessie

Spreekt u dezelfde taal
Verstaat u de taal van uw informatiebeveiliger? Kent uw informatiebeveiliger uw positie en belangen op gebied van informatieveiligheid? U leert in onze dialoogsessie elkaar beter begrijpen en meer dezelfde taal spreken. Zodat u informatieveiligheid samen goed kunt vormgeven.

Leerdoelen
- U ontdekt hoe u uw informatiepositie kunt versterken door het stellen van de juiste stuurvragen aan uw informatiebeveiliger
- Informatiebeveiligers leren om uw belangen mee te nemen in hun advies over informatieveiligheid

Voor wie
Bestuurders/topmanagers en informatiebeveiligers

Werkvorm
dialoog

TASKFORCE

Bestuur & Informatieveiligheid Dienstverlening

Willen: Risicobewustzijnsessie

Risicobewust sturen

Tijdens onze risicobewustzijn sessie krijgt u inzicht in risicoafwegingen. U leert bewust risico's te accepteren of te vermijden op basis van uw bestuurlijke risicogebieden. U ontdekt met welke criteria u passende maatregelen kunt kiezen.

Leerdoelen

- U onderkent welke bestuurlijke risicogebieden u belangrijk vindt
- U leert bewust een risicoafweging te maken: welke risico's accepteert u?
- U verkent hoe tijd, capaciteit en geld invloed hebben bij de keuze voor mitigerende maatregelen

Voor wie

Bestuurders en topmanagers

Werkvorm

scorekaart en dialoog

Kunnen: Verankersessie

Grip op informatieveiligheid

U leert hoe u informatieveiligheid kunt inrichten binnen uw organisatie tijdens onze verankersessie. De ISMS-principes helpen u grip te krijgen op informatieveiligheid via organisatie, beleid, uitvoering en lerend vermogen.

Leerdoelen

- U onderkent het belang van continue aandacht voor informatieveiligheid binnen uw organisatie
- U leert de stappen (ISMS) waarlangs u een informatieveiligheidsproces in kunt richten
- U verkent de rollen, verantwoordelijkheden en sturingsmiddelen binnen dat proces

Voor wie

Topmanagers, lijnmanagers en informatiebeveiligers

Werkvorm

fictieve casus, brainstormen

Kunnen: Procesworkshop

Bescherm uw proces

U leert hoe een belangrijk proces bedreigd kan worden en hoe u dit proces kunt beschermen. U ontdekt in deze procesworkshop hoe u kunt sturen op het aanscherpen van processen, als het gaat om informatieveiligheid. Ook het inbedden van informatieveiligheid in deze processen komt aan de orde.

Leerdoelen

- U onderkent het belang van bescherming van gevoelige en vertrouwelijke gegevens binnen processen
- U onderkent het belang van informatiebeveiliging voor het beschermen van processen
- U leert sturen op het toepassen van informatiebeveiligingsmaatregelen

Voor wie

Topmanagers, procesmanagers en informatiebeveiligers

Werkvorm

red & blue teaming

Doen: Informatieveiligheidsoefening

Informatieveiligheids-oefening

Elke organisatie doet een brandoefening. Met de vele calamiteiten en incidenten binnen de overheid is het opportuun om ook een informatieveiligheidsoefening te doen. Hoe weerbaar is uw organisatie eigenlijk? Toets het met onze informatieveiligheids-oefening.

Leerdoelen

- U checkt hoe weerbaar uw organisatie is
- U leert welke rol u heeft bij het beheersen van een incident
- U leert de stappen om een incident te beheersen
- U ervaart op welke punten u uw organisatie kunt verbeteren op gebied van beheersen van een incident.

Voor wie

Bestuurders en crisisteam

Werkvorm

table top oefening op basis van scenario

Meer informatie

Heeft u vragen over het leeraanbod zelf? [redacted] verantwoordelijke voor het leeraanbod van de Taskforce BID, beantwoordt deze graag via [redacted]@taskforcebid.nl.

Uiteraard kunt u ook een kijkje nemen op www.taskforcebid.nl/producten of www.informatieveiligheid.pleio.nl.

INFORMATIEVEILIGHEID TASKFORCE DOOR SAMENWERKING

TASKFORCE

Bestuur & Informatieveiligheid Dienstverlening

Leren binnen de overheid op informatieveiligheid

Opleidingsplan Taskforce BID

Auteur: [redacted]

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Inhoudsopgave

1 Zichtbare verandering in bewustzijn en handelen

Informatieveiligheid is binnen de overheid verscherpt op het netvlies gekomen na de DigiNotar-crisis, Lektober en een diversiteit aan DDoS-aanvallen. Deze impactvolle gebeurtenissen hebben aangetoond dat overheden uitermate kwetsbaar zijn. Niet alleen als het gaat om hun (digitale) dienstverlening, ook als het gaat om het veilig en beveiligd uitvoeren van deze dienstverlening.

Uit het rapport van de Onderzoeksraad Voor Veiligheid van juni 2012, blijkt eveneens dat overheden nog voor een aantal uitdagingen staan als het gaat om informatieveiligheid. Zo is het risicobewustzijn aangaande informatieveiligheid vooral aanwezig bij de ICT-afdeling. De bestuurlijke aandacht voor het thema informatieveiligheid is met name scherp in geval van impactvolle incidenten. Het mag duidelijk zijn dat continue bestuurlijke aandacht voor én sturing op dit onderwerp in onze digitale wereld noodzakelijk is geworden. Scherp oog hebben voor de veiligheidsrisico's, en de scenario's die ingezet worden in geval dergelijke risico's zich voordoen, is onontbeerlijk. Zeker op bestuursniveau.

Het rapport van de Onderzoeksraad van de Veiligheid laat zien dat bij bestuur en topmanagement binnen de overheid gebrek is aan bewustzijn, kennis en vaardigheden op:

- het verbinden van digitale veiligheid met primaire processen;
- een integrale aanpak voor leren van incidenten;
- digitale veiligheidsrisico's.

De Taskforce BID wil een zichtbare en meetbare verandering realiseren bij bestuur en topmanagement binnen de overheid op gebied van informatieveiligheidsbewustzijn en risicobewust handelen. De Taskforce BID streeft dan ook naar de volgende verandering:

1. versterkt bewustzijn van bestuur en managementtop van de eisen aan informatie-veiligheid, met name ook vanuit maatschappelijke en politieke risico's;
2. actieve gerichtheid van bestuur en ambtelijke top op adequate aanpak informatieveiligheid;
3. een lange termijn verankering van informatieveiligheid en gerichtheid daarop in de reguliere processen en informatieketens, waarbij gerichtheid op weerbaarheid en herstel deel zijn van die verankering. Een verplichtende vorm van zelfregulering per domein is het beoogde einddoel van die verankering.

Veranderimpuls bij bestuur

De vraag bij de opdracht van de Taskforce BID is wat de veranderimpuls is voor bestuur en topmanagement op gebied van informatieveiligheid. De bekende verandertriggers zijn:

- Dreigende imagoschade
- Onvrede over dienstverlening bij burgers en bedrijven
- Dreigend verlies van budgetten

1.1 Randvoorwaarden voor verandering

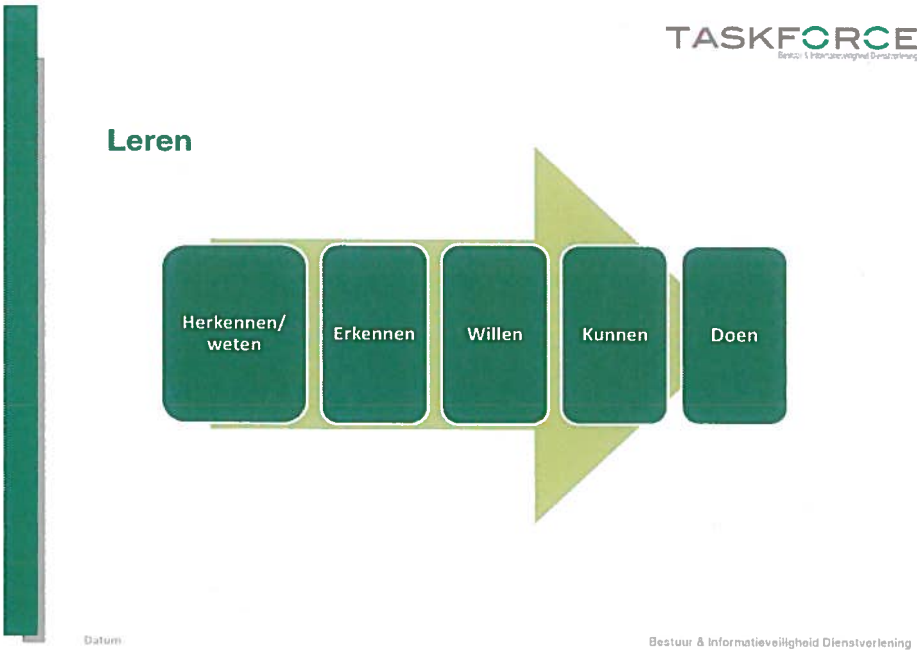
Betekenisgeving binnen organisatie
- besef van en inzicht in breedte van informatieveiligheid
- besef van en inzicht in belangen bij informatieveiligheid
- besef van en inzicht in risico's en sterktes
- stimuleren en waarderen van gewenst gedrag

Inbedding in organisatie
- nadrukkelijke (voorbeeld)rol van bestuur en topmanagement
- vanuit eigen organisatiedoelen en binnen organisatiestructuren veranderen
- samenwerken binnen organisatie
- wederzijds willen afkijken, ook van andere terreinen

De Taskforce BID geeft de verandering vorm via twee nauw verbonden sporen: leren en verankeren.

1.2 Leren

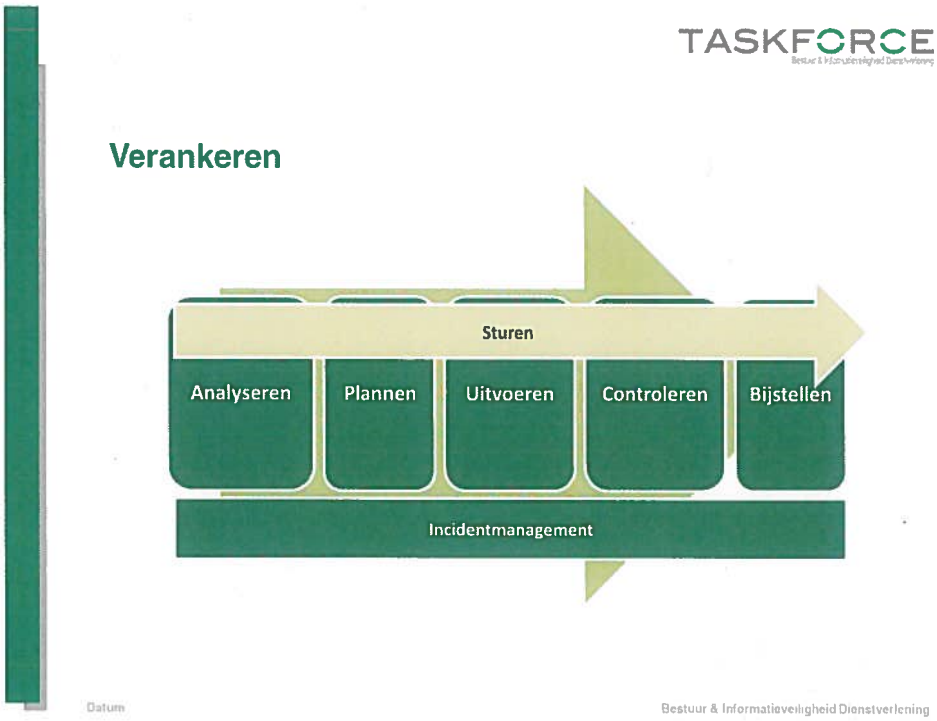
Het spoor 'leren' richt zich op verandering in kennis, houding en vaardigheden. Dit spoor werkt toe naar betekenisgeving en verandering in individueel gedrag via vijf bewustzijnstadia: weten, erkennen, willen, kunnen, doen. Het spoor legt een basis voor verankering.



1.3 Verankeren

Het spoor 'verankeren' richt zich op verandering in processen en structuren binnen de informatieveiligheidscyclus. Dit spoor werkt toe naar continue sturing op verandering in

organisatiegedrag binnen de stappen van de informatieveiligheidscyclus: analyseren, plannen, uitvoeren, controleren en bijstellen. Het zorgt voor inbedding in de organisatie. Dit spoor bouwt voort op een basis bewustzijn gecreëerd in het spoor 'leren'.



1.4 Uitgangspunten opleidingsplan

Dit plan geeft de doelen, strategie en middelen van de Taskforce BID weer voor het spoor 'leren' en de samenhang met het spoor 'verankeren'. De uitgangspunten voor dit opleidingsplan zijn:

1) Maken van een leerstrategie die bijdraagt aan Verplichtende zelfregulering;
2) Bepalen van leerdoelen voor bestuur, topmanagement en CISO/informatiebeveiliger;
3) Bedenken van leerinstrumenten die bewustzijn en handelingsgerichtheid vergroten.

2 Leerdoelen

Welke leerdoelen voor kennis, houding en vaardigheden zien we bij bestuurders en topmanagers? Deze leerdoelen leggen een basis voor een verandering in gedrag, structuren en processen.

2.1 Bestuur

Kennis:

- Bestuurders weten wat informatieveiligheid in de breedte inhoudt
- Bestuurders weten wat de top 10 risico's is en welke impact deze calamiteiten en incidenten hebben op bedrijfsvoering en dienstverlening
- Bestuurders kennen het belang van een werkende cyclus op gebied van informatieveiligheid

Houding:

- Bestuurders erkennen het belang van een werkende veiligheidscyclus
- Bestuurders erkennen de noodzaak tot sturen op informatieveiligheid
- Bestuurders erkennen belang van zicht op problemen/risico's binnen eigen organisatie (en binnen ketens)
- Bestuurders voelen zich opdrachtgever voor risicomanagement, ontwikkeling en naleving van beleid op gebied van informatieveiligheid en controlemechanismen
- Bestuurders zien het belang van controlemechanismen (self-assessment, peer review, audit).

Vaardigheden:

- Bestuurders kennen problemen/risico's binnen eigen organisatie (en binnen ketens) (doelstelling – risico's – beleid op informatieveiligheid)
- Bestuurders kunnen stuurvragen stellen aan alle verantwoordelijken op gebied van cylcus van informatieveiligheid en tijdens incidenten en calamiteiten (uit top 10)
- Bestuurders kennen beleid binnen eigen organisatie op gebied van informatieveiligheid en kunnen dit uitdragen
- Bestuurders en topmanagers kunnen integraal sturen op lerend vermogen van de hele organisatie (na incidenten en calamiteiten)

Basis voor verandering in gedrag en structuren:

- Bestuurders geven opdracht voor risicoanalyse na invoering van nieuw systeem, verandering van een proces, een incident of crisis
- Bestuurders geven opdracht voor risicomanagement.
- Bestuurders stellen beleid op gebied van informatieveiligheid of bijstelling daarvan vast via ondertekening van dit beleid
- Bestuurders handelen volgens beleid en tonen hiermee voorbeeldgedrag
- Bestuurders dragen het belang van naleving van het beleid op gebied van informatieveiligheid actief uit
- Bestuurders geven opdracht tot incidentmanagement en responsbeleid op gebied van informatieveiligheid
- Bestuurders geven opdracht tot periodieke inzet van controlemechanismen (self-assessment, peer review, audit).
- Bestuurders vragen inzicht in voorgekomen calamiteiten en incidenten.
- Bestuurders geven opdracht voor het meenemen van competenties op gebied van informatieveiligheid in HR-beleid

2.2 Topmanagement

Bij de meeste overheidsorganisaties bestaat het topmanagement met een rol op gebied van informatieveiligheid uit: secretaris, directeur/afdelingsmanager en CISO.

Secretaris (beleid en uitvoering):

Kennis:

- Secretarissen weten wat informatieveiligheid in de breedte inhoud
- Secretarissen kennen de verantwoordelijken voor informatieveiligheid in de uitvoering

Houding:

- Secretarissen erkennen belang van zicht op problemen/risico's binnen eigen organisatie
- Secretarissen voelen zich opdrachtgever voor uitvoering van het beleid, toepassing van de norm en informatieveiligheidsoefeningen

Vaardigheden:

- Secretarissen kunnen stuurvragen stellen aan alle verantwoordelijken op gebied van zelfregulering van informatieveiligheid en tijdens incidenten en calamiteiten
- Secretarissen kunnen sturen op het vormgeven van processen op gebied van informatieveiligheid (beleid, norm, implementatie, uitvoering)

Basis voor verandering in gedrag en structuren:

- Secretarissen geven opdracht voor bijstellen van beleid op gebied van informatieveiligheid
- Secretarissen dragen het belang van naleving van het beleid op gebied van informatieveiligheid actief uit
- Secretarissen handelen volgens beleid en tonen hiermee voorbeeldgedrag
- Secretarissen geven opdracht voor het vormgeven en optimaliseren van processen op gebied van informatieveiligheid
- Secretarissen geven opdracht voor het ontwikkelen en bijstellen van een continuïteitsplan voor top 10 risico's.
- Secretarissen geven opdracht voor periodieke oefeningen ter beheersing van calamiteiten en incidenten op gebied van informatieveiligheid
- Secretarissen bespreken periodiek voorgekomen calamiteiten en incidenten met bestuur en CISO/informatiebeveiliger

Raad (toezicht op optimale informatieveiligheid, financiële kaders):

Kennis:

- Raadsleden weten welke eisen te stellen aan optimale informatieveiligheid op gebied van resources

Houding:

- Raadsleden erkennen problemen/risico's binnen eigen organisatie (en binnen ketens)

Vaardigheden:

- Raadsleden kunnen sturen op optimale resources op informatieveiligheid binnen de bedrijfsvoering

Basis voor verandering in gedrag en structuren:

- Raadsleden bespreken risicoanalyse en beleid op gebied van informatieveiligheid in raadsvergadering
- Raadsleden checken of personeel periodiek getraind en opgeleid is op gebied van informatieveiligheid

Directeur/afdelingsmanager (uitvoeringsprocessen, kennis en competenties):

Kennis:

- Directeuren/afdelingsmanagers kennen de verantwoordelijken voor informatieveiligheid in de uitvoering

Houding:

- Directeuren/afdelingsmanagers voelen zich opdrachtgever voor training en opleiding op gebied van informatieveiligheid

Vaardigheden:

- Directeuren/afdelingsmanagers kunnen sturen op het goed verlopen van processen op gebied van informatieveiligheid
- Directeuren/afdelingsmanagers kunnen sturen op aanwezigheid van voldoende kennis en competenties op gebied van informatieveiligheid binnen teams

Basis voor verandering in gedrag en structuren:

- Directeuren/afdelingsmanagers geven opdracht tot periodieke training en opleiding op gebied van informatieveiligheid binnen cluster/afdeling
- Directeuren/afdelingsmanagers geven opdracht tot steekproeven op het goed verlopen van processen op gebied van informatieveiligheid

2.3 CISO

Kennis:

- CISO weet wanneer bij welke instanties incidenten te melden en wanneer op te schalen
- CISO weet welke ontwikkelingen en innovatie er zijn op gebied van informatieveiligheid

Houding:

- CISO/informatiebeveiliger voelt zich verantwoordelijk voor het delen van de inhoud van het beleid op gebied van informatieveiligheid binnen de hele organisatie

Vaardigheden:

- CISO kan gesprek met bestuur en topmanagement voeren over risico's en impact daarvan
- CISO kan bestuur en topmanagement in hun eigen taal het beleid op gebied van informatieveiligheid uitleggen

Basis voor verandering in gedrag en structuren:

- CISO/informatiebeveiliger doet aanbevelingen over prioritering van maatregelen aan bestuur en topmanagement op basis van risicoanalyses
- CISO/informatiebeveiliger bespreekt periodiek de (verbetering van de) naleving van het beleid met bestuur en topmanagement
- CISO/informatiebeveiliger bespreekt periodiek alle voorgekomen calamiteiten en incidenten met bestuur en secretaris

- CISO/informatiebeveiliger maakt actieplannen voor bijstelling en kennisdeling na jaarlijkse controle en audits
- CISO/informatiebeveiligers meldt incidenten bij de juiste instanties
- CISO maakt en deelt protocol voor incidentmelding en opschaling.

3 Leerstrategie

Deze leerstrategie bevat de visie op welke wijze en met welke middelen de Taskforce BID de leerdoelen wil bereiken. De Taskforce BID werkt aan het behalen van de leerdoelen via het bewerkstelligen van organisatieleren via een brede mix aan leer- en verankerinstrumenten.

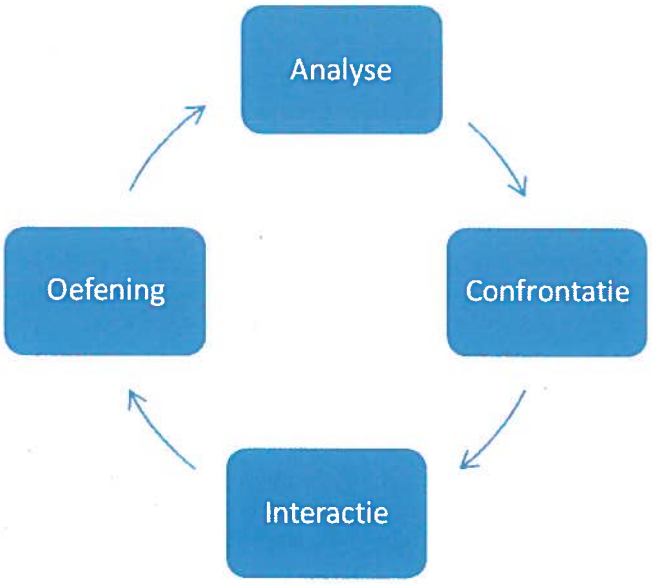
3.1 Wat is organisatieleren?

Organisatieleren richt zich op het vergroten van een gezamenlijke organisatorische prestatie. In het geval van de Taskforce BID is dit het vergroten van het niveau van informatieveiligheid binnen een overheidslaag en uiteindelijk de gehele overheid. Organisatieleren vindt plaats wanneer nieuwe kennis getransformeerd wordt in nieuwe routines van het individu naar de organisatie of omgeving en andersom. Het helpt mensen in een organisatie verandering als een constante factor te omarmen. Organisatieleren verbindt leren en verankeren.

Proces organisatieleren

Organisaties leren door de ervaringen en acties van individuen en het effect daarvan op anderen. Organisatieleren begint dan ook bij voortdurend individueel leren en dialoog. Verankering volgt via gezamenlijke reflectie, gezamenlijke oefening en toepassing. Bij het traject van de Taskforce BID vindt reflectie, oefening en toepassing plaats binnen een concept voor een informatieveiligheidscyclus, verplichtende zelfregulering.

Het veranderproces loopt van nadruk op persoonlijke bewustwording en het verkrijgen van inzicht en kennis, naar verankering binnen organisatie, (bestuurlijke) omgeving en overheidslaag. Via het principe van action learning (integratie van werk en leren) kan doorlopend geleerd en verbeterd worden.



3.2 Hoofdcompetenties organisatieleren

Organisatieleren vraagt om een aantal competenties op bestuurlijk en topmanagement niveau: goed opdrachtgeverschap, gedeelde visie, integraal leren, mentale modellen en systeemdenken.

Goed opdrachtgeverschap
Het hebben van de juiste (zelf)kennis, ontwikkelde vaardigheden gecombineerd met relationele vaardigheden om veranderprocessen effectief te kunnen sturen.

Gedeelde visie
De sleutelvraag bij gedeelde visie is: wat willen we met elkaar creëren? Het is van belang dat vanuit de sturing al vroeg het gesprek met de organisatie wordt gevoerd welke visie omarmd wordt en welk doel bereikt moet worden. Hiermee kan weerstand in de organisatie verminderd worden.

Integraal leren
Om goed te kunnen functioneren heeft een organisatie en daarbinnen een team het delen van inzichten, ervaringen en kennis nodig. Tezamen met vaardigheden als reflectie, discussie en onderzoek kan een organisatie de gedeelde visie tot realiteit brengen.

Mentale modellen
Overtuigingen, waarden, vooroordelen, aannames en dergelijke zijn bepalend voor de mate waarin een organisatie succes kan boeken. Het kunnen herkennen van je eigen mentale model en die van anderen is een belangrijke vaardigheid. Dit helpt elkaars wereld en taal te begrijpen.

Systeemdenken
Het is vaak verleidelijk om een probleem niet in zijn context te zien maar te proberen op te lossen. Het dichten van een lek maar de achterliggende oorzaak niet aanpakken. In het geval van informatieveiligheid een incident verhelpen. Door in dit geval informatieveiligheid systemisch te benaderen kan ook geleerd worden van de totale context waarin het probleem zich voordoet. Hierdoor kunnen fundamentele oplossingen gecreëerd worden. Het als zodanig benaderen van een probleem is een belangrijke competentie van een manager of bestuurder.

Afbakening scope

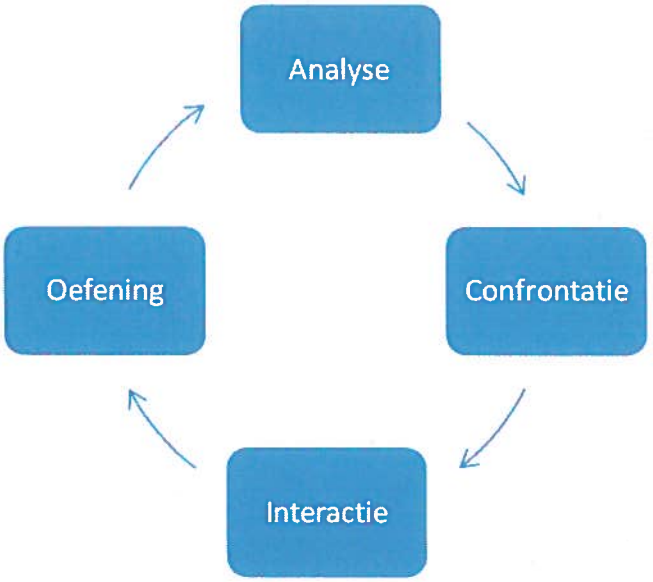
Organisatieleren onderscheidt verschillende doelgroepen, die een verschillende benadering vragen:

- Bestuurders;
- Topmanagement zoals gemeentesecretaris en directeuren;
- CIO en ICT-management, zoals CISO;
- ICT-professionals;
- Alle medewerkers.

De Taskforce BID richt zich volgens haar opdracht op de eerste 3 doelgroepen. Ze stimuleert en motiveert koepelorganisaties, belangenverenigingen en leveranciers om

de andere twee doelgroepen zo goed mogelijk te bedienen. Initiatieven die andere overheden kunnen inspireren of herbruikbaar zijn bij andere overheden gericht op deze laatste twee doelgroepen, zet de Taskforce BID in de etalage.

3.3 Aanbod organisatieleren



Aanbod leren: zelftest, Gateway

Aanbod verankeren: GAP-analyse, nulmeting, self assessment

Aanbod leren: confrontatiefilms, confrontatieworkshops, simulatie, bewustwordingspresentaties

Aanbod verankeren: top 10 risico's in beeld

Aanbod leren: dialoogsessies, risicobewustzijn sessies, procesworkshops

Aanbod verankeren: top 10 stuurvragen, bestuurlijke beleidsprincipes, profielen, peer reviews

Aanbod leren: oefenscenario's incidenten, managementgame, verankersessies

Aanbod verankeren: systematiek voor risicoanalyses, draaiboeken incidenten, handboek optimalisatie processen, systematiek voor veranderen en bijstellen, formats plannen

4 Leeraanbod

De Taskforce BID ontwikkelt eigen leeraanbod voor bestuur en topmanagement. Dit doet ze waar mogelijk samen met overheden. Daarnaast biedt de Taskforce BID bestaand leeraanbod op gebied van informatieveiligheid binnen de overheid een etalage. De Taskforce BID wil hiermee hergebruik van goede opleidingen en goede mediamix stimuleren. Bij alle doelgroepen binnen organisatieleren.

Behoefte binnen overheid

De Taskforce BID werkt met verschillende overheidslagen aan programmeringen. In de gesprekken met deze overheidslagen kwam de volgende behoefte op gebied van 'leren' naar voren waarvoor nog geen aanbod bestaat op bestuurlijk en topmanagement niveau:

- Meer kunnen sturen vanuit risicobewustzijn en risico-omgang
- Hulp bij bedenken en formuleren stuurvragen informatieveiligheid
- Gat dichten tussen bestuur en techniek: zelfde taal leren spreken
- Leren aansluiten bij huidige bestuurlijke thema's en projecten
- Bewustzijn creëren aan de hand van belang continuïteit en kwaliteit
- Samenwerking intern en extern stimuleren
- Hergebruik van opleidingen

4.1 Etalage bestaand leeraanbod

De Taskforce BID verkent bestaand leeraanbod binnen de overheid dat organisatieleren bevordert. Dit aanbod deelt de Taskforce BID via een 'etalage' op haar site (nog in te richten).

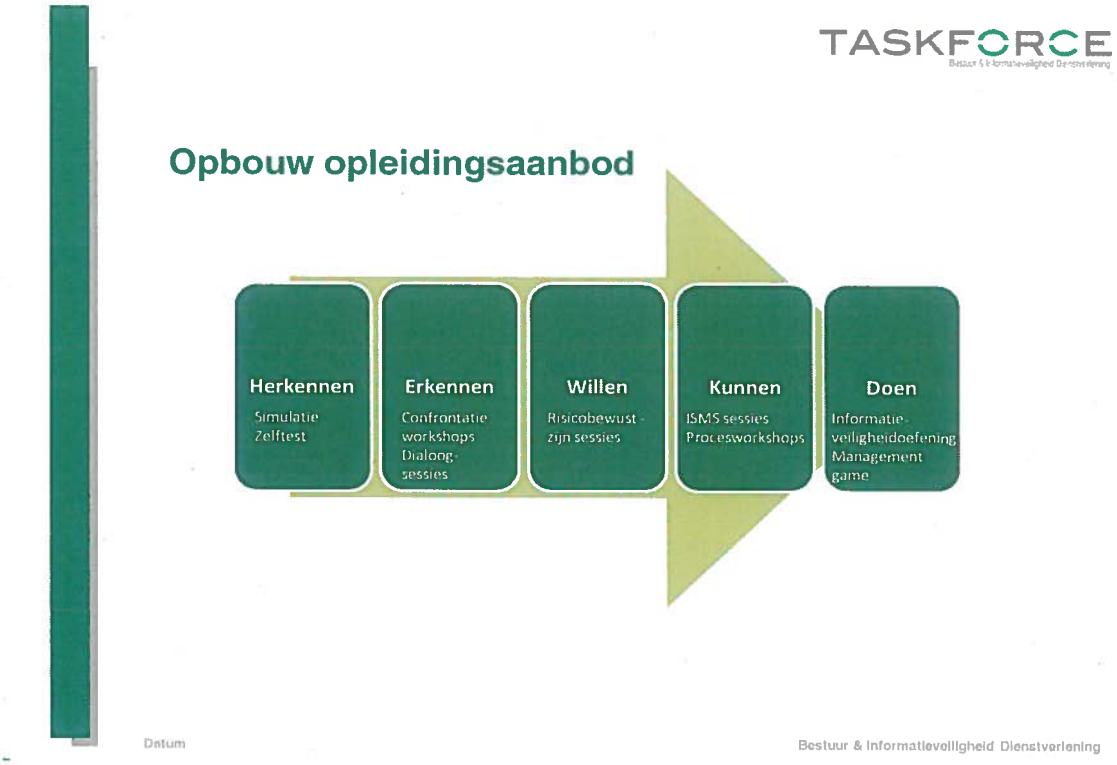
Criteria voor etalage

- Aanbod werkt aan verhogen van één of meer competenties voor organisatieleren;
- Aanbod is beproefd in de praktijk of in een pilot;
- Aanbod is makkelijk herbruikbaar door andere overheden of aanpasbaar op eigen situatie andere overheden;
- Aanbod is gratis te gebruiken.

4.2 Ontwikkeling eigen leeraanbod

De Taskforce BID ontwikkelt daarnaast eigen leeraanbod, via aanbesteding. De leerinstrumenten die de Taskforce BID ontwikkelt, zijn:

- Zelftest
- Simulatie
- Confrontatieworkshop
- Dialoogsessie bestuur/topmanagement – CISO
- Risicobewustzijn sessie
- Verankersessies (ISMS)
- Procesworkshops
- Informatieveiligheidoefening
- Management game (oefening)



4.3 Leerinstrumenten

1) Zelftest:

online zelftest die basiskennis en bewustzijn checkt op gebied van informatieveiligheid bij bestuurders.

Doelgroep:

- Bestuurders

Wanneer inzetten: Altijd

2) Simulatie:
awareness simulatie die dilemma's en verantwoordelijkheden benadrukt bij een incident of crisis.

Doelgroep:

- Bestuurders en topmanagers

Wanneer inzetten:

- Als er geen incidentmanagementproces en responsbeleid is
- Als er geen crisisteam met standaardproces is ingericht
- Als bestuur en topmanagement niet meedraaien in crisisteam

3) Confrontatieworkshop:
Awareness workshop die via een praktijkcase het belang van actieve rol bestuur en het stellen van juiste stuurvragen benadrukt.

Doelgroep:

- Bestuurders en topmanagers
- Topmanagers en lijnmanagers

Wanneer inzetten:

- Als bestuurders en topmanagers (nog) geen actieve rol spelen bij informatieveiligheid
- Als bestuurders en topmanagers niet weten welk stuurvragen (bij incidenten uit cases) te stellen
- Als er geen intern draaiboek bestaat voor incidenten uit cases

4) Dialoogsessie:
Sessie waarin bestuur en CISO/informatiebeveiligers bespreken hoe ze elkaar (beter) kunnen verstaan en kunnen samenwerken om informatieveiligheid te optimaliseren.

Doelgroep:

- Bestuurders/topmanagers en CISO/informatiebeveiliger

Wanneer inzetten:

- Als bestuur en CISO elkaars taal niet spreken
- Als samenwerking op gebied van informatieveiligheid stokt bij bestuur
- Als bestuurders en topmanagers niet weten welk stuurvragen te stellen
- Als CISO/informatiebeveiligers niet weten welke informatie het bestuur en het topmanagement nodig heeft om bestuurlijke/management beslissingen te nemen

5) Risicobewustzijn sessie:
Sessie waarin bestuurders, topmanagers en CISO/informatiebeveiligers het gesprek aangaan in welke mate de organisatie bereid is om risico's te accepteren, geredeneerd vanuit bestuurlijke belangen, en welke preventiestrategie ze kiezen voor de risico's die ze niet willen accepteren.

Doelgroep:

- Bestuurders, topmanagers en CISO/informatiebeveiliger

Wanneer inzetten:

- Als bestuurders geen opdrachtgever zijn voor risicoanalyse en risicomanagement en de CISO/informatiebeveiligers dit graag willen veranderen
- Als bestuurders opdrachtgever willen zijn voor risicoanalyse en risicomanagement
- Als CISO/informatiebeveiligers niet weten welke informatie bestuurders en topmanagers nodig hebben om risicobewust te maken en van daaruit de strategie (lees: prioritering van maatregelen) te bepalen.

6) Verankersessie:
Sessie waarin topmanagers en informatiebeveiligers de verankering van het beleid, de sturing op uitvoering en het bijstellen, vormgeven via principes van ISMS.

Doelgroep:

- Topmanagers en informatiebeveiligers

Wanneer inzetten:

- Als topmanagers het beleid actief willen uitdragen
- Als topmanagers niet weten hoe ze kunnen sturen

7) Procesworkshops:
Workshops waarin de stuurvragen op gebied van informatieveiligheid voor de top 5

processen doorlopen worden en de opdrachten voor aanscherping van de processen gegeven worden

Doelgroep:

- Topmanagers en CISO/informatiebeveiliger

Wanneer inzetten:

- Als topmanagers niet weten hoe informatieveiligheid te koppelen aan primaire processen
- Als topmanagers willen sturen op vormgeving van processen op gebied van informatieveiligheid

8) Management game:
Game waarin bestuur, topmanagement en CISO alle stuurvragen en opdrachten op alle aspecten van zelfregulering oefent in een game.

Doelgroep:

- Bestuur, topmanagement en CISO

Wanneer inzetten:

- Als bestuurders en topmanagers het belang van sturing op samenwerking binnen informatieveiligheid zien
- Als bestuurders en topmanagers het belang van verplichtende zelfregulering zien en die zelfregulering wil gaan toepassen
- Als bestuurders en topmanagers een actieve rol wil spelen binnen informatieveiligheid

Onderbouwing leerinstrumenten

Het aanbod in spoor 'leren' is gebaseerd op:

- Bewustzijnstadia;
- De leerdoelen;
- De rol van doelgroep bij verdere verankering;
- De competenties.

Gerichtheid	Aanbod	Competenties	Verandering in kennis, houding, vaardigheden
(H)erkennen/ weten	Zelftest en bewustwordings-presentaties <u>Ondersteunend verankeringsinstrument</u>: Best practices	Integraal leren Gedeelde visie	<u>Bestuurders en topmanagers</u> weten wat informatieveiligheid in de breedte inhoudt. <u>Bestuurders en topmanagers</u> erkennen het belang van een werkende cyclus op gebied van informatieveiligheid.
	Simulatie	Goed opdrachtgeverschap Integraal leren	<u>Bestuurders en topmanagers</u> erkennen de noodzaak tot sturen op informatieveiligheid. <u>Bestuurders en topmanagers</u> erkennen de noodzaak tot samenwerking binnen en buiten eigen organisatie.
Willen	Confrontatieworkshops, dialoogsessies en risicobewustzijn sessies <u>Ondersteunend verankeringsinstrument</u>: Top 10 stuurvragen Bestuurlijke beleidsprincipes IB Systematiek voor risicoanalyse	Mentale modellen Systeemdenken	<u>Bestuurders en topmanagers</u> kennen problemen/risico's binnen eigen organisatie (en binnen ketens). <u>Bestuurders en topmanagers</u> weten wat de top 10 risico's is en welke impact deze calamiteiten en incidenten hebben op bedrijfsvoering en dienstverlening. <u>CISO/informatiebeveiliger</u> kan gesprek met bestuur en topmanagement voeren over risico's en impact daarvan, in taal van bestuur en

			topmanagement.
Kunnen	Procesworkshops Ondersteunend verankeringsinstrument: Handboek optimalisatie processen	Goed opdrachtgeverschap Systeemdenken	Secretarissen kunnen sturen op het vormgeven van processen op gebied van informatieveiligheid. Directeuren/afdelingsmanagers kunnen sturen op het goed verlopen van processen op gebied van informatieveiligheid.
Doen	Verankersessies en managementgame Ondersteunend verankeringsinstrument: Top 10 stuurvragen Bestuurlijke beleidsprincipes IB Protocol melden incidenten Systematiek voor veranderen en bijstellen	Goed opdrachtgeverschap Gedeelde visie Systeemdenken Integraal leren Mentale modellen	Bestuurders en topmanagers kunnen beleid binnen eigen organisatie op gebied van informatieveiligheid uitdragen. Bestuurders en topmanagers handelen volgens beleid en tonen hiermee voorbeeldgedrag. Bestuurders voelen zich opdrachtgever voor risicomanagement, ontwikkeling en naleving van beleid op gebied van informatieveiligheid en controlemechanismen. Secretarissen voelen zich opdrachtgever voor uitvoering van het beleid, toepassing van de norm en informatieveiligheid-oefeningen Raadsleden kunnen sturen op optimale resources op informatieveiligheid binnen de bedrijfsvoering.

			Directeuren/afdelingsmanagers voelen zich opdrachtgever voor training en opleiding op gebied van informatieveiligheid. CISO/informatiebeveiliger voelt zich verantwoordelijk voor het delen van de inhoud van het beleid op gebied van informatieveiligheid binnen de hele organisatie. CISO/informatiebeveiliger maakt actieplannen voor bijstelling en kennisdeling na jaarlijkse controle en audits.
	Instructiesessie monitoring Ondersteunend verankeringsinstrument: Format overdrachts-rapportage	Goed opdrachtgeverschap	Bestuurders en topmanagers kunnen rapporteren aan domein en stelsel.
	Oefenscenario's calamiteiten en incidenten Ondersteunend verankeringsinstrument: Voorbeeld draaiboek calamiteiten en incidenten	Goed opdrachtgeverschap Integraal leren	Secretarissen geven opdracht voor periodieke oefeningen ter beheersing van calamiteiten en incidenten op gebied van informatieveiligheid. Overheidsorganisaties oefenen periodiek ter beheersing van calamiteiten en incidenten op gebied van informatieveiligheid

5 Vermarkten aanbod

Welke stappen kan de Taskforce BID zetten om haar doelgroepen te bereiken en haar aanbod te vermarkten? Bestuurders en topmanagers hebben drukke agenda's. Hoe krijgt de Taskforce BID haar aanbod toch bij deze doelgroepen?

5.1 Inzet aanbod

De Taskforce BID zet de volgende stappen om haar doelgroepen te bereiken:

Stap 1: via pilots

De Taskforce BID zal haar opleidingsaanbod in een aantal pilots toetsen. Ze benadert uit elke overheidslaag een aantal organisatie om hieraan mee te doen. Met die organisatie toetst de Taskforce BID of haar aanbod aansluit bij de behoefte, effectief is en in welke mix het aanbod het best werkt. De leerervaringen uit de pilots delen de deelnemende organisaties via verschillende communicatiemiddelen om andere bestuurders en topmanagers te enthousiasmeren.

Stap 2: via bestaande opleidingen en themadagen

De Taskforce BID zal het getoetste aanbod waar mogelijk incorporeren in bestaande opleidingen en inzetten tijdens bestaande themadagen binnen de overheid. De Taskforce BID verkent hiervoor bestaande opleidingen die de opdracht van de Taskforce BID raken. Ook kunnen bestaande opleidingen voor ICT-professionals en medewerkers het aanbod overnemen en aanpassen voor deze doelgroepen. De Taskforce BID zal haar aanbod hiervoor aanbieden op de etalage op haar site.

Stap 3: via bestaande congressen

De Taskforce BID biedt het leeraanbod aan tijdens sessies op bestaande congressen waar bestuurders en topmanagers al komen.

Stap 4: via een vijftal vaste opleidingsmomenten

De Taskforce BID organiseert vijf keer cursusdagen waar geïnteresseerde bestuurders en topmanagers het opleidingsaanbod kan volgen. Bestuurders en topmanagers worden hiervoor gericht uitgenodigd. Een groep erkende sprekers uit bestuur en topmanagement binnen de overheid zal deze opleidingsmomenten promoten en een deel van de sessies moderen.

Marketing
Bekendheid met het leeraanbod is cruciaal. Een marketingplan bij deze stappen is noodzakelijk. De communicatie-expert van de Taskforce BID zal deze verzorgen.

5.2 Inzet trainers

De sessies en workshops zullen door een groep trainers gefaciliteerd worden. De Taskforce BID vormt deze groep uit erkende sprekers en trainers binnen de overheid en een aantal commerciële trainers. Het idee is dat de trainers alle sessies en workshops kunnen begeleiden. Zodat ze goed kunnen sturen op resultaat en samenhang. Deze groep trainers zal zo snel mogelijk geworven moeten worden. Via een train de trainer opleiding zal de groep de leerstrategie en het aanbod eigen maken.

Het idee is om het leeraanbod het laatste half jaar ook te laten adopteren door leveranciers en interne trainers binnen de overheid. Zodat het leeraanbod geborgd wordt. Geïnteresseerde leveranciers en interne trainers kunnen een train de trainer opleiding volgen.

6 Actielijnen

Hoe wordt dit opleidingsplan gerealiseerd? Welke actielijnen ziet de Taskforce BID voor de komende maanden? Een eerste aanzet van deze actielijnen. De actielijnen worden waar nodig in aparte plannen verder uitgewerkt.

6.1 Ontwikkeling leeraanbod

Wanneer	Wat
Mei t/m juli	Offerteaanvragen leerinstrumenten Coördinatie ontwikkeling leerinstrumenten Koppeling aan verankerinstrumenten
September/oktober	Offerteaanvraag managementgame Coördinatie ontwikkeling managementgame Koppeling aan verankerinstrumenten

6.2 Samenstellen groep trainers voor leeraanbod

Wanneer	Wat
Juni	Keuze maken voor trainers binnen overheid of commercieel, of mix Offerteaanvraag moderatie leerinstrumenten
Juli	Train de trainer sessie op deel 1 leeraanbod Begeleiding trainers

6.3 Pilots leeraanbod

Wanneer	Wat
Mei t/m juli	Invulling pilots gemeenten
Juni	Start pilots gemeenten

	Invulling pilot provincie en ZBO

6.4 Etalage ontwikkelen en vullen

Wanneer	**Wat**
Juni	Voorstel opzet etalage
Juli	Verkenning van bestaand opleidingsmateriaal in de markt
Juli - september	Vullen etalage

6.5 Leeraanbod in programmeringen

Wanneer	**Wat**
Juni	Programmeringen bespreken
Juli - september	Planning leeraanbod in programmeringen inbrengen Bijstellen programmeringen waar nodig

6.6 Opleidingsmomenten

Wanneer	**Wat**
Juni	Voorstel opzet opleidingsmomenten
Juli	Organisatie eerste opleidingsmoment
Augustus	Begeleiden opleidingsmoment

6.7 Marketing

Wanneer	**Wat**
Juni	Opdracht en check marketingplan leeraanbod

Juli	Eerste marketingcampagne voor leeraanbod

7 Borging

De Taskforce BID is opgericht voor de duur van 2 jaar. De komende tijd bekijkt de Taskforce BID hoe ze het aanbod kan borgen. Waar het kan gebeurt dit via (het verbinden van) bestaande opleidingsinstituten (i-Academy KING, bestuursacademie,etc.) binnen de overheid. Een verkenning van deze opleidingsinstituten vindt op dit moment plaats.