centrum informatiebeveiliging en privacybescherming

Handreiking Sturing Informatieveiligheid en Privacy

BIO 7-driver KPI's

December 2021 [versie 1.0]

Titel	Handreiking Sturing Informatieveiligheid en Privacy
Datum	December 2021
Status	Versie 1.0
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	Maarten Baljon, Ad Reuijl
Reviewers	CIP kernteam

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

1.1 Leeswijzer

Deze handreiking biedt een beschrijving van het 7-driver KPI-model. Dit is een initiatief om Informatie Veiligheid en Privacy in overheidsorganisaties echt tot Chefsache (zaak voor persoonlijke bemoeienis van de baas) te maken:

In hoofdstukken 1 t/m 3, ofwel t/m pagina 12, staat de kern beschreven. Dit deel is bedoeld voor Bestuurders, leden afdeling MT's, IB&P staf en alle andere betrokkenen.

- In 1.2 t/m 1.5 wordt de positionering t.o.v. de BIO toegelicht met een voorbeeld erbij.
- Hoofdstuk 2 toont een schema van de jaarcyclus dat in 2.1 t/m 2.6 nader wordt toegelicht.
- In hoofdstuk 3 staan de vragen die in en jaargesprek met de Bestuurder en de afdeling MT's aan bod kunnen komen.

Hoofdstuk 4 beschrijft nadere details voor CISO's en andere vakinhoudelijk betrokkenen:

- Er worden suggesties gedaan voor de omzetting van vragenlijst-items uit hoofdstuk 3 naar 7-driver dashboard items.

1.2 Positionering 7-driver KPI's t.o.v. de BIO

Het belang van weerbaarheid van organisaties tegen dreigingen van cybercriminaliteit wordt breed onderkend. Vanuit dit bewustzijn heeft de Nederlandse overheid sinds 2020 een gemeenschappelijk kader aangenomen voor een basis-veiligheidsniveau: de BIO (Baseline Informatiebeveiliging Overheid). Risicoanalyse vormt de basis voor het treffen en prioriteren van de generieke maatregelen uit de BIO. Dat is de eerste stap. De tweede stap betreft het doorvoeren van specifieke maatregelen op basis van de risicoafwegingen in de eerste stap en de sturing daarop.

Lijnmanagement dient bij beide stappen goed betrokken en verantwoordelijk te zijn. In de praktijk blijkt het echter heel lastig om dat spel goed op de wagen te krijgen. Al snel gaat het gesprek, vooral bij stap 2, over diep-technische details van de maatregelen en haakt de verantwoordelijke bestuurder af. Daarmee wordt sturing op informatieveiligheid in veel organisaties het exclusieve terrein van de CISO en zijn team.

Tegelijkertijd spreekt men naar elkaar uit dat informatieveiligheid Chefsache is, een zaak voor de baas. Er valt dus een stevig gat te dichten tussen de wenssituatie, dat bestuur/directie echt betrokken is bij de sturing op informatieveiligheid, en de realiteit van bestuurders en managers die afhaken vanwege een veelheid aan detailmaatregelen. Vandaar dat we aan de slag zijn gegaan met de vraag: 'Hoe kun je op organisatieniveau wel echt sturen op informatieveiligheid? Welke handvatten zijn daarvoor vereist?'

In essentie gaat het daarbij om het verbinden van de wereld van bestuurder/directie aan die van de CISO en IB&P professionals. Na een reeks van gesprekken met verantwoordelijken in 12 organisaties zijn we uitgekomen op een eenvoudige opzet. Door het stellen van vragen wordt de bestuurder/directie geholpen om zijn verantwoordelijkheid concreet in de vullen en effectief te sturen naar verbetering. De opzet helpt tevens de CISO aan passende taal om over doelen en middelen met bestuurder/directie in gesprek te gaan en te blijven.

Gezien de verschillen tussen de organisaties wat betreft doelstellingen, risicoappreciatie en de mate waarin al bewust op onderdelen wordt gestuurd, biedt de 7-driver aanpak de ruimte om het met eigen accenten toe te gaan passen. De 7 hoofdonderwerpen zijn voor iedereen herkenbaar, maar elke organisatie zal een eigen afweging maken welke daarvan de prioriteit krijgen. Wat hieronder als voorbeeld wordt geschetst is uitdrukkelijk niet meer dan een denkbeeldige optie.

1.3 Korte weergave van de 7 drivers

Een korte impressie van de 7 drivers:

1. Risico's: Bepaal top-risico's en de daarvoor meest relevante extra maatregelen.
2. Inkoop: Breng leverancier- en andere ketenafspraken in lijn met BIO en aanvullende kaders.
   Benut de ICO wizard om dit te borgen.
3. Bijwerken: Breng security wijzigingen tijdig aan. Vervang oude software tijdig.
4. Veilig thuiswerken: Pas 2-factor authenticatie consequent toe.
   Stel hoge(re) eisen aan bijzondere toegang (beheer/testen met name).
5. Afscherming: Regel CERT- en SOC diensten.
   Bescherm top-risico applicaties tegen domino-effecten door segmentatie.
6. Crisismanagement: Heb waterdichte herstel-aanpak voor top-risico applicaties.
   Oefen regelmatig Cyber Crisismanagement.
7. Maturiteit: Meet kwaliteit Security-processen middels self-assesments (BIO-SA, PriSA).
   Houd medewerkers scherp op feitelijk security-gedrag middels bijv. red-teaming.

1.4 Aanbeveling tot fasegewijs invlechten

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

- Kies jaarlijks 3 maatregelen uit de 7-driver-set.
- Rapporteer daarover 3 maandelijks en bespreek dat in MT-overleggen.
- Continueer rapportages in volgende jaren, dus elk jaar 3 dashboard items erbij.

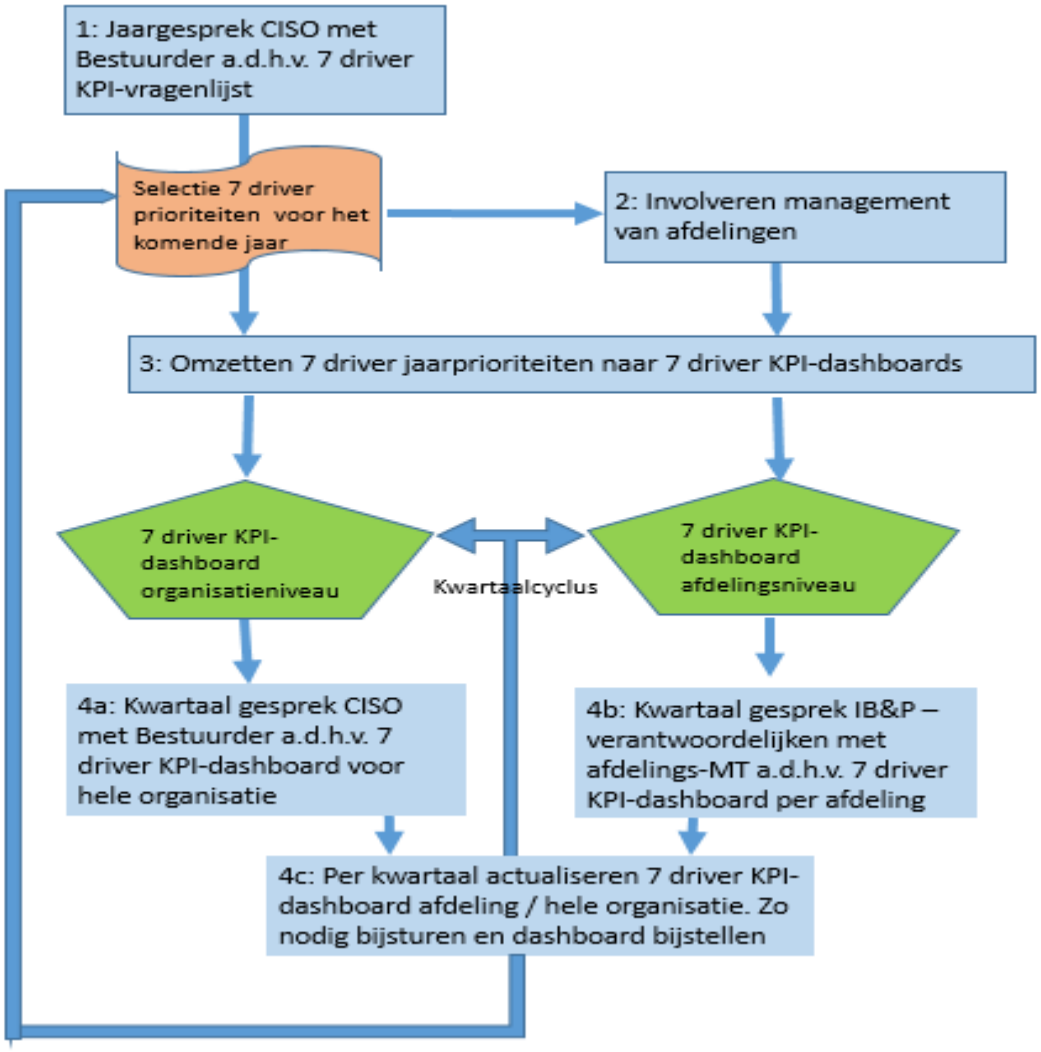
1.5 Een voorbeeld van fasegewijs invlechten

Hieronder een voorbeeld van fasegewijs invlechten:

Dashboard in jaar 1:	In jaar 2:	In jaar 3:
• Waterdicht herstel top-risico's • ICO bij nieuwe contracten en ketenafspraken • SOC diensten inregelen	• 2 factor authenticatie • Plaats top-risico applicaties in aparte segmenten/Zero Trust • Waterdicht herstel top-risico's • ICO bij nieuwe contracten en ketenafspraken • SOC diensten inregelen	• Maturiteit meten & versterken (Selfassesments/ red teaming) • Vervangen oude software • ICO ook voor herijking bestaande ketenafspraken • 2 factor authenticatie • Plaats top-risico applicaties in aparte segmenten/Zero Trust • Waterdicht herstel top-risico's • ICO bij nieuwe contracten en ketenafspraken • SOC diensten inregelen

2 Jaarcyclus 7-driver KPI's

De 7-driver KPI's dienen hun plek krijgen in een jaarcyclus: Hieronder een schets daarvan:



2.1 Toelichting

Het kan elke organisatie gebeuren dat op maandagochtend de gegevensverwerking gehackt blijkt te zijn. Als de Media eind van de maandagochtend (zeer bijtijds want ze zijn getipt door de hackers) contact zoeken met de Bestuurder, is zijn/haar reactie dan:

- Voor security heb ik mijn mensen: een prima team!;
- Zij hebben me herhaaldelijk verzekerd dat we in control zijn;
- Deze hack is de uitzondering: het blijft mensenwerk!;
- Aan het herstel wordt, as we speak, hard gewerkt;
- Nadere info kan ik nu niet geven, later deze week zal meer bekend zijn, is mij verzekerd!

of meer als volgt:

- Voor security heeft onze organisatie een gedegen aanpak;
- Risico's zijn in kaart gebracht, ook die van een hack zoals deze;
- Bij deze aanpak zijn de meest gevoelige gegevens/dienstverlening extra afgeschermd. Deze zijn nu daardoor gelukkig ook buiten schot gebleven;
- Door onze back-up aanpak zijn we, ook na deze hack, binnen 6 uur weer up en running.

De 7-driver aanpak heeft als doel dat de tweede, de blauwe, reactie zal kunnen worden gegeven en dat deze ook klopt. Als je er 100% zeker van bent dat je organisatie en je Bestuurder nu al de blauwe reactie zullen kunnen geven, dan kan je dit 7-driver verhaal verder ongelezen terzijde schuiven.

Heb je besloten toch verder te lezen vat dan moed: Incidenten met een majeure IB&P impact zijn van alledag en met een goede sturing en een gedegen aanpak zoals in dit document beschreven, zijn de kansen op een onvoorspelbare en slechte afloop tot een aanvaardbaar laag niveau terug te brengen.
Wanneer je organisatie onderstaande 7-driver aanpak volgt, kun je als Bestuurder ervan op aan dat er binnen een jaar tijd al sprake zal zijn van een sterk verbeterde situatie. Ook na dit eerste jaar zal je organisatie verdere verbeteringen door moeten blijven voeren. Ook dit continue verbeterproces maakt onderdeel uit van de beschreven aanpak.

De jaarcyclus bestaat uit 4 stappen (samengevat in het jaarcyclus-schema op de vorige bladzij).

2.2 Stap 1: (Jaar-)Gesprek met Bestuurder

Vraag als CISO een gesprek aan met je Bestuurder. Onderwerp is de 7-driver KPI-vragenlijst. Het gesprek kent de volgende deelstappen:

1. Vraag als intro wat de grootste zorgen zijn van de bestuurder op IB&P-vlak.
2. Loop met de bestuurder de 7-driver KPI-vragenlijst langs (zie 2 pagina's verderop).
3. Noteer per driver welke van de vragen bij de bestuurder leven.
4. Verwerk de gegeven antwoorden tot een 7-driver KPI-jaarprioriteitenoverzicht. In Hoofdstuk 4 is beschreven hoe je deze kunt opstellen.
   Het kan handig zijn om voorafgaand aan het gesprek voor je zelf al een concept-KPI-jaarprioriteitenoverzicht op te stellen en dat dan tijdens of na het gesprek bij te punten.
5. Formuleer een kort en bondig gespreksverslag en deel deze met je Bestuurder.

6. Stel gelijktijdig of als eerstvolgende vervolgstap een opdrachtbrief op (Bijlage 1) om de afdeling-MT's te involveren. Deze brief benadrukt de Bestuurder het belang om het 7-driver jaarprioriteitenoverzicht/dashboard elk kwartaal bij te werken en deze met zowel de Bestuurder als met de afdeling-MT's te bespreken. Middels de opdrachtbrief reserveer je voldoende tijd en aandacht bij de leden van de afdeling-MT's en ook bij de IB&P stafmedewerkers van elke afdeling. Tevens reserveer je ruimte voor omzetting naar een KPI-dashboard. Zie ook bij stap 3 hieronder.

2.3 Stap 2: Involveren afdelingsmanagement

Nu is het zaak afdelings MT's er bij te betrekken. Dat kan middels de volgende deelstappen:

1. Informeer de in de Opdrachtbrief vermelde direct betrokkenen over de goedkeuring van de nieuwe 7-driver KPI-jaarcyclus door de Bestuurder. Het gaat met name om leden van afdeling-MT's en IB&P-stafmedewerkers op de afdelingen.
2. Informeer ze middels verspreiding van het concept 7-driver jaarprioriteitenoverzicht plus een link naar deze jaarcyclus aanpak.
3. Maak afspraken in de agenda's om deze met iedereen individueel of in groepjes door te nemen en om verbetersuggesties te ontvangen en te bespreken.

2.4 Stap 3: Omzetten 7-driver jaarprioriteiten-overzicht naar 7-driver KPI-dashboard

Nu gaan we de beantwoorde vragen omzetten naar een meer aansprekend dashboard:.

1. Bespreek met een Excel-expert of met je GRC tool leverancier hoe het afgestemde 7-driver 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.
2. Neem, zodra de leverancier dit heeft ingericht, het KPI-status update proces 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.

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

1. Zorg per kwartaal voor een bespreking in het MT van elke afdeling van de KPI-status van de afdeling. De IB&P stafmedewerker van de afdeling neemt dan het KPI-dashboard met het voltallige afdelings-MT door.
2. Bespreek de voor de hele organisatie gecombineerde 7-driver KPI-status met de Bestuurder.
3. Bespreek naast de status ook elk kwartaal mogelijk gewenste verbeteringen/uitbreidingen met je Bestuurder. Ook in de afdeling MT's wordt dat aangemoedigd.
4. Informeer je team(s) over de uitkomsten van de kwartaalgesprekken en bespreek met hen de mogelijkheden om de gewenste verbeteringen/uitbreidingen te effectueren. Als dat een Yes-we-can reactie oplevert, breng die wijziging dan aan. Op die manier heb je een continu verbeter aanpak te pakken met een driemaandelijkse heart-beat.

2.6 Jaarcyclus

In de beschrijving hierboven wordt vooral beschreven hoe de stappen in het eerste jaar kunnen worden doorlopen. Dat eerste jaar zal spannend zijn omdat het voorziene proces nieuw is en de nodige weerstand daartegen dient te worden omgezet naar nieuwe energie.

Na dit eerste jaar blijft het spannend met vooral als uitdaging om de aandacht blijvend vast te houden. Jaarlijks bijstellen van de prioriteiten en het levend houden van het besef van de urgentie zijn daarbij belangrijke ingrediënten. Blijvend support van de Bestuurder(s) is daarbij cruciaal.

3 De 7-driver KPI vragenlijst

Onderstaande vragenlijst is bedoeld als leidraad voor het gesprek over Informatieveiligheid en Privacy bescherming tussen de Bestuurder/Directeur/Businessverantwoordelijke en de CISO. Geordend naar een 7-tal onderwerpen zijn concrete, activerende vragen geformuleerd. De kritische procesindicatoren zijn suggesties om de vragen te vertalen in meetbare acties en resultaten. Een periodiek gesprek langs de as van deze vragen en de rapportage over de mate waarin de KPI's worden gerealiseerd, kan de bestuurder helpen zijn rol te pakken. De alom onderschreven slogan 'Informatieveiligheid is Chefsache' wordt daarmee een feit.

Het gesprek is niet alleen nodig op bestuursniveau maar ook op het niveau van de afdeling-MT's c.q. de lijnverantwoordelijken in de organisatie.

Het is aan de gesprekspartners om, op basis van risicoafwegingen, zelf te bepalen welke van onderstaande onderwerpen met prioriteit ter hand worden genomen.

IB&P driver	3-deling	Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
1 IB&P risico's	Weerbaar-heid	Wat zijn top-risico's en zijn de juiste maatregelen getroffen voor de mitigatie ervan?	Top-risico's afgestemd, auditplan wordt uitgevoerd volgens planning. Lijst met top-risico's beschikbaar en besproken met Bestuurder. 1. Per top-risico een overzicht van mitigerende maatregelen; 2. Er is een auditplan afgestemd met daarin minimaal een audit van derde partij op alle top-risico-maatregelen; 3. Verslag Bestuurder-CISO met vastlegging van deze bespreking.
2 IB&P-uitbesteding	Weerbaar-heid	Zijn de uitbestedingen onderworpen aan eisen om feitelijke veiligheid en privacybescherming te borgen?	Aanbestedingen, inkopen en 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 en inkopen 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.

IB&P driver	3-deling	Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
3 IB&P-technische schuld	Weerbaar-heid	Nemen mijn restrisico's t.g.v. technische schuld af in de tijd? Uitleg: Technische schuld = kosten van wegwerken verouderde soft-/hardware met nadelige IB&P-impact	Patchmanagement is op orde. Technische schuld van informatiesystemen die de dienstverlening ondersteunen wordt planmatig weggewerkt. Websites en mail voldoen aan veilige internet standaarden. 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 standaards van de Pas-Toe-of-Leg-Uitlijst van Forum voor Standaardisatie: streefscore internet.nl: 100%; 3. Een lijst met alle applicaties/applicatie-omgevingen die gerelateerd zijn aan de top-risico's is met Management afgestemd; 4. Voor elk van deze top-risico applicaties/applicatie-omgevingen is de technische schuld berekening uitgevoerd en geaccordeerd door Management incl. afbouwplan. 5. Technische schuld neemt af conform planning.
			6.
4 Veilig (thuis)werken	Weerbaar-heid	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 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 en signalering	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 systeem-domeinen is zodanig ingericht dat de kans op (malware-)besmettingen van top-risico-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 robuustheid daarvan; 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.

IB&P driver	3-deling	Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
6 Crisis-management	Herstel	Is de crisisorganisatie voldoende geëquipeerd om in te grijpen bij crises tgv 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 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.
7 IB&P-maturiteit	Leren	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?	Maturiteit 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-maturiteit is minstens niveau 3 op schaal 1-5 van de BIO-Self assessment en groei ervan is conform afspraken; 2. P-maturiteit 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.

4 Omzetting van de 7-driver jaarprioriteiten naar KPI's

Over de omzetting naar KPI's het volgende:

- 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.
- Het hoeft zeker geen apart dashboard te zijn, het kan ook een toevoeging zijn aan een reeds bestaand dashboard.
- Op het dashboard zullen vaak meetwaarden worden getoond. Dat kan ook ja/nee antwoorden op vragen betreffen. Soms zal/kan er voor worden gekozen om ook nadere details te tonen op onderliggende schermen. Dat kan bijvoorbeeld toelichting betreffen op meetwaardes op het eerste scherm, het 'primaire dashboard'.
- Dit hoofdstuk is vrij gedetailleerd en is vooral bedoeld voor de CISO en andere IB&P stafleden.
- Om noodzaak tot terugbladeren te beperken worden steeds, per driver, de te beantwoorden vragen uit het vorige hoofdstuk opnieuw weergegeven.

4.1 Driver 1: IB&P risico's

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
Wat zijn top-risico's en zijn de juiste maatregelen getroffen voor de mitigatie ervan?	Top-risico's afgestemd, auditplan wordt uitgevoerd volgens planning. Lijst met top-risico's beschikbaar en besproken met bestuurder. 1. Per top-risico een overzicht van mitigerende maatregelen; 2. Er is een auditplan afgestemd met daarin minimaal een audit van derde partij op alle top-risico-maatregelen; 3. Verslag Bestuurder-CISO met vastlegging van deze bespreking.

Lijst van top-risico's kan bijvoorbeeld als volgt luiden:
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

Oorzakelijke risico's:
5. Chantage m.b.v. ransomware
6. Medewerkers gedragen zich onzorgvuldig m.b.t. IB&P 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 aan de weet te komen welke risico's voor jouw organisatie het meest van belang zijn in de beleving van de Bestuurder (en van afdeling MT-leden). Als ze toch aandringen op enkele suggesties van jouw kant dan kan het ook handig zijn om de auditverslagen erop na te slaan: Welke risico's worden daarin benoemd?

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 stand-opname voordat de organisatie de KPI-sturing oppakt: Bij de drivers 2 t/m 7 worden diverse mitigerende maatregelen gesuggereerd. Die zullen zeker in de beginfase niet geheel overeenkomen met mitigerende 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 afgelopen twee jaren, met daarbij per audit de majeure bevindingen/adviezen en vermelding of deze zijn opgevolgd;

2. Overzicht met de geplande audits, met daarbij vermeld zowel de bevindingen van de voorgaande audit van deze auditor/van dit type audit als ook van de top-risico's waarvoor de audit relevant is.

De stand-opname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Stand-opname per item organisatie-breed	Status
1.1: Lijst top-risico's	Mate waarin dit al in beeld is
1.2: Overzicht mitigerende maatregelen per top-risico	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 mitigerende maatregelen worden aangegeven. In de stand-opname per afdeling kunnen de volgende items een plek krijgen:

Stand-opname per item per afdeling	Status
1.1: Lijst top-risico's	Mate waarin dit al in beeld is
1.2: Overzicht mitigerende maatregelen per top-risico	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. Werkt heel goed voor het draagvlak en kan ivoren-toren-effecten helpen voorkomen.

4.2 Driver 2: IB&P uitbesteding

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
Zijn de uitbestedingen onderworpen aan eisen om feitelijke veiligheid en privacybescherming te borgen?	Aanbestedingen, inkopen en 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) en wordt aanbevolen door de ministeries van BZK en EZK voor overheid-breed gebruik om eisen te IB&P-eisenpakketten samen te stellen als bijlagen bij aanbestedingen en contracten. Het gebruik is ook mogelijk in relaties met interne ontwikkelafdelingen en met shared service centra.

De stand-opname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Stand-opname 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 of dit het geval is
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 stand-opname per afdeling die te maken heeft met aanbestedingen, kunnen de volgende items een plek krijgen:

Stand-opname 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: IB&P technische schuld

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
Nemen mijn restrisico's t.g.v. technische schuld af in de tijd? Uitleg: Technische schuld = kosten van wegwerken verouderde soft-/hardware met nadelige IB&P-impact	Patchmanagement is op orde. Technische Schuld van informatiesystemen die de dienstverlening ondersteunen wordt planmatig weggewerkt. Websites en mail voldoen aan veilige internet standaarden. 1. Veiligheidspatches worden aantoonbaar tijdig aangebracht. (Tijdig is: passend bij de ernst van de dreiging en kans van misbruik en overeenkomstig advies van de betr. leverancier/CERT). 2. Voor web en mail wordt voldaan aan de standaards van de Pas-toe-of-leg-uitlijst van Forum voor Standaardisatie: streefscore internet.nl: 100%. 3. Een lijst met alle applicaties/applicatie-omgevingen die gerelateerd zijn aan de top-risico's is met Management afgestemd. 4. Voor elk van deze Top-risico applicaties/applicatie-omgevingen is de Technische Schuld berekening uitgevoerd en geaccordeerd door Management incl. afbouwplan. 5. Technische Schuld neemt af conform planning.

IB&P Technische Schuld staat voor verouderende soft- en hardware en de toenemende risico's dat deze door hackers of andere actoren worden uitgenut. Op korte termijn is tijdig aanbrengen van patches essentieel. Dat volstaat allerminst. Web en mail dienen per se aan de door Forum voor Standaardisatie (FvS) voorgeschreven standaards te voldoen. Ook voor alle andere (top-risico) domeinen dienen mogelijkheden en kosten om zwakke-IB&P- plekken uit de weg te ruimen bekend te zijn als vertrekpunt om dit stapsgewijs door te voeren.

De stand-opname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Stand-opname per item organisatie-breed	Status
3.1: Patches alle tijdig aangebracht	Schatting % gerealiseerd
3.2: Voor alle mail en web toepassingen wordt voor 100% aan FvS eis voldaan	% waarin dit het geval is
3.3a: Een lijst van top-risico domeinen is opgesteld	Wel/niet gerealiseerd
3.3b: De lijst van top-risico domeinen is afgestemd met mgt	Wel/niet gerealiseerd
3.4: Technische Schuld berekend voor alle top-risico domeinen	Wel/niet en Schatting omvang financieel
3.5: Technische schuld neemt af conform planning	Voortgang t.o.v. plan

Toelichting: De lijst van top-risico applicaties c.q. systeemdomeinen (zie 3.3a en3.3b hierboven) is niet alleen voor deze Driver zeer gewenst om deze opgesteld en afgestemd te hebben. Bij andere drivers kan er ook voor gekozen worden om deze lijst te benutten voor een juiste, risico-gebaseerde, prioritering.

In de stand-opname per afdeling kunnen gelijksoortige items een plek krijgen:

Stand-opname per item per afdeling	Status
3.1: Patches alle tijdig aangebracht voor systemen van de afdeling	Schatting % gerealiseerd
3.2: Voor alle mail en web toepassingen van de afdeling wordt voor 100% aan FvS eisen voldaan	% waarin dit het geval is
3.3a: Een lijst van top-risico domeinen van de afdeling is opgesteld	Wel/niet gerealiseerd
3.3b: De lijst van top-risico domeinen van de afdeling is afgestemd met mgt.	Wel/niet gerealiseerd
3.4: Technische Schuld berekend voor alle top-risico domeinen van de afdeling	Wel/niet en Schatting omvang financieel
3.5: Technische schuld van de afdeling neemt af conform planning	Voortgang t.o.v. plan

4.4 Driver 4: Veilig (thuis)werken

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 Toegang management. Ook dreigt er minder zicht op incidenten als er niet extra wordt opgelet op een adequate follow-up van gemelde incidenten en op het stimuleren van het melden van optredende incidenten.

De stand-opname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Stand-opname 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 top-risico**-domeinen 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 toprisico domeinen is er een inzichtelijk overzicht m.b.t. optreden en melden van incidenten en het effectief afhandelen ervan	Wel/niet gerealiseerd
4.3b: Voor **toprisico domeinen** blijkt uit rapportages een goede status van de incidentafhandeling	Schatting % gerealiseerd
4.3c: Voor **alle domeinen** blijkt uit rapportages een goede status van de incidentafhandeling	Schatting % gerealiseerd

In de stand-opname per afdeling kunnen gelijksoortige items een plek krijgen:

Stand-opname 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 top-risico-domeinen 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 toprisico domeinen 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 toprisico domeinen van deze afdeling blijkt uit rapportages een goede status van de incidentafhandeling	Schatting % gerealiseerd
4.3c: Voor alle domeinen van deze afdeling blijkt uit rapportages een goede status van de incidentafhandeling	Schatting % gerealiseerd

4.5 Driver 5: Afscherming en signalering

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
Zijn systeemsegmenten zo aangebracht dat besmetting van laag-risico-domeinen niet tot besmetting van Top-risico-domein 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 top-risico-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 Internet en met ketenpartners maar ook intern tussen top-risico-segmenten en medium-risico segmenten. Op die interne segmentering is laatste jaren steeds meer nadruk komen te liggen. Bij interne segmentering komt het nodige kijken en 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 stand-opname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Stand-opname per item organisatie-breed	Status
5.1a: SOC aansluiting gereed	J/N of dit het geval is
5.1b: SOC adviezen/vereisten 100% opgevolgd	Wel/niet gerealiseerd
5.2a: CERT aansluiting gereed	J/N of dit het geval is
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 stand-opname per afdeling kunnen de volgende items een plek krijgen:

Stand-opname 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 of dit het geval is
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 zal het doorgaans niet handig zijn 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 een of twee afdelingen met een hoog risicoprofiel.

4.6 Driver 6: Crisismanagement

Te beantwoorden vragen	Kritische Proces Indicatoren (KPI's)
Is de crisisorganisatie voldoende geëquipeerd om in te grijpen bij Crises tgv 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 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 stand-opname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Stand-opname 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 Management plan, dan wel een specifiek Crisis-management-plan plan, goedgekeurd door het Management	Wel/niet gerealiseerd
6.3a: Het Business Continuity Management plan is afgelopen jaar grondig getest en in orde bevonden	J/N of dit het geval is
6.3b: Met dit plan is afgelopen jaar organisatie-breed geoefend	J/N of dit het geval is

In de stand-opname per afdeling kunnen de volgende items een plek krijgen:

Stand-opname per item per afdeling	Status
6.3a: Business Continuity Management plan is afgelopen jaar grondig getest voor het afdelingsdomein en in orde bevonden	J/N of dit het geval is
6.3b: Afdeling heeft goed meegedaan aan de meest recente jaarlijkse Business Continuity oefening.	J/N of dit het geval is

4.7 Driver 7: IB&P maturiteit

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?	Maturiteit 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-maturiteit is minstens niveau 3 op schaal 1-5 van de BIO-Self assessment en groei ervan is conform afspraken; 2. P-maturiteit 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 de BIO-Selfassessment (BIO-SA) en de Privacy-Selfassessment (PriSA) zijn er ook andere Self-Assessments, zoals het NBA-model van NOREA. En in de gemeentesector zal ENSIA ook mogelijkheden bieden tot volwassenheidsmeting. Elke organisatie kan hier zelf een keuze maken.

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

De stand-opname voor deze driver kan er voor de hele organisatie als volgt uitzien:

Stand-opname 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 stand-opname per afdeling kunnen gelijksoortige items een plek krijgen:

Stand-opname 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 1: Voorbeeld-opdrachtbrief voor 7-driver-KPI-aanpak

Beste *naam-CISO*,

Op *datum-eerste-gesprek* heb ik, in overleg met jou, vastgesteld dat een verbeterde sturing op IB&P vlak voor onze organisatie zeer wenselijk, ja zelfs zeer noodzakelijk is.

In dat eerste gesprek hebben we de KPI-vragen samen doorgenomen. Naderhand heb je het besprokene omgezet naar een 7-driver-status-overzicht. Deze is als bijlage bij deze brief gevoegd.

Ik geef je opdracht om dit statusoverzicht om te zetten naar een dashboard dat organisatiebreed zal worden bijgehouden. *(Variant: Ik geef je opdracht om dit status overzicht toe te voegen aan het dashboard dat organisatiebreed en per afdeling wordt bijgehouden).* Dit dashboard zal elk kwartaal met de deelnemende afdeling-MT's worden doorgenomen. Ik zelf zal dit dashboard in samenspraak met jou elk kwartaal met het voltallige directieteam doornemen. In de kwartaalgesprekken zal feedback op de noodzakelijke betere sturing als vast punt worden besproken.

In onderstaande lijst heb ik de namen opgenomen van een aantal collega's. Ik geef hen opdracht om het komende jaar voldoende tijd vrij te maken voor het realiseren en bijhouden van dit 7-driver-KPI dashboard voor alle afdelingen *(alternatief: benoem enkele, tenminste 3, afdelingen die het eerste jaar de spits gaan afbijten)* inclusief een samengevoegd dashboard voor de hele organisatie als geheel.

naam	**Functie**

In de loop van de komende maanden zullen extra namen aan deze lijst kunnen 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 vr gr,

Naam-bestuurder

Bijlage: concept 7-driver-KPI-status-overzicht