centrum informatiebeveiliging en privacybescherming

Sturen op informatieveiligheid; handvatten voor bestuurders en CISO

Met 7 drivers die aansluiten op de Baseline Informatiebeveiliging Overheid

Maart 2022 [versie 1.1]

Titel	Sturen op informatieveiligheid; Handvatten voor bestuurders en CISO's
Datum	Maart 2022
Status	Versie 1.1
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	Maarten Baljon, Ad Reuijl
Reviewers	CIP kernteam, Mariëlle de Groot, Margot van der Linden

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als uit de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Inhoudsopgave

1. Inleiding

De Nederlandse samenleving en de overheid digitaliseren. Dat biedt veel nieuwe kansen, maar geeft ook nieuwe bedreigingen, bijvoorbeeld voor de informatieveiligheid. U kent de voorbeelden vast uit het nieuws. Organisaties die gegijzeld worden door hackers, en niet meer bij hun eigen gegevens kunnen zonder betaling. Ze kunnen hun taken niet meer uitvoeren. Of vertrouwelijke gegevens liggen na een datalek op straat. Die bedreigingen worden steeds groter, en dat stelt hogere eisen aan de organisatie. En daarmee ook aan u als bestuurder, de directie, businessverantwoordelijken en de CISO (Chief Information Security Officer).

1.1 Inhoud en leeswijzer

Dit stuk bevat praktische handvatten voor bestuurders en CISO's om de sturing op informatieveiligheid in de organisatie op te pakken. Deze aanpak is ontwikkeld op basis van gesprekken in 12 overheidsorganisaties.

Bestuurders

De inleiding is geschreven voor bestuurders en CISO's. Geïnteresseerde bestuurders vinden daarnaast in hoofdstuk 2 een blauwdruk voor de sturingscyclus op informatieveiligheid. Hoofdstuk 3 geeft meer inzicht wat de 7 drivers voor de organisatie inhouden, met een aantal verdiepingsvragen op alle 7 drivers.

CISO's en informatieveiligheidsprofessionals

- Hoofdstuk 2 bevat naast de opzet voor een gesprekcyclus een praktische aanpak om de hele organisatie te betrekken.
- Hoofdstuk 3 gaat dieper in op de 7-drivers, met een uitgewerkte vragenlijst, en suggesties voor KPI's. Dit is de basis voor afspraken tussen bestuurder en de CISO. In de bijlage staat een voorbeeld van een opdrachtbrief om deze afspraken te bekrachtigen.
- Hoofdstuk 4 is vooral bedoeld voor de CISO (en zijn team): de vertaling van gemaakte afspraken in meetbare resultaten, en het opstellen van een dashboard dat de voorgang inzichtelijk maakt voor bestuurders en afdelingen.

1.2 Informatieveiligheid als chefsache

Als bestuurder bent u verantwoordelijk voor een veilige informatievoorziening in uw organisatie, als voorwaarde voor de dienstverlening en de bedrijfsvoering. Informatieveiligheid is dus chefsache, daar zijn de meeste bestuurders en managers zich vaak wel van bewust. Het is aan u als bestuurder om te bepalen welke risico's de organisatie neemt. Nul risico bestaat niet, het gaat erom dat de maatregelen die uw organisatie neemt die risico's terugbrengen tot een acceptabel niveau. De Nederlandse overheid heeft in 2020 een gemeenschappelijk kader vastgesteld voor een basisveiligheidsniveau: de Baseline Informatiebeveiliging Overheid (BIO). Op basis van een risicoanalyse specificeert en prioriteert de organisatie de generieke maatregelen uit de BIO, werkt deze zo nodig uit naar specifieke maatregelen en stuurt daarop. Het proces waarmee de organisatie de effectiviteit van de genomen maatregelen ten opzichte van de toenemende risico's beoordeelt, hoort continu plaats te vinden. Zo kan steeds worden bepaald wat (extra) nodig is om informatie steeds adequaat te kunnen beschermen.

1.3 Samenspel tussen bestuurder en CISO

Informatieveiligheid krijgt in de praktijk handen en voeten in een samenspel tussen bestuurders, (top)management en experts als de CISO, de Functionaris Gegevensbescherming (FG) en/of een beleidsadviseur Informatieveiligheid. In de praktijk blijkt dat samenspel vaak nog lastig. Voor veel bestuurders gaan die gesprekken te vaak over technische details van de maatregelen, en ze haken daardoor af. Gevolg is dat de sturing op informatieveiligheid in veel organisaties het exclusieve terrein is van de CISO en zijn team.

1.4 Handvatten voor gesprek en sturing

Dit document biedt u en de experts binnen uw organisatie handvatten om informatieveiligheid in samenspel daadwerkelijk chefsache te maken. Zodat u bewust en goed geïnformeerd keuzes kunt maken over de risico's die uw organisatie loopt, en actief sturing kunt geven. De geschetste aanpak biedt u meer kennis en inzicht om - mocht het onverhoopt misgaan - als bestuurder uw verantwoordelijkheid als crisismanager te pakken. En het biedt een goed uitgangspunt om verantwoording af te leggen over risico's, keuzes, maatregelen en beleid.

7 drivers: zeven onderwerpen voor een goed gesprek met de CISO

Zeven onderwerpen (de zogenaamde *drivers* van informatieveiligheid) helpen bij een goed gesprek tussen bestuurder en CISO. Deze drivers hangen samen met de BIO. Ze bieden een clustering, selectie en nadere verdieping van de meest kritische onderwerpen daaruit.

1. **De kroonjuwelen goed beschermen**

De kroonjuwelen zijn die gegevens, processen en applicaties die (de continuïteit van) de dienstverlening en bedrijfsvoering in gevaar brengen als er iets mee gebeurt. Een risico-analyse focust dan ook op het inzichtelijk krijgen van die kroonjuwelen:

- Welke processen en applicaties – ofwel welke delen van het hele informatievoorzieningslandschap (IV-landschap) - zijn cruciaal?
- Welke gegevens mogen zeker niet op straat komen te liggen?

De volgende zes drivers zijn bedoeld om

- Te bepalen welke maatregelen nodig zijn om deze risico's op een aanvaardbaar niveau te krijgen.
- Continu vinger aan de pols te houden.

2. **Kijk verder dan de eigen organisatie**

Maak goede afspraken met leveranciers en ketenpartners in lijn met de BIO en aanvullende kaders.

3. **Zorg dat wat veilig is, ook veilig blijft**

Doe tijdig security-updates om nieuwe technische bedreigingen het hoofd te kunnen bieden En vervang oude software tijdig.

4. **Veilig werken, ook thuis**

Pas 2-factor authenticatie consequent toe. Stel hoge(re) eisen aan bijzondere toegang.

Zorg voor adequate afhandeling van incidenten. Creëer een klimaat waarin medewerkers zich veilig voelen om incidenten te melden, óók als hun eigen gedrag daarbij een rol heeft gespeeld.

5. **Afscherming, detectie, monitoring en response**

Bescherm de toprisico applicaties door segmentatie tegen domino-effecten; voorkom dat uitval van een een applicatie leidt tot uitval van andere of zelfs het hele IV-landschap. Zorg voor detectie, monitoring en response (CERT- en SOC-diensten).

6. **Effectief handelen bij incidenten en crisissen**

Zorg voor een waterdichte herstel-aanpak voor toprisico applicaties. Oefen regelmatig met cybercrisismanagement.

7. **Meet, leer en stuur bij**

Meet de kwaliteit van securityprocessen met self-assesments. Houd medewerkers scherp op feitelijk security-gedrag, bijvoorbeeld met redteaming.

Van een goed gesprek naar effectieve sturing

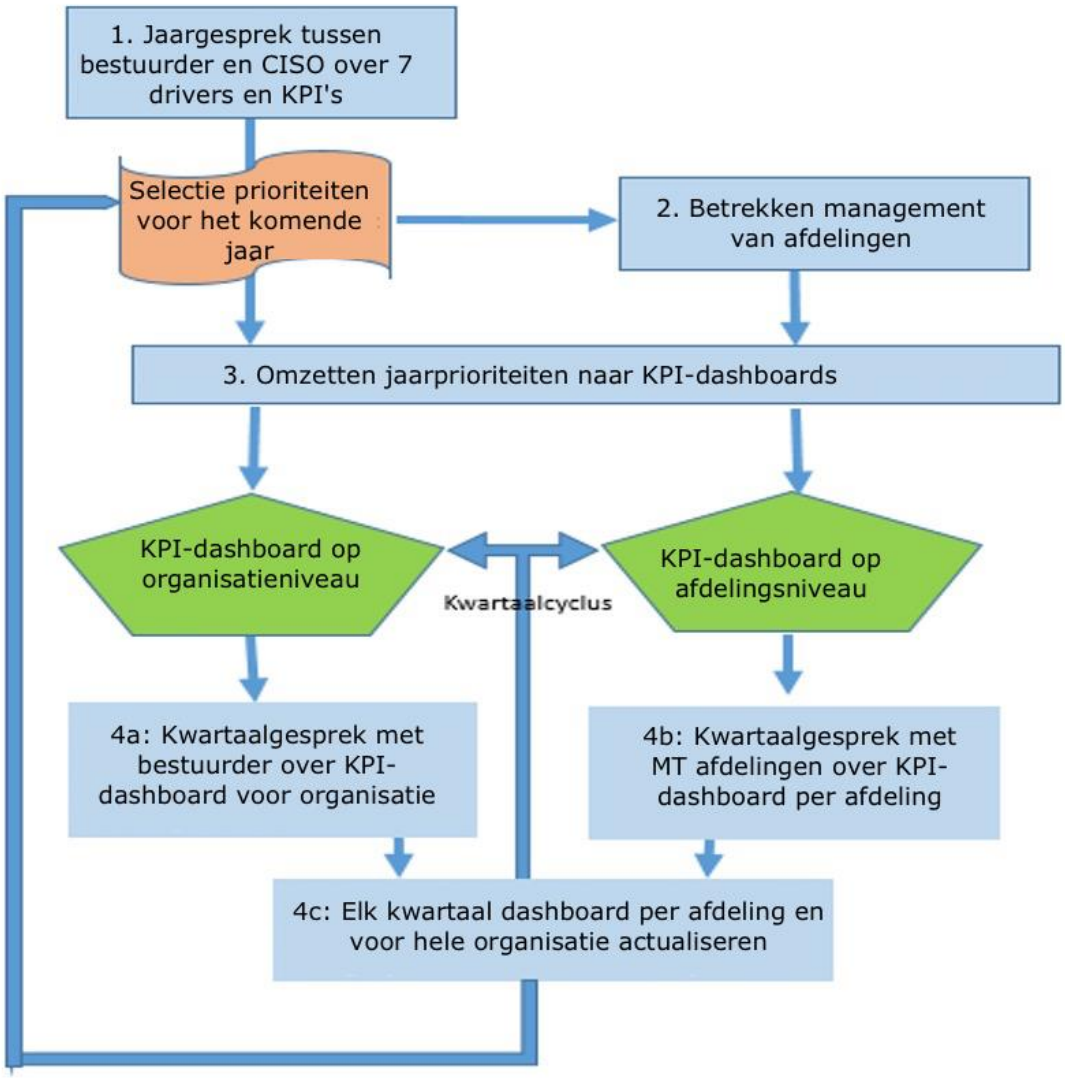
Met de zeven drivers kunt u de weerbaarheid, het herstelvermogen en een continu verbeter- en leerproces (leervermogen) in samenhang bespreken. Sturing begint met goede gesprekken tussen bestuurder en CISO. U leert elkaars werelden en opgaven beter te begrijpen. Een volgende stap is om samen afspraken te maken over wat de organisatie wil bereiken op het gebied van informatieveiligheid en de te nemen maatregelen daarvoor. In hoofdstuk 3 vindt u de verdieping op de drivers, met een aantal vragen die u kunt stellen De drivers en gerichte vragen daarover geven u tijdens het gesprek meer grip op de informatieveiligheid van uw organisatie, maar ook daarna. Door regelmatig de voortgang en nieuwe ontwikkelingen te bespreken, komt u als bestuurder steeds meer aan het roer. Een gesprekscyclus op basis van afspraken en een periodieke rapportage op basis van KPI’s stellen u in staat steeds actiever te sturen.

2. Van gesprek tot sturing: een aanpak

Incidenten met grote impact op informatiebeveiliging en privacy komen veel voor. Met goede sturing en een gedegen aanpak zijn de kansen op een onvoorspelbare en slechte afloop tot een aanvaardbaar niveau terug te brengen. Die aanpak begint met een gesprek over de zorgen en prioriteiten van de bestuurders aan de hand van de 7 drivers. Dit hoofdstuk beschrijft stap voor stap hoe bestuurder en CISO op basis van dat gesprek samen de sturing op informatieveiligheid kunnen vormgeven.

2.1 Jaarcyclus

De jaarcyclus ziet er als volgt uit.



In de beschrijving hieronder wordt vooral beschreven hoe de stappen in het eerste jaar kunnen worden doorlopen. Dat eerste jaar zal best wennen zijn omdat het proces nieuw is. Wellicht is er weerstand in de organisatie die overwonnen moet worden. Na dit eerste jaar is het de uitdaging om de aandacht vast

te houden. Dat gebeurt door het besef van de urgentie levend te houden en jaarlijks de prioriteiten bij te stellen. Blijvend support en sturing van de bestuurder(s) is daarbij cruciaal.

2.2 Stappenplan jaarcyclus

Hoe zet je zo'n jaarcyclus op? Volg daarvoor deze vier concrete stappen.

Stap 1: gesprek tussen bestuurder en CISO

Plan een (jaar)gesprek met bestuurder en CISO. Het gesprek kent de volgende onderwerpen:

1. Bespreek de grootste zorgen en prioriteiten van de bestuurder over informatieveiligheid en privacy. Gebruik als kapstok de 7 drivers.
2. Loop met de bestuurder de 7-driver vragenlijst langs (zie hoofdstuk 3). Licht de belangrijkste aspecten per driver kort toe. Noteer per driver welke van de vragen bij de bestuurder leven.
3. Verwerk de antwoorden van de bestuurders in een jaarprioriteitenoverzicht op basis van de 7 drivers. In Hoofdstuk 4 is beschreven hoe je deze kunt opstellen. Voor de CISO: het kan handig zijn om voorafgaand aan het gesprek al een concept-KPI-jaarprioriteitenoverzicht op te stellen en dat dan tijdens of na het gesprek bij te werken.
4. Formuleer een bondig gespreksverslag en deel deze met je bestuurder.
5. Stel een opdrachtbrief op (zie het voorbeeld in bijlage 1) om de afdeling-MT's te betrekken. In deze brief benadrukt de bestuurder/directie het belang om het dashboard met prioriteiten elk kwartaal bij te werken en deze met de bestuurder/directie als met de afdeling-MT's te bespreken.

Advies: stap voor stap invoeren

Aanbeveling is om de sturing op de 7 drivers gefaseerd in te voeren, bijvoorbeeld als volgt:

- Kies jaarlijks drie maatregelen uit de 7-driver-set.
- Continueer deze rapportages in volgende jaren, en pak elk jaar drie dashboard items erbij.

Stap 2: betrek het afdelingsmanagement

Gebruik de opdrachtbrief voor het gesprek met (de leden van) de afdeling-MT's en met de IB&P stafmedewerkers van elke afdeling. Bijvoorbeeld met de volgende stappen:

1. Informeer de in de opdrachtbrief vermelde direct betrokkenen over de goedkeuring van de prioriteiten en de rapportage daarover door de bestuurder.
2. Stuur ze het concept jaarprioriteitenoverzicht met de afspraken over rapportage, en een concept dasboard.
3. Maak afspraken in de agenda's om deze met iedereen individueel of in groepjes door te nemen en om aanvullingen verbetersuggesties te krijgen en te bespreken.

Stap 3: Vertaal het jaarprioriteitenoverzicht in een KPI-dashboard

1. Zet de beantwoorde vragen om naar een aansprekend dashboard. (Hoe je dit doet, lees je in hoofdstuk 4).
2. Neem het proces rond de statusupdate van de KPI's door met de betrokkenen, je team(s), op elke afdeling. Organiseer desnoods een mini-competitie waarbij (het team van) elke afdeling

het klaar speelt om binnen 1 werkdag na de sluitingsdatum van het ISMS of van andere bronapplicaties de KPI-status in het dashboard bij te werken.

Stap 4: Kwartaalgesprekken met bestuurder(s) en afdeling MT's

1. Bespreek ieder kwartaal bij iedere afdeling in het MT de KPI-status van de betreffende afdeling. De IB&P stafmedewerker van de afdeling neemt dan het KPI-dashboard met het voltallige afdelings-MT door.
2. Bespreek het gecombineerde dasboard met KPI-statussen voor de hele organisatie met de bestuurder.
3. Bespreek naast de status ook mogelijk gewenste verbeteringen/uitbreidingen met de bestuurder en de afdeling MT's.
4. Informeer je team(s) over de uitkomsten van de kwartaalgesprekken en bespreek met hen de mogelijkheden om de gewenste verbeteringen/uitbreidingen door te voeren. Breng de wijzigingen die volgens het team mogelijk zijn aan. Op die manier is er een continue verbeteraanpak met een driemaandelijkse voortgangsrapportage.

3. De 7-driver vragenlijst, met KPI's

De vragenlijst in dit hoofdstuk is bedoeld als leidraad voor het gesprek over informatieveiligheid en privacybescherming tussen de bestuurder en de CISO. Alle 7 drivers krijgen verdieping door een aantal concrete vragen. De kritische procesindicatoren (KPI's) daarbij zijn suggesties om de vragen te vertalen in meetbare acties en resultaten. Een periodiek gesprek over deze vragen en de rapportage over de realisatie van de KPI's, kan de bestuurder helpen zijn rol te pakken.

Dit gesprek is overigens niet alleen nodig op bestuursniveau, maar ook op afdelingsniveau, met de MT's. Zij bepalen zelf op basis van risicoafwegingen aan welke van onderstaande onderwerpen zij prioriteit willen geven.

Driver	Draagt bij aan	Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
1. De kroonjuwelen goed beschermen	Weerbaar-heid	- Wat zijn de toprisico's? Wat zijn de kroonjuwelen; de delen van het IV-landschap die top-risico zijn? - Is per kroonjuweel vastgesteld wat de juiste maatregelen zijn om de risico's terug te brengen naar een aanvaardbaar niveau?	- Toprisico's en kroonjuwelen afgestemd, auditplan wordt uitgevoerd volgens planning. - Lijst met toprisico's/kroonjuwelen beschikbaar en besproken met bestuurder. Met: 1. Per kroonjuweel een overzicht van type/klasse van passende maatregelen; 2. Een afgestemd auditplan dat minimaal voorziet in een audit van een externe partij op alle toprisico maatregelen; 3. Verslag bestuurder-CISO met vastlegging van deze bespreking.
2. Kijk verder dan de eigen organisatie	Weerbaar-heid	- Bevatten uitbestedingen en andere ketenafspraken eisen om feitelijke veiligheid en privacy-bescherming te borgen?	Aanbestedingen, inkopen en contracten met alle soorten ketenpartners met een ICT-component zijn voorzien van scherpe informatieveiligheidseisen. 1. In alle nieuwe aanbestedingen/inkopen en contracten met een ICT-component worden specifieke en toepasbare eisen gesteld[1]. 2. Bestaande contracten zijn herijkt op deze toepasbare en specifieke eisen. 3. Overzicht van contracten en aanbestedingen met herijking-status is beschikbaar en gerapporteerd aan bestuurder.

[1] Gebruik bijvoorbeeld de ICO-Wizard voor ondersteuning van aanbestedingen en inkopen;

Driver	Draagt bij aan	Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
3. Zorg dat wat veilig is, ook veilig blijft	Weerbaar-heid	- Nemen de risico's door verouderde soft- en hardware die informatieveiligheid en privacy in de weg staan af in de tijd?	- Patchmanagement is op orde. - Verouderde informatiesystemen die de dienstverlening ondersteunen worden planmatig weggewerkt. - Websites en mail voldoen aan veilige internetstandaarden. 1. Veiligheidspatches worden aantoonbaar tijdig aangebracht. Tijdig is: passend bij de ernst van de dreiging en kans van misbruik en overeenkomstig advies van de betrokken leverancier/CERT; 2. Voor web en mail wordt voldaan aan de standaarden van de Pas-Toe-of-Leg-Uitlijst van Forum voor Standaardisatie: streefscore internet.nl: 100%; 3. Er is een plan om verouderde hard/software risico-gebaseerd weg te werken. 4. Dit vernieuwingsplan wordt volgens planning uitgevoerd.
4. Veilig werken, ook thuis	Weerbaar-heid	- Is toegang voldoende afgeschermd? - Worden incidenten adequaat afgehandeld? - Neemt de meldingsbereidheid toe? - Neemt de ernst van incidenten af?	Toegangsmanagement voldoet aan aangescherpte eisen. Incidenten worden afgehandeld conform de vereisten uit de BIO. Meldingsbereidheid neemt aantoonbaar toe. 1. 2FA (2 factor authenticatie) wordt toegepast voor reguliere toegang conform NCSC-publicaties; 2. Ook bijzondere toegang voor beheer/foutherstel en testen is ingericht conform NCSC-publicaties; 3. Uit een periodiek overzicht van aantallen incidenten, gekwalificeerd naar ernst en periode, blijkt: a. een afname van het aantal ernstige incidenten met x% per kwartaal; b. een toename van efficiëntie van de oplossing van incidenten met y% per kwartaal; c. bij een onverminderde meldingsbereidheid.
5. Afscher-ming, detectie, monitoring en response	Weerbaar-heid	- Zijn afdoende maatregelen getroffen om te voorkomen dat uitval van een systeem niet leidt tot uitval van een ander of zelfs van alle systemen? - Worden dreigingen die mogelijk disruptief zijn voor onze dienstverlening of bedrijfsvoering bijtijds gesignaleerd?	Segmentering van het IV-landschap is zodanig ingericht dat de kans op (malware-)besmettingen van kroonjuwelen/toprisico segmenten sterk is gereduceerd. 1. Een SOC op 7x24 basis is ingericht conform NCSC/IBD/sector CERT adviezen/eisen; 2. CERT aansluiting 100% operationeel en alle CERT adviezen worden binnen de gestelde termijnen uitgevoerd; 3. Er is een actueel overzicht van de doorgevoerde segmentering binnen het IV-landschap en een audit op de robuustheid daarvan; 4. Er is een plan voor het oplossen van de manco's in de segmentering van het IV-landschap en dit plan wordt uitgevoerd conform planning.

Driver	Draagt bij aan	Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
6 Effectief handelen bij incidenten en crisissen	Herstelvermogen	- Is de crisisorganisatie voldoende geëquipeerd om in te grijpen bij crises door hacks en datadiefstal? - Is recovery te allen tijde mogelijk?	Back-up & recovery is adequaat geborgd. Crisisplan is compleet en actueel en wordt periodiek beproefd. 1. Er is een actueel backup- en recoveryplan, geaccordeerd door het verantwoordelijk management; 2. Er is een actueel business-continuïteit-managementplan, geaccordeerd door het topmanagement; 3. Beide plannen worden minimaal 1 keer per jaar geoefend, actualisaties en leerpunten worden direct verwerkt in de plannen.
7 Meet, leer e stuur bij	Leervermogen	- Is er een cultuur van eigenaarschap en verantwoord gedrag in de organisatie? - Zijn de processen voor de bescherming tegen IB&P-bedreigingen op orde? - Groeien deze processen mee met de toenemende kwetsbaarheden?	De volwassenheid voor zowel informatie- als privacybescherming is op het minimaal vereiste niveau en neemt jaarlijks toe conform gemaakte afspraken. Feitelijk gedrag wordt regelmatig getest en uitkomsten daarvan zijn conform afspraken. 1. IB-volwassenheid is minstens niveau 3 op schaal 1-5 van de BIO-Self assessment en groei ervan is conform afspraken; 2. P- volwassenheid is minstens niveau 3 op schaal 1-5 van de Privacy Self assessment en groei ervan is conform afspraken; 3. Gedragstoetsing in vormen als phishing-acties en red-teaming vinden regelmatig plaats; de leerpunten worden gebruikt voor: a. Het dichten van de gaten in de veiligheid van processen en systemen; b. Terugkoppeling van confronterende boodschappen ter bevordering van bewustzijn en verantwoord gedrag. 4. Elke ondernomen gedragstoetsing wordt gepresenteerd aan het management met daarin de belangrijkste leerpunten. 5. Is er een toereikend aanbod van leermiddelen voor alle werknemers en ook vooor bestuurders voorhanden en wordt dat goed benut?

4. Omzetten van de jaarprioriteiten naar meetbare KPI's

In dit hoofdstuk worden per driver suggesties gedaan om (de antwoorden op) de vragen uit het vorige hoofdstuk om te zetten naar (items op) een dashboard. Dit hoofdstuk is vrij gedetailleerd en is vooral bedoeld voor de CISO en andere IB&P stafleden.

Het hoeft overigens geen apart dashboard te zijn, het kan ook een toevoeging zijn aan een bestaand dashboard. Op het dashboard zullen vaak meetwaarden worden getoond. Dat kan ook een antwoord op een ja/nee vraag zijn. Bij sommige items wil je ook nadere details tonen op onderliggende schermen. Bijvoorbeeld om meetwaardes op het eerste scherm - het 'primaire dashboard'- toe te lichten.

Nieuwe tooling nodig? Tips en wenken

Bespreek met een Excel-expert of met een GRC-toolleverancier hoe het afgestemde jaarprioriteitenoverzicht kan worden omgezet naar een dashboard waarin IB&P staf van de afdelingen en andere betrokkenen de status van elke afdeling periodiek kunnen bijwerken. Zorg er ook voor dat in Excel of in het GRC-tool de status van elke afdeling periodiek kan worden gecombineerd tot een status van de hele organisatie.

Wanneer het dashboard klaar is, neem dan het proces van update van de KPI-statussen door met de betrokkenen, je team(s) en de betrokken afdelingen. Organiseer eventueel een mini-competitie rond de uitdaging voor (teams) iedere afdeling om binnen 1 werkdag na de sluitingsdatum van het ISMS of van andere bronapplicaties de KPI-status in het dashboard bij te werken.

4.1 Driver 1: De kroonjuwelen goed beschermen

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
Wat zijn toprisico's/kroonjuwelen en zijn de juiste maatregelen getroffen?	Toprisico's afgestemd, auditplan wordt uitgevoerd volgens planning. Lijst met toprisico's/kroonjuwelen beschikbaar en besproken met bestuurder. Met: 1. Per kroonjuweel vastgesteld welke delen van IV-landschap erbij betrokken zijn 2. Per toprisico een overzicht van (klasse van) mitigerende maatregelen; 3. Er is een auditplan afgestemd met daarin minimaal een audit van derde partij op alle toprisico-maatregelen; 4. Verslag Bestuurder-CISO met vastlegging van deze bespreking.

Een voorbeeldlijst van toprisico's:

A. Risico's voor de dienstverlening en bedrijfsvoering:
   1. Disruptie van primaire klantprocessen
   2. Disruptie keten-dienstverlening
   3. Wegsluizen van gelden
   4. Schade aan imago t.g.v. geslaagde hacks of een groot datalek

B. Oorzakelijke risico's:
   5. Chantage m.b.v. ransomware
   6. Onvoldoende informatieveilig gedrag bij medewerkers, waardoor de kans op hacken en lekken groot is.
   7. Achterstand in het verwerken van veiligheidspatches waardoor de kans op hacken en lekken groot is.

Het is vooral van belang te weten welke risico's voor jouw organisatie in de beleving van de bestuurder (en van afdeling MT-leden) het meest van belang zijn. Wees zelf voorbereid: welke risico's worden in de auditverslagen benoemd? En breng deze in ter aanvulling/aanscherping.

Dit advies tot naslag van de auditverslagen geldt ook voor de mitigerende maatregelen. Zie wat je met deze eerste vraag ophaalt (en vastlegt) vooral als een standopname voordat de organisatie de KPI-sturing oppakt. Bij de drivers 2 t/m 7 worden diverse maatregelen gesuggereerd. Die komen in de beginfase niet geheel overeen met de maatregelen die je nu eerst ophaalt. Laat die verschillen zo.

Bij het auditplan, onderdeel 1.2, kunnen twee eenvoudige overzichten voldoende zijn:

1. Overzicht uitgevoerde audits van de afgelopen twee jaren, met daarbij per audit de belangrijkste bevindingen/adviezen en vermelding of deze zijn opgevolgd;
2. Overzicht met de geplande audits, vermeld daarbij zowel de bevindingen van de voorgaande audit van deze auditor/van dit type audit als ook van de toprisico's waarvoor de audit relevant is.

De standopname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Standopname per item organisatie-breed	Status
1.1: Lijst toprisico's/kroonjuwelen	Mate waarin dit al in beeld is
1.2: Overzicht (klasse van) mitigerende maatregelen per toprisico/kroonjuweel	Mate waarin dit al in beeld is
1.3: auditplan vastgesteld door Bestuur(der)	Status van bespreking/vaststelling van

Per afdeling en/of alleen voor de organisatie als geheel?
Niet alleen de bestuurder, ook per afdeling is het van belang dat het afdeling-MT risico's benoemt en daarin prioriteert en daarvoor mitigerende maatregelen aangegeven. In de standopname per afdeling kunnen de volgende items een plek krijgen:

Standopname per item per afdeling	Status
1.1: Lijst toprisico's/kroonjuwelen	Mate waarin dit al in beeld is
1.2: Overzicht (klasse van) mitigerende maatregelen per toprisico/kroonjuweel	Mate waarin dit al in beeld is

Qua opbouw is het goed als eerst op zijn minst twee, maar liefst alle niet-stafafdelingen hun eigen lijsten opstellen. Deze kunnen dan worden samengevoegd voor de organisatie als geheel. Dat werkt heel goed voor het draagvlak en zorgt dat het beeld aansluit op de praktijk.

4.2 Driver 2: Kijk verder dan de eigen organisatie

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
Bevatten uitbestedingen eisen om feitelijke veiligheid en privacybescherming te borgen?	Aanbestedingen, inkopen en andere ketenpartner-contracten met ICT-component zijn voorzien van scherpe informatieveiligheidseisen. 1. In alle nieuwe aanbestedingen/inkopen en contracten met een ICT-component worden specifieke en toegepaste eisen gesteld. Sterke aanbeveling: gebruik de ICO-wizard, bedoeld voor ondersteuning van aanbestedingen binnen alle overheidslagen. 2. Bestaande contracten worden herijkt met deze toepaste en specifieke eisen; dit verloopt via een afgestemd plan. 3. Overzicht van contracten en aanbestedingen met herijking-status is beschikbaar en gerapporteerd aan bestuurder.

In de formulering van de vragen hierboven wordt uitgegaan van de ICO-wizard. Deze tool is ontwikkeld als onderdeel van de Roadmap Digitaal Veilige Hard- en Software (DVHS). De wizard wordt aanbevolen door de ministeries van BZK en EZK voor overheidsbreed gebruik om eisenpakketten voor informatieveiligheid samen te stellen als bijlagen bij aanbestedingen en contracten. De wizard is ook te gebruiken in relaties met interne ontwikkelafdelingen en met shared service centra.

De standopname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Standopname per item organisatie-breed	Status

2.1: ICO-wizard wordt bij nieuwe aanbestedingen toegepast	Percentage waarin dit het geval is
2.2a: ICO-herijkingsplan is vastgesteld door Bestuur(der)	J/N
2.2b: ICO-herijking verloopt volgens plan	Voortgang t.o.v. plan
2.3: Er is een overzicht van alle ICT-contracten met vermelding van wel/niet ICO benut	Wel/niet gerealiseerd

In de standopname per afdeling die te maken heeft met aanbestedingen, kunnen de volgende items een plek krijgen:

Standopname per item per afdeling	**Status**
2.1: ICO-wizard aanpak is ingevoerd voor de afdeling bij nieuw aanbestedingen	Percentage waarin dit het geval is
2.2: ICO-herijking verloopt bij deze afdeling volgens plan	Voortgang t.o.v. plan
2.3: De afdeling heeft haar input geleverd voor het overzicht van alle ICT contracten met vermelding van wel/niet ICO benut	Wel/niet gerealiseerd

4.3 Driver 3: Zorg dat wat veilig is, ook veilig blijft

Te beantwoorden vragen	**Kritische Proces Indicatoren (KPI's)**
Nemen mijn restrisico's door technische schuld af in de tijd? **Uitleg: Technische schuld = kosten van wegwerken verouderde hard/software die informatieveiligheid in de weg staat**	Patchmanagement is op orde. Technische schuld van informatiesystemen die de dienstverlening ondersteunen wordt planmatig weggewerkt. Websites en mail voldoen aan veilige internetstandaarden. 1. Veiligheidspatches worden aantoonbaar tijdig aangebracht. (Tijdig is: passend bij de ernst van de dreiging en kans van misbruik en overeenkomstig advies van de betreffende leverancier/CERT). 2. Voor web en mail wordt voldaan aan de standaards van de Pas-toe-of-leg-uitlijst van Forum Standaardisatie: streefscore internet.nl: 100%. 3. Voor elke kroonjuweel is de Technische Schuld berekening uitgevoerd en geaccordeerd door Management incl. afbouwplan. 4. Technische schuld neemt af conform planning.

De technische schuld staat hier voor verouderende soft- en hardware en de toenemende risico's dat kwetsbaarheden daarin door hackers of andere actoren worden benut. Op korte termijn is tijdig aanbrengen van patches essentieel. Dat is echter niet voldoende. Web en mail moeten aan de door Forum Standaardisatie voorgeschreven standaarden te voldoen. Ook voor alle andere (toprisico) domeinen moeten de mogelijkheden en kosten om zwakke plekken uit de weg te ruimen bekend zijn. De aanpak van die zwakke plekken kan dan stapsgewijs worden doorgevoerd.

De standopname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Standopname per item organisatie-breed	**Status**
3.1: Patches alle tijdig aangebracht	Schatting % gerealiseerd
3.2: Voor alle mail- en webtoepassingen wordt voor 100% aan de eisen van Forum Standaardisatie voldaan	% waarin dit het geval is
3.3: Technische schuld berekend voor alle kroonjuwelen	Wel/niet en schatting kosten
3.4: Technische schuld neemt af conform planning	Voortgang ten opzichte van plan

Toelichting: Een opgestelde en afgestemde lijst van toprisico applicaties of systeemdomeinen (zie 3.3a en3.3b hierboven) is niet alleen voor deze driver zeer gewenst. Ook bij andere drivers kun je ervoor kiezen om deze lijst te benutten voor een juiste risico-gebaseerde prioritering.

In de standopname per afdeling kunnen gelijksoortige items een plek krijgen:

Standopname per item per afdeling	**Status**
3.1: Patches alle tijdig aangebracht voor systemen van de afdeling	Schatting % gerealiseerd
3.2: Voor alle mail- en webtoepassingen van de afdeling wordt voor 100% aan de eisen van Forum Standaardisatie voldaan	% waarin dit het geval is

3.3: Technische schuld berekend voor alle Ikroonjuwelen van de afdeling	Wel/niet en Schatting omvang financieel
3.4: Technische schuld van de afdeling neemt af conform planning	Voortgang t.o.v. plan

4.4 Driver 4: Werk veilig, ook thuis

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
- Is toegang voldoende afgeschermd? - Worden incidenten adequaat afgehandeld? - Neemt meldingsbereidheid toe? - Neemt ernst van incidenten af?	Toegangsmanagement voldoet aan aangescherpte eisen. Incidenten worden afgehandeld conform BIO vereisten. Meldingsbereidheid neemt aantoonbaar toe. 1. 2FA (2 factor authenticatie) wordt toegepast voor reguliere toegang conform de NCSC-publicaties. 2. Ook bijzondere toegang voor beheer/foutherstel en testen is ingericht conform NCSC-publicaties. 3. Uit een periodiek overzicht van aantallen incidenten, gekwalificeerd naar ernst en periode, blijkt: a. een afname van het aantal ernstige incidenten met x% per kwartaal; b. een toename van efficiëntie van de oplossing van incidenten met y% per kwartaal; c. bij een onverminderde meldingsbereidheid.

Veilig (thuis)werken vereist extra (waakzaamheid bij) maatregelen voor toegangsmanagement. Het zicht op incidenten dreigt te verminderen als er niet extra wordt gelet op het stimuleren van het melden van optredende incidenten en een adequate follow-up daarop.

De standopname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Standopname per item organisatie-breed	Status
4.1: 2FA (2 factor authenticatie) is organisatie-breed doorgevoerd conform NCSC adviezen	Schatting % gerealiseerd
4.2a: Bijzondere toegang voor beheer/foutherstel/testen is **voor kroonjuwel**en ingericht volgens aangescherpte voorschriften	Schatting % gerealiseerd
4.2b: Bijzondere toegang voor beheer/foutherstel/testen is voor **alle** domeinen ingericht volgens aangescherpte voorschriften	Schatting % gerealiseerd
4.3a: Voor kroonjuwelen is er een inzichtelijk overzicht m.b.t. optreden en melden van incidenten en het effectief afhandelen ervan	Wel/niet gerealiseerd
4.3b: Voor **kroonjuwelen** blijkt uit rapportages een goede status van de incidentafhandeling	Schatting % gerealiseerd
4.3c: Voor **alle kroonjuwelen** blijkt uit rapportages een goede status van de incidentafhandeling	Schatting % gerealiseerd

In de standopname per afdeling kunnen gelijksoortige items een plek krijgen:

Standopname per item per afdeling	Status
4.1: 2FA (2 factor authenticatie) is voor deze afdeling doorgevoerd conform NCSC-adviezen	Schatting % gerealiseerd
4.2a: Bijzondere toegang voor beheer/foutherstel/testen is voor kroonjuwelen van deze afdeling ingericht volgens aangescherpte voorschriften	Schatting % gerealiseerd
4.2b: Bijzondere toegang voor beheer/foutherstel/testen is voor alle domeinen van deze afdeling ingericht volgens aangescherpte voorschriften	Schatting % gerealiseerd
4.3a: Voor kroonjuwelen van deze afdeling is er een inzichtelijk overzicht m.b.t. optreden en melden van incidenten en het effectief afhandelen ervan	Wel/niet gerealiseerd
4.3b: Voor kroonjuwelen van deze afdeling blijkt uit rapportages een goede status van de incidentafhandeling	Schatting % gerealiseerd
4.3c: Voor alle kroonjuwelen van deze afdeling blijkt uit rapportages een goede status van de incidentafhandeling	Schatting % gerealiseerd

4.5 Driver 5: Afscherming, detectie, monitoring en response

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
- Zijn systeemsegmenten zo aangebracht dat besmetting van laag-risicosegment niet tot besmetting van (een) kroonjuweel(en) leidt? - Worden dreigingen die mogelijk disruptief zijn voor onze dienstverlening of bedrijfsvoering bijtijds gesignaleerd?	Segmentering van systeem-domeinen is zodanig ingericht dat de kans op (malware-)besmettingen van toprisico segmenten sterk is gereduceerd. 1. Een SOC op 7x24 basis is ingericht conform NCSC/IBD/sector CERT adviezen/eisen. 2. CERT-aansluiting 100% operationeel en alle CERT-adviezen worden binnen de gestelde termijnen uitgevoerd. 3. Er is een actueel overzicht van de doorgevoerde segmentering binnen de IV-infrastructuur en een audit op de effectiviteit ervan. 4. Er is een plan voor het oplossen van de manco's in de segmentering van de IV-infrastructuur en dit plan wordt uitgevoerd conform planning.

Adequate afscherming is vereist zowel aan de buitenrand, op de koppelvlakken met het internet en met ketenpartners, maar ook intern tussen toprisico segmenten en mediumrisico segmenten. Op die interne segmentering is laatste jaren steeds meer nadruk komen te liggen. Bij interne segmentering komt het nodige kijken; een aantal overheidsorganisaties hebben de vereiste (eerste) stappen nog niet gezet. Aansluiten op een SOC en een CERT en het opvolgen van hun adviezen zijn no-brainers, vooral als deze voor een sector goed georganiseerd zijn.

De standopname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Standopname per item organisatie-breed	Status
5.1a: SOC aansluiting gereed	J/N
5.1b: SOC adviezen/vereisten 100% opgevolgd	Wel/niet gerealiseerd
5.2a: CERT aansluiting gereed	J/N
5.2b: CERT adviezen/vereisten 100% opgevolgd	Wel/niet gerealiseerd
5.3a: Plan voor segmentering opgesteld en goedgekeurd	Wel/niet gerealiseerd
5,3b: Plan voor segmentering wordt uitgevoerd conform planning	Wel/niet gerealiseerd
5.4: Segmenteringsoverzicht is volledig en goedgekeurd door de auditor	Wel/niet gerealiseerd

In de standopname per afdeling kunnen de volgende items een plek krijgen:

Standopname per item per afdeling	Status
5.1b: SOC adviezen/vereisten 100% opgevolgd voor afdelingsdomein	Wel/niet gerealiseerd
5.2b: CERT adviezen/vereisten 100% opgevolgd voor afdelingsdomein	Wel/niet gerealiseerd
5.3a: Plan voor segmentering opgesteld en goedgekeurd voor afdelingsdomein	J/N
5,3b: Plan voor segmentering voor afdelingsdomein wordt uitgevoerd conform planning	Wel/niet gerealiseerd
5.4: Segmenteringsoverzicht voor afdelingsdomein is volledig en goedgekeurd door de auditor	Wel/niet gerealiseerd

In relatief kleine organisaties is het doorgaans niet handig om apart te sturen op de afscherming per afdeling. In grotere organisaties kan het juist wel handig zijn om (een deel van deze) aanscherpingen eerst uit te voeren bij één of twee afdelingen met een hoog risicoprofiel.

4.6 Driver 6: Effectief handelen bij incidenten en crisissen

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
- Is de crisisorganisatie voldoende geëquipeerd om in te grijpen bij crises door hacks en datadiefstal? - Is recovery te allen tijde mogelijk?	Back-up & Recovery is adequaat geborgd. Het crisisplan is compleet en actueel en wordt periodiek beproefd. 1. Er is een actueel Back-up en Recovery-plan, geaccordeerd door het verantwoordelijk Management. 2. Er is een actueel Business Continuïteit-Management plan, geaccordeerd door het topmanagement. 3. Beide plannen worden minimaal 1 keer per jaar geoefend, waarna actualisaties en leerpunten direct worden verwerkt in de plannen.

De standopname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Standopname per item organisatie-breed	Status
6.1: Er is een actueel back-up en recovery) plan, goedgekeurd door het Management	Wel/niet gerealiseerd
6.2: Er is een actueel Business Continuity Managementplan, dan wel een specifiek Crisis-management-plan plan, goedgekeurd door het Management	Wel/niet gerealiseerd
6.3a: Het Business Continuity Managementplan is afgelopen jaar grondig getest en in orde bevonden	J/N
6.3b: Met dit plan is afgelopen jaar organisatie-breed geoefend	J/N

In de standopname per afdeling kunnen de volgende items een plek krijgen:

Standopname per item per afdeling	Status
6.3a: Het Business Continuity Managementplan is afgelopen jaar grondig getest voor het afdelingsdomein en in orde bevonden	J/N
6.3b: De afdeling heeft goed meegedaan aan de meest recente jaarlijkse Business Continuity oefening.	J/N

4.7 Driver 7: Meet, leer en stuur bij

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
-Is er een cultuur van eigenaarschap en verantwoord gedrag in de organisatie? - Zijn de processen voor de bescherming tegen IB&P-bedreigingen op orde? - Groeien deze processen mee met de toenemende kwetsbaarheden?	Volwassenheid voor zowel IB als P is op minimaal vereiste niveau en neemt jaarlijks toe conform afspraken. Feitelijk gedrag wordt regelmatig getest en uitkomsten daarvan zijn conform afspraken. 1. IB-volwassenheid is minstens niveau 3 op schaal 1-5 van de BIO-Self assessment en groei ervan is conform afspraken; 2. P-volwassenheid is minstens niveau 3 op schaal 1-5 van de Privacy Self assessment en groei ervan is conform afspraken; 3. Gedragstoetsing in vormen als phishing-acties en red-teaming vinden regelmatig plaats; de leerpunten worden gebruikt voor: a. het dichten van de gaten in de veiligheid van processen en systemen; b. terugkoppeling van confronterende boodschappen ter bevordering van bewustzijn en verantwoord gedrag. 4. Elke ondernomen gedragstoetsing wordt gepresenteerd aan het management met daarin de belangrijkste leerpunten.

Naast het BIO-Selfassessment (BIO-SA) en het Privacy-Selfassessment (PriSA) zijn er ook andere self-Assessments, zoals het NBA-model van NOREA. Voor gemeenten biedt ENSIA ook mogelijkheden voor volwassenheidsmeting. Elke organisatie kan hier zelf een keuze maken.

NB: Veel organisaties hebben al een ISMS-pakket dat doorgaans veel vragen bevat die overeenkomen vragen in de self-assessments. Zo'n ISMS kan dan ook als basis voor deze driver worden benut.

De standopname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Standopname per item organisatie-breed	Status
7.1a: IB-selfassessment is organisatie-breed ingevuld en gemiddelde score is 3 of hoger	Gerealiseerde score
7.1b: Gemiddelde groei in IB-volwassenheid t.o.v. meting vorig jaar is minstens *<af te spreken niveau>*	Gerealiseerde %-punten groei
7.2a: Privacy-selfassessment is organisatie-breed ingevuld en gemiddelde score is 3 of hoger	Gerealiseerde score
7.2b: Gemiddelde groei in privacy-volwassenheid t.o.v. meting vorig jaar is minstens *<af te spreken niveau>*	Gerealiseerde %-punten groei
7.3a: Er is organisatie-breed real-life geoefend met detecteren & dichten IB&P gaten	Wel/niet gerealiseerd
7.3b: Er is organisatie-breed real-life geoefend met verantwoord gedrag	Wel/niet gerealiseerd
7.4: Er zijn rapporten van beide typen real-life oefeningen opgeleverd met duidelijke leerpunten	Wel/niet gerealiseerd

In de standopname per afdeling kunnen gelijksoortige items een plek krijgen:

Standopname per item per afdeling	Status
7.1a: IB-Selfassessment is organisatie-breed ingevuld en gemiddelde score is 3 of hoger	Gerealiseerde score
7.1b: Gemiddelde groei in IB-volwassenheid t.o.v. meting vorig jaar is minstens *<af te spreken niveau>*	Gerealiseerde %-punten groei
7.2a: Privacy- Selfassessment is organisatie-breed ingevuld en gemiddelde score is 3 of hoger	Gerealiseerde score
7.2b: Gemiddelde groei in privacy-volwassenheid t.o.v. meting vorig jaar is minstens *<af te spreken niveau>*	Gerealiseerde %-punten groei
7.3a: Er is organisatie-breed real-life geoefend met detecteren&dichten IB&P gaten	Wel/niet gerealiseerd
7.3b: Er is organisatie-breed real-life geoefend met verantwoord gedrag	Wel/niet gerealiseerd
7.4: Er zijn rapporten van beide typen real-life oefeningen opgeleverd met duidelijke leerpunten	Wel/niet gerealiseerd

Bijlage: Voorbeeld opdrachtbrief KPI-aanpak op basis van de 7 drivers

Beste *naam-CISO*,

Op *datum-eerste-gesprek* hebben we samen afgesproken om de sturing van informatiebeveiliging voor onze organisatie te verbeteren.

In dat eerste gesprek hebben we de KPI-vragen op basis van de 7-drivers samen doorgenomen. Naderhand heb je het besprokene omgezet naar een statusoverzicht. Deze vind je als bijlage bij deze brief.

Ik geef je opdracht om dit statusoverzicht om te zetten naar een dashboard dat organisatiebreed wordt bijgehouden. Dit dashboard zal elk kwartaal met de deelnemende afdelings-MT's worden doorgenomen. Ikzelf zal dit dashboard in samenspraak met jou elk kwartaal met het directieteam doornemen. In de kwartaalgesprekken vormt feedback op de noodzakelijke betere sturing als vast punt.

In onderstaande lijst heb ik de namen opgenomen van een aantal collega's. Ik geef hun opdracht om het komende jaar voldoende tijd vrij te maken voor het realiseren en bijhouden van dit KPI dashboard voor alle afdelingen *(alternatief: benoem enkele, tenminste 3, afdelingen die het eerste jaar de spits afbijten)* inclusief een samengevoegd dashboard voor de hele organisatie als geheel.

naam	**Functie**

In de loop van de komende maanden kunnen extra namen aan deze lijst worden toegevoegd; zo nodig na afstemming met ondergetekende.

Ik wens je succes en zal zorgen dat ik zelf ook beschikbaar ben mocht dat nodig zijn voor nadere tussentijdse afstemming,

Met vriendelijke groet,

Naam-bestuurder

Bijlage: concept statusoverzicht van de KPI's