centrum informatiebeveiliging en privacybescherming

De Bestuurder aan zet: sturen op informatieveiligheid

Met 7-drivers die aansluiten op de Baseline Informatiebeveiliging Overheid 2

Januari 2026 [versie 2.0]

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.

© Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons licentie Naamsvermelding-NietCommercieel-GelijkDelen Internationaal (CC BY-NC-SA 4.0) verleend. Voor meer informatie zie: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl.

Titel	Sturen op informatieveiligheid. Met 7-drivers die aansluiten op de Baseline Informatiebeveiliging Overheid 2. Handvatten voor bestuurder, lijn en CISO.
Datum	Januari 2026
Status	Versie 2.0
Auteur	Centrum Informatiebeveiliging en Privacybescherming (CIP)

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt. Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Januari 2026

Inhoud

1. Samenvatting 4

1.1 Leeswijzer 7

2. Inleiding 8

2.1 Informatieveiligheid is chefsache 8

2.2 Samenspel tussen bestuurder, lijn en CISO 9

2.3 Handvatten voor gesprek en sturing 11

2.4 Van een goed gesprek naar effectieve sturing 11

3. Van organisatie tot sturing 12

3.1 Governance en ondersteuning 12

3.2 Jaarcyclus 12

3.3 De opzet van een jaarcyclus: vier concrete stappen 14

Stap 1: gesprek tussen bestuurder en CISO 14

Stap 2: betrek het afdelingsmanagement – zij zijn verantwoordelijk 14

Stap 3: Vertaal het jaarprioriteitenoverzicht in een KPI-dashboard 15

Stap 4: Kwartaalgesprekken met bestuurder(s) en lijn 15

4. De 7-drivers uitgewerkt 17

4.1 Driver 1: De kroonjuwelen beschermen 18

4.2 Driver 2: Kijk verder dan de eigen organisatie 20

4.3 Driver 3: Zorg dat wat veilig is, ook veilig blijft 23

4.4 Driver 4: Identity & Access Management 25

4.5 Driver 5: Afscherming, detectie, monitoring en response 27

4.6 Driver 6: Effectief handelen bij incidenten en crisissen 30

4.7 Driver 7: Meet, leer en stuur bij 32

Bijlage 1: Voorbeeld Opdrachtbrieven aan de CISO en de Lijn 35

1. Samenvatting

Waarom vraagt dit onderwerp nu bestuurlijke aandacht?

Digitalisering maakt onze organisaties steeds afhankelijker van betrouwbare informatiesystemen. Tegelijkertijd worden we daardoor ook kwetsbaarder. De Nederlandse overheid heeft in 2025 een vernieuwd normenkader vastgesteld: de Baseline Informatiebeveiliging Overheid 2 (BIO2). Dit normenkader geldt voor alle overheidsorganisaties en wordt via de Cbw - zodra deze in werking treedt - wettelijk verankerd. Met de komst van de BIO2, de Cyberbeveilingswet (Cbw) en Europese kaders zoals de NIS2-richtlijn, de CER-richtlijn, de Digital Operational Resilience Act (DORA) en de Cyber Resilience Act (CRA) worden organisaties gericht op het:

- Sturen op risico's en weerbaarheid;
- Toezicht houden op maatregelen;
- Besluiten over restrisico's;
- Verantwoording afleggen aan toezichthouders;
- Het vergoten van kennis en bewustzijn.

Informatieveiligheid is chefsache. De vraag is niet óf we geconfronteerd worden met incidenten, maar hoe we de kans erop en de impact ervan zo beperkt mogelijk houden.

Wat bestuurlijke sturing concreet betekent?

Bestuurlijke sturing draait om het geven van richting, maken van keuzes, stellen van prioriteiten en houden van toezicht. De focus ligt niet op de technische details, maar gaat om het dienen van het belang van de organisatie.

Deze handreiking biedt hiervoor een praktisch kader in de vorm van 7-drivers, die direct aansluiten op wet- en regelgeving en de eisen van de BIO2.

Bestuurders sturen op:

- Kroonjuwelen: Welke processen en systemen zijn cruciaal voor onze dienstverlening?
- Risicobereidheid: Welk risico accepteren we tot op welke hoogte wel of niet?
- Voortgang en naleving: Worden de voor onze organisatie gewenste maatregelen tijdig uitgevoerd?
- Knelpunten: Budget, capaciteit, afhankelijkheden, leveranciers.
- Escalaties: Wanneer grijpen we bestuurlijk in?

Rollen en verantwoordelijkheden bij inrichting governance informatiebeveiliging

De handreiking benadrukt het inrichten van een heldere governance met daarbij de onderstaande taakverdeling. Hierbij wordt uitgegaan van de verdeling dat de bestuurder die de eindverantwoordelijkheid draagt (in het RASCI-model is dit *Accountable*) de uitvoerende en operationele verantwoordelijkheid (*Responsible*) heeft belegd bij de lijn. De CISO vervult hierbij een adviserende en ondersteunende rol (*Support, Consult* en *Informed*).

Ook in het geval van meerdere benamingen voor bestuurders, bedoelen we diegene, waarvan is afgesproken die de eindverantwoordelijkheid (*Accountable*) draagt.
In dit document verdelen we de verantwoordelijkheid voor informatiebeveiliging en bedrijfscontinuïteit als volgt:
Bestuurder:

- Eindverantwoordelijk voor inrichten van risicomanagement gericht op borging digitale weerbaarheid van de organisatie;

- Verantwoordelijk voor het treffen van passende en evenredige technische, operationele en organisatorische maatregelen en ziet toe op naleving daarvan;
- Bepaalt risicobereidheid van de organisatie;
- Stelt middelen beschikbaar.

Lijn (directies, afdelingen, proceseigenaren):
- Eigenaar van informatie(systemen) en daarmee verantwoordelijk voor het identificeren van dreigingen en risico's van deze informatie(systemen);
- Verantwoordelijk voor het toepassen van de verplichte beheersmaatregelen uit wet- en regelgeving voor het informatiesysteem;
- Informeert en vraagt CISO om advies, in alle gevallen waar het afwijkt van de kaders, ook waar dat expliciet als bevoegdheid genoemd is;
- Rapporteert via CISO en legt verantwoording af aan Bestuurder

CISO:
- Verantwoordelijk voor de coördinatie en het faciliteren van informatiebeveiliging;
- Ondersteunt de bestuurder en kan gevraagd en ongevraagd advies geven over risico's en maatregelen aan de bestuurder;
- Vertaalt wet- en regelgeving en bedrijfsdoelstellingen naar een informatiebeveiligingsbeleid en toe te passen kaders;
- Monitort en rapporteert aan het bestuur hoe het lijnmanagement het informatiebeveiligingsbeleid implementeert en op welke wijze wordt voldaan aan de kaders. Om ervoor zorg te dragen dat de bestuurder geïnformeerde besluiten kan nemen over de behandeling van informatiebeveiligingsrisico's;
- Is niet verantwoordelijk voor informatiebeveiliging door het lijnmanagement, maar kan wel bijdragen bij implementaties.

De 7-drivers: de basis voor bestuurlijke gesprekken

Deze handreiking geeft hulp in de vorm van 7 onderwerpen (zgn. drivers) waarop de informatiebeveiliging in de organisatie ingericht kan worden. Deze bestaan uit:

1. Kroonjuwelen beschermen;
2. Kijk verder dan de eigen organisatie;
3. Zorg dat wat veilig is, veilig blijft;
4. Identity & Access Management;
5. Afscherming, detectie monitoring en response;
6. Incident- en crisismanagement;
7. Meten, leren en bijsturen.

Jaarcyclus voor bestuurlijke sturing:

Om bovenstaande drivers in de organisatie te accepteren en te implementeren, is het te adviseren om in een voorgestelde jaarcyclus de volgende stappen uit te voeren:

Stap 1 – Bestuurder ↔ CISO – opdracht tot inrichting informatiebeveiliging
Stap 2 – Bestuurder ↔ Lijn – opdracht tot uitvoering informatiebeveiliging
Stap 3 – Dashboard opstellen (CISO) – inzichtelijk maken van scores, voortgang en risico's
Stap 4 – Kwartaalgesprekken Bestuurder, Lijn en CISO– bewaking en monitoring voortgang en status informatiebeveiliging

Wat de Bestuurder vandaag nog moet besluiten?

Ter bewaking en de borging van de risico's die er zijn op het gebied van informatiebeveiliging is het te adviseren dat de volgende zaken in de organisatie al zijn opgepakt of nog worden opgepakt:

- Governance vaststellen;
- 7-drivers als indeling van de kaders accepteren;
- Jaarcyclus borgen;
- Risicobereidheid bevestigen;
- Sturen op naleving wet- en regelgeving en kaders voor informatiebeveiliging;
- Periodieke rapportages volgens 7-drivers indeling en jaarcyclus.

Welke bestuurlijke risico's zijn er bij niet-handelen?

Het niet inzichtelijk hebben en het niet bewaken van de risico's op het gebied van informatiebeveiliging kunnen de volgende ongewenste zaken tot gevolg hebben:

- Verstoorde dienstverlening – continuïteit van de organisatie is niet geborgd;
- Verlies van legitimiteit;
- Verlies van vertrouwen van de samenleving (burgers en bedrijven) in de (digitale) overheid;
- Aansprakelijkheid bestuur(ders);
- Non-compliance met geldende wet- en regelgeving;
- Externe interventie;
- Escalaties in ketens.

Het advies luidt dan ook: maak gebruik van de aanpak van 7-drivers, bewaak de uitkomsten van de indicatoren en borg de inrichting in een jaarcyclus.

1.1 Leeswijzer

Deze handreiking bevat praktische handvatten voor bestuurders, lijn en CISO's om de sturing op informatieveiligheid in de organisatie op te pakken in de vorm van 7-drivers.
Deze aanpak is ontwikkeld op basis van gesprekken in 12 overheidsorganisaties en vervolgens geactualiseerd door een inhoudelijke toetsing met de eisen uit de BIO2 en de *Handreiking cybersecurity voor bestuurders en bedrijfseigenaren*[1] van de Cybersecurityraad (CSR).

- Hoofdstuk 2 vormt de inleiding en schetst het belang van informatieveiligheid als bestuurlijke verantwoordelijkheid, plaatst cyberdreiging in het perspectief van bedrijfscontinuïteit en beschrijft het noodzakelijke samenspel tussen bestuurder, lijn en CISO om hier effectief op te sturen.
- Hoofdstuk 3 richt zich op het opzetten van een goede governance voor informatiebeveiliging, waarbij een monitoring managementsysteem voor informatiebeveiliging (ISMS) wordt ingericht. Daarnaast bevat het de opzet voor een gesprekcyclus, een praktische aanpak om de hele organisatie te betrekken. Hierbij wordt verwezen naar bijlage 1; voorbeeld opdrachtbrieven naar de lijn en de CISO.
- Hoofdstuk 4 presenteert de 7-drivers als basis voor gesprekken tussen bestuurders en de lijn (ondersteund door de CISO). Elke driver is uitgewerkt aan de hand van bestuurlijke vragen, meetbare KPI's en een bijbehorend sturingskader, die helpen bij het formuleren van concrete acties en het monitoren van voortgang.
  Dit hoofdstuk vormt de basis voor het afstemmen van prioriteiten en het implementeren van effectieve informatieveiligheidsmaatregelen.

Voor bestuurders van private ondernemingen (bestuurders, leden van raden van commissarissen en toezicht in alle organisaties) is en blijft cybersecurity net zo van belang om rekening mee te houden voor bedrijfscontinuïteitsvraagstukken. De inhoud van deze handreiking is in eerste instantie bedoeld voor overheidsorganisaties, maar het is ook voor private ondernemingen toepasbaar.

[1] *https://www.cybersecurityraad.nl/documenten/2025/06/04/handreiking-cybersecurity-voor-bestuurders-en-bedrijfseigenaren*

2. Inleiding

De Nederlandse samenleving en de overheid digitaliseren in hoog tempo. Deze ontwikkeling maakt overheid en bedrijfsleven steeds afhankelijker van betrouwbare digitale systemen, maar vergroot tegelijkertijd de kwetsbaarheid voor digitale dreigingen en risico's. Veelvoorkomende risico's zijn bijvoorbeeld ketenafhankelijkheden, kwetsbaarheden in operationele technologie (OT), menselijke fouten, zwakke wachtwoorden en cyberaanvallen. Ook het uitbesteden van diensten of het werken met cloud-oplossingen kunnen extra risico's met zich meebrengen. Cyberdreiging is daarmee niet alleen een reëel en voortdurend risico, maar een fundamenteel bedrijfscontinuïteitsvraagstuk. Effectieve maatregelen verlagen de risico's tot binnen de risicobereidheid van de organisatie. Tot het restrisico, dat door het bestuur als acceptabel wordt gezien, nadat passende beheersmaatregelen zijn getroffen. Dat stelt hogere (en wellicht nieuwe) eisen aan de organisatie én daarmee ook aan bestuurders, directieleden en verantwoordelijken voor de bedrijfsvoering en informatieveiligheid.

2.1 Informatieveiligheid is chefsache

Informatieveiligheid is chefsache: bestuurders[2] zijn (eind-)verantwoordelijk voor een veilige en betrouwbare informatievoorziening. Wanneer cyberrisico's werkelijkheid worden, raken de gevolgen direct de continuïteit van de organisatie, het vertrouwen van burgers en bedrijven en de uitvoerbaarheid van publieke taken. De bestuurder bepaalt welke risico's de organisatie accepteert en ziet erop toe dat maatregelen die risico's beperken tot een aanvaardbaar niveau. Daarbij is het van belang dat bestuurders zicht hebben op de zogenoemde kroonjuwelen van de organisatie: de gegevens, processen en applicaties waarvan verstoring of uitval directe gevolgen heeft voor de betrouwbaarheid en/of continuïteit van de productie, dienstverlening en de bedrijfsvoering.

Voor bestuurders in de overheidssector wordt gesproken over verantwoordelijkheid, terwijl er in het bedrijfsleven vaak wordt gesproken over aansprakelijkheid. Deze handreiking is in eerste instantie gericht op bestuurders binnen de overheid, daarom wordt het begrip verantwoordelijk (*Accountable* in de RASCI-methode) gebruikt. Toch kunnen bestuurders uit het bedrijfsleven ook zeker passende handvatten terugvinden die toepasbaar zijn op hun organisatie. In dit document zullen we hierna het begrip verantwoordelijkheid gebruiken.

De Nederlandse overheid heeft in 2025 een vernieuwd normenkader vastgesteld: de Baseline Informatiebeveiliging Overheid 2 (BIO2). Dit normenkader geldt voor alle overheidsorganisaties en wordt via de Cbw - zodra deze in werking treedt - wettelijk verankerd via een ministeriële regeling. De BIO2 bepaalt dat bestuurders verantwoordelijk zijn voor de inrichting en werking van het managementsysteem voor informatieveiligheid (ISMS). Het ISMS[3][4] moet daarom volledig worden geïntegreerd in de algemene managementstructuur en reguliere jaarcyclus. Bestuurders moeten actief sturen op risicomanagement, monitoring en continue verbetering. Deze verantwoordelijkheid wordt versterkt door Europese kaders, die bestuurders verplichten toezicht te houden op de uitvoering van cybersecuritymaatregelen en te

[2] *Met 'bestuurders' wordt het bevoegde bestuursorgaan bedoeld zoals aangewezen in artikel 24 van de Cbw (waaronder bij overheidsorganisaties de minister, het college van B&W, gedeputeerde staten en het dagelijks bestuur).*

[3] *https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/besturen/beginnen-met-een-isms*

[4] *De ISO-vereisten voor een Information Security Management System (ISMS) conform ISO 27001 omvatten het opzetten, implementeren, onderhouden en continu verbeteren van een aanpak voor informatiebeveiliging. Dit omvat het begrijpen van de context van de organisatie, het identificeren van belanghebbenden, het uitvoeren van risicoanalyses, het implementeren van beveiligingsmaatregelen en het periodiek evalueren van de prestaties.*

beschikken over voldoende kennis en deskundigheid om risico's te begrijpen en te beheersen. In geval van tekortschietend toezicht worden zij bestuurlijk verantwoordelijk geacht.

Deze verplichtingen voor organisaties (en daarmee bestuurders) vloeien voort uit o.a.:

- Cyberbeveiligingswet (Cbw) – verplicht organisaties tot robuust risicobeheer en passende technische en organisatorische maatregelen, en legt een expliciete bestuurlijke verantwoordelijkheid vast voor goedkeuring, toezicht en rolverdeling (artikel 24 Cbw). De wet geeft uitvoering aan de Europese NIS2- en CER-richtlijnen.
- Digital Operational Resilience Act (DORA) – verplicht financiële instellingen en hun ICT-leveranciers tot geïntegreerd beheer van ICT- en cyberrisico's, waarbij het leidinggevend orgaan (waaronder de bestuurder) verantwoordelijk is voor vaststelling, goedkeuring en toezicht op digitale weerbaarheid, incidentrespons en uitbesteding (artikelen 5 en 6 DORA).
- Cyber Resilience Act (CRA) – stelt beveiligingseisen aan producten met digitale elementen en verplicht fabrikanten en leveranciers tot veilig ontwerp, onderhoud en kwetsbaarheidsbeheer gedurende de gehele productlevenscyclus, waarvoor bestuurders verantwoordelijk zijn voor de borging van naleving binnen de organisatie (artikelen 10 en 13 CRA).

Om de basis in een organisatie op orde te brengen, moet duidelijk zijn welke normen gelden, wie verantwoordelijk is en welke eisen aan informatiesystemen worden gesteld. De 7-driversaanpak die in dit document is opgenomen, is één van de instrumenten die kan helpen dit te borgen. De toepassing ervan is afhankelijk van de volwassenheid, context en het risicoprofiel van de organisatie; niet elke organisatie doorloopt alle stappen gelijktijdig of in dezelfde diepgang. Deze handreiking ondersteunt organisaties bij het (verder) versterken en inbedden van sturing op informatieveiligheid, ongeacht hun startpunt.

2.2 Samenspel tussen bestuurder, lijn en CISO

Informatieveiligheid krijgt in de praktijk handen en voeten in een samenspel tussen bestuurders, lijnmanagement 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. Het gevolg is dat informatieveiligheid onvoldoende onderdeel wordt van bestuurlijke afwegingen en de sturing in de praktijk grotendeels bij de CISO en zijn team komt te liggen. In dit document wordt hierna de CISO genoemd als de vertegenwoordiger van de sturing op informatieveiligheid. Hiermee wordt voorkomen dat we hierbij ook de FG en beleidsadviseurs (of andere functionarissen die in uw organisatie zich hiermee inlaten) moeten noemen.

Een effectieve governance-structuur[5] voor informatiebeveiliging en bedrijfscontinuïteit is daarom essentieel om dit samenspel beter vorm te geven. De hieronder beschreven rolverdeling is, met behoud van de eindverantwoordelijkheid van de bestuurder, richtinggevend en kan afhankelijk van context en volwassenheid anders zijn ingevuld. In dit document wordt de verdeling van verantwoordelijkheden als volgt beschreven:

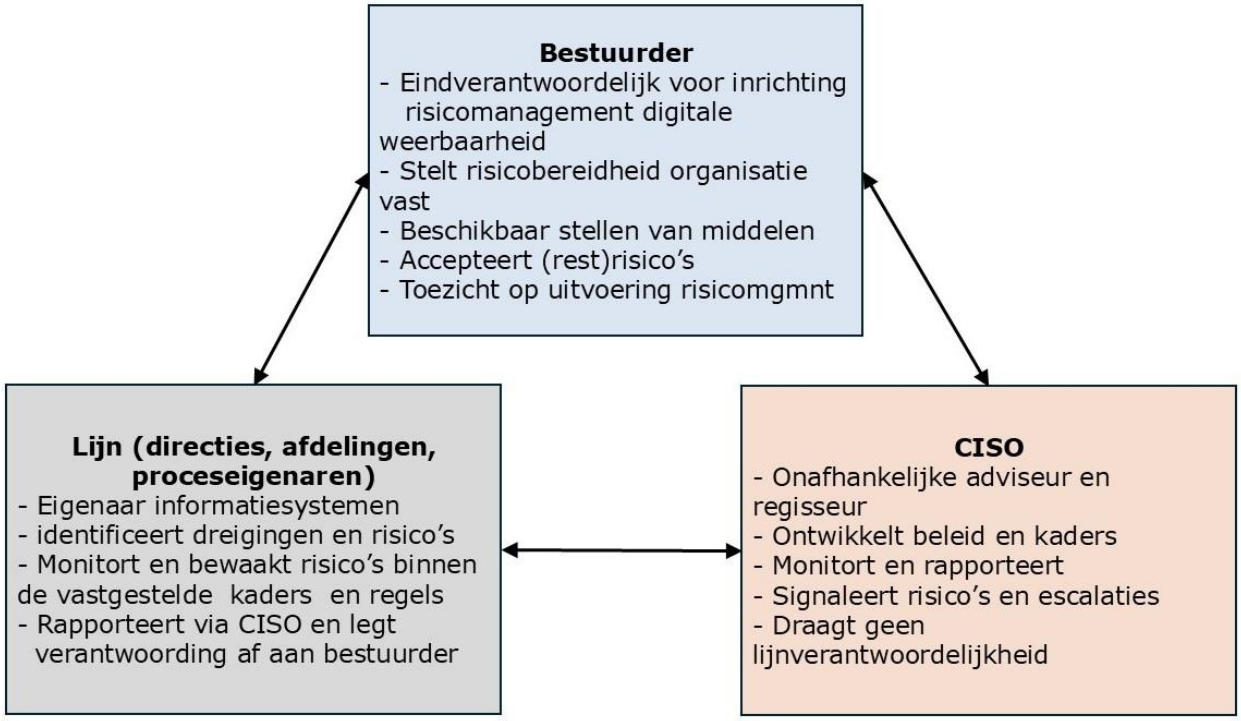
- De bestuurder is eindverantwoordelijk voor informatieveiligheid in de organisatie. De bestuurder bepaalt de strategie, stelt middelen beschikbaar en accepteert restrisico's.

[5] *Governance betekent het (be-)sturen, leidinggeven en omvat de samenhang van regels, processen, structuren en gedragscodes waarmee een organisatie (bedrijf, overheid, non-profit) wordt geleid, beheerd en gecontroleerd, met focus op verdeling van verantwoordelijkheid, transparantie en verantwoording afleggen.*

- De 'lijn' (directies, afdelingen, proceseigenaren) is verantwoordelijk voor het borgen van de informatieveiligheid binnen hun domein. Zij implementeren maatregelen, maken afwegingen en dragen de operationele verantwoordelijkheid. In het RASCI-model is dit weergegeven als *Responsible*.
- De CISO heeft een adviserende en ondersteunende rol. De CISO ontwikkelt beleid en richtlijnen, adviseert bestuur en lijn over risico's en maatregelen, monitort de voortgang en rapporteert over het niveau van informatieveiligheid. De CISO heeft geen lijnverantwoordelijkheid, maar kan adviseren en inhoudelijk ondersteunen. In het RASCI-model is dit weergegeven als *Support, Consult & Informed.*

Belangrijk om te benadrukken: de verantwoordelijkheid voor informatieveiligheid ligt bij u als bestuurder en bij 'de lijn' (directies, afdelingen en proceseigenaren die de dienstverlening verzorgen). De CISO en het informatiebeveiligingsteam zijn adviseurs en ondersteuners, ontwikkelen beleid, monitoren en rapporteren. De lijn neemt de besluiten en voert de maatregelen uit.

Een goede samenwerking tussen bestuurder, lijn en CISO vraagt om duidelijke rolverdeling, open communicatie en wederzijds vertrouwen. Met duidelijke rollen en goede samenwerking wordt de informatieveiligheid en bedrijfscontinuïteit duurzaam geborgd en verbeterd binnen de organisatie. Daarnaast is het implementeren van een governance-structuur verplicht volgens de BIO2 en de Cbw. Hieronder is een overzicht van verantwoordelijkheden opgenomen, wat de basis is geweest voor deze handreiking.



2.3 Handvatten voor gesprek en sturing

Dit document biedt de bestuurder en de experts binnen de organisatie handvatten om informatieveiligheid in samenspel echt chefsache te maken. Zodat de bestuurder bewust en goed geïnformeerd keuzes kan maken over de risico's die de organisatie loopt, en actief sturing kan geven. De geschetste aanpak stelt de bestuurder beter in staat hun verantwoordelijkheid te nemen. En het biedt directie- en lijnmanagement, net als CISO's, het benodigde inzicht om hen daarin effectief te ondersteunen. Dit document biedt daarnaast een goed uitgangspunt om verantwoording af te leggen over risico's, keuzes, maatregelen en beleid.
De zeven onderwerpen (de 7-drivers van informatieveiligheid) helpen om verandering te activeren en beweging te brengen in de organisatie. Ze ondersteunen bovendien een goed gesprek tussen de bestuurder en de lijn (ondersteund door de CISO). De 7-drivers sluiten aan op de BIO2 en vormen een praktische clustering en verdieping van de meest kritische onderwerpen daaruit.

7-drivers: zeven onderwerpen voor een goed gesprek tussen bestuurder en lijn, ondersteund door de CISO:

- De kroonjuwelen beschermen;
- Kijk verder dan de eigen organisatie;
- Zorg dat wat veilig is, ook veilig blijft;
- Identity & access management (IAM);
- Afscherming, detectie, monitoring en response;
- Effectief handelen bij incidenten en crisissen;
- Meet, leer en stuur bij.

2.4 Van een goed gesprek naar effectieve sturing

Met de 7-drivers kan de bestuurder de weerbaarheid, het herstelvermogen en een continu verbeter- en leerproces (leervermogen) in samenhang bespreken. Randvoorwaarden voor effectieve sturing zijn goede gesprekken en concrete afspraken tussen bestuurder en de lijn (ondersteund door de CISO), waarbij vertrouwen en eerlijkheid essentieel zijn. Niet alle signalen over risico's komen in organisaties vanzelf naar boven, daarom is het belangrijk dat de bestuurder een cultuur bevordert waarin openheid wordt gestimuleerd waarbij de focus ligt op een 'goede werking' en niet (alleen) op 'vinkjes zetten'. Daarnaast zijn een duidelijke governance met heldere rolverdeling, een vaste gespreks- en rapportagecyclus en de inbedding van informatieveiligheid in de reguliere management- en jaarcyclus essentieel. Hierdoor ontstaat gezamenlijk begrip en kan structureel worden gestuurd op risico's en verbetering.

Binnen deze randvoorwaarden worden vervolgens gezamenlijk afspraken gemaakt over wat de organisatie wil bereiken op het gebied van informatieveiligheid en de daarbij te nemen maatregelen. In hoofdstuk 4 wordt deze sturing verder uitgewerkt aan de hand van de 7-drivers en bijbehorende bestuurlijke vragen. Door voortgang en nieuwe ontwikkelingen periodiek te bespreken, ontstaat een doorlopend beeld van de informatieveiligheid. Een gesprekscyclus met afspraken en KPI-rapportages ondersteunt de bestuurlijke sturing.

3. Van organisatie tot sturing

In organisaties kunnen mogelijke incidenten met grote impact op informatiebeveiliging worden voorkomen. Met goede en passende organisatie-inrichting, sturing en een grondige aanpak zijn de kansen op een onvoorspelbare en slechte afloop tot een beheersbaar en aanvaardbaar niveau terug te brengen.

3.1 Governance en ondersteuning

Voor deze beheersbaarheid vereist BIO2 dat er een formele governancestructuur, zoals uitgelegd in hoofdstuk 2.2, is opgebouwd. De governance voor informatiebeveiliging verwijst naar de manier waarop dit in de organisatie wordt geleid en bestuurd. Het omvat de regels, processen en structuren die zijn ingesteld om verantwoordelijkheid, rekenschap en control binnen de organisatie te beheren. Binnen deze governancestructuur ligt de verantwoordelijkheid voor de uitvoering van informatieveiligheid in de lijn: directies, afdelingen en proceseigenaren zijn verantwoordelijk voor de informatieveiligheid binnen het eigen domein. De CISO ondersteunt en adviseert de lijn met beleid, kaders, monitoring en rapportages, maar neemt geen lijnbeslissingen.

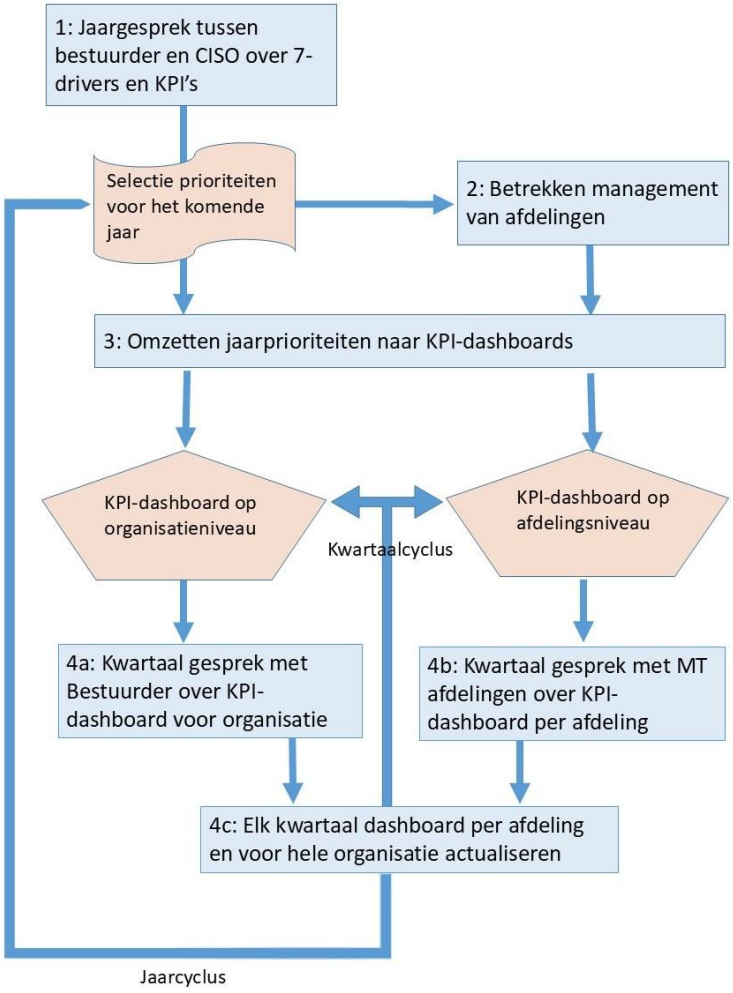
Centraal in de formele structuur is het inrichten van een managementsysteem voor informatiebeveiliging (ISMS) de werkwijze om informatiebeveiliging op een gestructureerde manier toe te passen in de organisatie. Zo wordt de organisatie, en een bestuurder in het bijzonder, in staat gesteld om de juiste afwegingen te maken. Om een veelvoorkomend misverstand te voorkomen: een managementsysteem is géén IT-systeem of applicatie, maar een samenhangend geheel van processen, verantwoordelijkheden en beheersmaatregelen voor informatiebeveiliging, waarvoor de CISO verantwoordelijk is voor het opzetten en bijhouden. Dit ISMS omvat onder meer de context van de organisatie, leiderschap, planning, ondersteuning, uitvoering, evaluatie van prestaties en continue verbetering.

De reikwijdte van het ISMS is aan de organisatie zelf, maar moet minimaal de bedrijfsprocessen en informatiesystemen ‘beveiligen’ die kritisch zijn voor het betrouwbaar blijven leveren van diensten en/of producten aan haar afnemers. In de 7-driversaanpak noemen we dit de kroonjuwelen. Het is belangrijk dat het ISMS deel uitmaakt van en geïntegreerd is met de reguliere procedures van de organisatie en met de algehele managementstructuur, en dat informatiebeveiliging een integraal onderdeel is bij het ontwerpen van processen, informatiesystemen en beheersmaatregelen. Met behulp van de juiste procedures en de ondersteuning van een ISMS wordt het uitvoeren van de in BIO2 verplichte items, zoals een actueel risicoregister en een gedocumenteerde PDCA-cyclus (Plan-Do-Check-Act), eenvoudiger. Het is een organisatiebreed hulpmiddel om de risico’s in kaart te brengen en te kunnen beoordelen.

3.2 Jaarcyclus

In de procedures is het van belang op te nemen met welke regelmaat de bestuurder op de hoogte wordt gebracht van de voortgang van informatieveiligheid. De BIO2 vereist een cyclische aanpak (PDCA) om structurele sturing, monitoring en continue verbetering mogelijk te maken; in deze handreiking wordt deze cyclus concreet ingevuld als een jaarcyclus. Het vaststellen van deze jaarcyclus is formeel de verantwoordelijkheid van de bestuurder. De uitvoering van de jaarcyclus is echter een gezamenlijke opdracht van bestuurder en CISO en maakt onderdeel uit van een meerjarenaanpak, waarin de cyclus jaarlijks wordt herhaald. In deze handreiking wordt toegelicht welke onderwerpen, momenten en rapportages binnen deze cyclus kunnen worden opgenomen.

De jaarcyclus ziet er op hoofdlijnen als volgt uit:



[6]

In de beschrijving in paragraaf 3.3 wordt vooral beschreven hoe de stappen in het eerste jaar kunnen worden doorlopen. Dat eerste jaar kan onwennig zijn, omdat het proces en de inrichting nieuw zijn. Wellicht is er weerstand in de organisatie die overwonnen moet worden. Echter vormt het een startpunt van een meerjarenaanpak waarin de jaarcyclus steeds wordt herhaald en verder wordt aangescherpt. 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.

Nieuwe tooling nodig? Tips en aandachtspunten

Het kan behulpzaam zijn om met een Excel-expert of met een GRC (Governance, Risk & Compliance)-toolleverancier te bespreken 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. Daarbij is het van belang dat in Excel of in de GRC-tool de status van elke afdeling periodiek kan worden gecombineerd tot een status voor de hele organisatie.

[6] *Als voorbeeld is hier de regelmaat kwartaal gebruikt. Aansluiting op bestaande sturings- en verantwoordingscyclus van de organisatie (maand, twee-maands, kwartaal of tertaal) heeft de voorkeur.*

3.3 De opzet van een jaarcyclus: vier concrete stappen

Stap 1: gesprek tussen bestuurder en CISO

De bestuurder neemt het initiatief om een (jaar)gesprek in te plannen met de CISO, waarin de volgende onderwerpen worden besproken:

1. De bestuurder en de CISO bespreken de grootste zorgen, kansen en prioriteiten van de bestuurder over informatieveiligheid en bedrijfscontinuïteit. De CISO brengt hierbij de actuele stand van zaken, dreigingen en ontwikkelingen in, waarbij de 7-drivers als kapstok dienen.
2. De bestuurder en de CISO bespreken aan de hand van de 7-drivers gezamenlijk de vragenlijst (zie hoofdstuk 4). De CISO licht per driver de belangrijkste aspecten kort toe. Per driver wordt vastgesteld welke vragen en aandachtspunten bij de bestuurder leven.
3. De CISO verwerkt de inbreng van de bestuurder in een jaarprioriteitenoverzicht op basis van de 7-drivers. In hoofdstuk 4 is beschreven hoe dit overzicht kan worden opgesteld. Voor de CISO kan het behulpzaam zijn om voorafgaand aan het gesprek een concept-KPI- en jaarprioriteitenoverzicht op te stellen en dit tijdens of na het gesprek bij te werken.
4. De CISO stelt een bondig gespreksverslag op en deelt dit met de bestuurder.
5. De bestuurder (of directie) stelt een opdrachtbrief op (zie het voorbeeld in bijlage 1) om de lijn te betrekken. In deze brief benadrukt de bestuurder het belang om het dashboard met prioriteiten elk afgesproken moment bij te werken en deze zowel met de bestuurder als met de lijn te bespreken. De voorbeeldbrief in de bijlage kan helpen om helderheid te geven over de opdracht.

Advies: Stap voor stap invoeren

De aanbeveling is te blijven denken aan de eindsituatie, maar start klein. Het is gebleken dat het erg lastig is om alle sturing op de 7-drivers in éénmaal volledig uit te voeren. Daarom het advies om wel al te starten, maar om het (indien noodzakelijk) gefaseerd in te voeren en om een beperkt aantal KPI's in te zetten.
Daarom kun je het bijvoorbeeld als volgt invoeren:

- Kies in eerste instantie jaarlijks drie maatregelen uit de 7-drivers-set.
- Continueer deze rapportages in volgende jaren en voeg elk jaar drie dashboard items toe.

Stap 2: betrek het afdelingsmanagement – zij zijn verantwoordelijk

De bestuurder gebruikt de opdrachtbrief als basis voor het gesprek met (de leden van) de lijn. In dit gesprek wordt benadrukt dat de lijn verantwoordelijk is voor informatieveiligheid binnen hun eigen divisie/directie/afdeling, met aandacht voor eventuele weerstand en hoe daarmee wordt omgegaan.

De CISO ondersteunt de lijn hierbij met:

- Advies over risico's en passende maatregelen;
- Hulp bij het opstellen van plannen;
- Monitoring en rapportage van de voortgang;
- Expertise en kennis van standaarden en best practices.

De lijn neemt zelf de besluiten over:

- Welke prioriteiten zij stellen;
- Hoe zij maatregelen implementeren;
- Welke risico's zij accepteren (binnen de vastgestelde/geldende risicobereidheid);
- Welke middelen zij inzetten.

Advies: Gezamenlijk vaststellen hoe de lijn betrokken blijft

Een aanbeveling is om de lijn niet af te schrikken met alle controles die plaats gaan vinden, maar samen af te stemmen welke aspecten voor hen direct van belang zijn.
Daarom is het advies om dit bijvoorbeeld als volgt in te voeren:

- starten met de controles die mogelijk al worden gemonitord vanuit de lijn;
- starten met contols die het grootste effect kunnen hebben;
- samen vast stellen welke onderdelen direct als dashboarditems kunnen worden opgenomen.

Stap 3: Vertaal het jaarprioriteitenoverzicht in een KPI-dashboard

1. De CISO zet de beantwoorde vragen om naar een aansprekend dashboard. De werkwijze hiervoor is beschreven in hoofdstuk 4.
2. De CISO neemt het proces rond de statusupdate van de KPI's door met de betrokkenen en zijn/haar team(s) op elke afdeling. Om tijdige actualisatie te stimuleren, kan een mini-competitie worden georganiseerd. Daarbij streeft (het team van) elke afdeling het klaar te spelen om binnen één werkdag na de sluitingsdatum van het ISMS of van andere bronapplicaties de KPI-status in het dashboard bij te werken.

Advies: Toegankelijkheid van het dashboard voor bestuurders en lijn

Een aanbeveling is om het dashboard direct toegankelijk te maken voor bestuurders en lijn, waarbij zij zich direct herkennen in de controls en uitkomsten. Bijvoorbeeld door:

- starten met een indeling van controls en uitkomsten die gebaseerd zijn op de structuur van de organisatie.

Stap 4: Kwartaalgesprekken met bestuurder(s) en lijn

1. Ieder kwartaal bespreekt de lijn de KPI-status van de betreffende afdeling(en). De uitvoerende InformatieBeveliging en Privacybewaking (IB&P)-stafmedewerker van de afdeling neemt dan het KPI-dashboard met het voltallige lijn-MT door. Ook worden mogelijke gewenste verbeteringen afgestemd.
2. De CISO bespreekt het gecombineerde dasboard met KPI-statussen voor de hele organisatie met de bestuurder. Feitelijk moeten alle statussen en risico's gerapporteerd worden en centraal beschikbaar zijn. De bestuurder kiest welke risico's besproken moeten worden. De CISO geeft hiervoor advies.
3. De CISO bespreekt, naast de status, ook mogelijk gewenste verbeteringen en uitbreidingen met de bestuurder en lijn.
4. De uitkomsten van de kwartaalgesprekken worden door de CISO gedeeld met de betrokken (afdelings-)teams. De teams bespreken, onder verantwoordelijkheid van het lijn-MT, welke

verbeteringen en uitbreidingen worden doorgevoerd en met welke prioriteit. De uitvoering van deze verbeteringen ligt bij de (afdelings-)teams zelf. Op die manier is er een continue verbeteraanpak met een driemaandelijkse voortgangsrapportage.

Advies: Plan vooruit

Een aanbeveling is om afspraken vooruit in de agenda's vast te leggen:

- De afspraak wordt onderdeel gemaakt van reguliere overleggen, zodat direct operationele en informatiebeveiligingsbevindingen aan elkaar kunnen worden gekoppeld.

4. De 7-drivers uitgewerkt

De vragenlijst in dit hoofdstuk is bedoeld als leidraad voor het gesprek over informatieveiligheid en privacybescherming tussen de bestuurder en de lijn (ondersteund door de CISO). Alle 7-drivers krijgen een verdieping door een aantal concrete bestuurlijke 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 en voor de lijn (ondersteund door de CISO) om in hun rol te komen. Dit gesprek is overigens niet alleen nodig op bestuursniveau, maar ook op afdelingsniveau, met de afzonderlijke MT's. Zij bepalen zelf op basis van risicoafwegingen aan welke van de onderstaande onderwerpen zij prioriteit willen geven. De voorbeelden in dit hoofdstuk zijn generiek en voor veel organisaties toepasbaar. Organisaties dienen aan deze uitgangspunten te voldoen, maar kunnen de vragen, KPI's en bijbehorende uitwerkingen waar nodig aanpassen aan hun eigen context en risico's.

Per driver zijn opgenomen:

1. **Bestuurlijke vragen**: korte, strategische vragen die helpen om het gesprek te voeren over risico's, prioriteiten en verantwoordelijkheden. Deze vragen zijn bedoeld voor bestuurders en houden het gesprek op hoofdlijnen.
2. **KPI's**: opsomming van prestatie-indicatoren die aangeven wat minimaal gemonitord moet worden vanuit de diverse kaders. Ze maken daarmee de drivers bestuurbaar en vormen de basis voor rapportage.
3. **Uitwerking door de lijn (ondersteund door de CISO):** een concreet overzicht van de maatregelen, processen en technische invullingen die nodig zijn om aan de KPI's te voldoen. Dit is de werkagenda voor de lijn.
4. **Bestuurlijk sturingskader (KPI-tabel):** onder elke driver is een KPI-tabel opgenomen met per KPI een voorstel voor de norm, het bestuurlijk risico en het escalatiepunt. De tabel vormt het sturingsinstrument voor bestuur en directie. De status wordt periodiek bepaald via een verkeerslichtmodel: groen (norm gehaald, geen actie), oranje (afwijking of verhoogd risico, bestuur geïnformeerd) en rood (norm niet gehaald of escalatiepunt bereikt, bestuurlijke besluitvorming vereist).

De lijn is verantwoordelijk voor de uitvoering van de maatregelen binnen het eigen domein en voor het periodiek bepalen en toelichten van de status. De CISO ondersteunt dit met:

- Advisering over aanpak en prioritering
- Ontwikkeling van beleid en richtlijnen
- Monitoring en rapportage van voortgang
- Expertise en best practices
- Coördinatie tussen afdelingen (bijv. bij gemeenschappelijke of gedeelde applicaties)

In dit hoofdstuk worden per driver suggesties gedaan om antwoorden, KPI's en statusinformatie om te zetten naar een dashboard. Dit hoeft 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.

4.1 Driver 1: De kroonjuwelen beschermen

Het beschermen van de kroonjuwelen vormt de kern van goed informatiebeveiligingsbeleid. Kroonjuwelen zijn de processen, systemen en gegevens waarvan uitval, verlies of aantasting direct grote impact heeft op de organisatie, dienstverlening of publieke taak. Het vaststellen van deze kroonjuwelen en de bijbehorende ISMS-scope is een noodzakelijk onderdeel van een basis-ISMS; de verdere uitwerking kan meegroeien met de volwassenheid van het ISMS. Dit vereist een volledig en actueel overzicht van de bedrijfsprocessen en het ICT-landschap (inclusief cloud, SAAS, kritieke koppelingen en eventuele schaduw-ICT). De risicoanalyse focust op het inzichtelijk krijgen van de meest kritieke onderdelen. Deze analyse wordt regelmatig organisatiebreed herijkt, inclusief nieuwe technologische risico's. De diepgang en frequentie kunnen daarbij meegroeien met de volwassenheid van het ISMS. Risicobeoordelingen, -acceptaties en restrisico's worden vastgelegd in het risicoregister en het ISMS, zodat risicomanagement aantoonbaar onderdeel is van de sturing en kan worden afgezet tegen de risicobereidheid.

Voor bestuurders ligt hier een belangrijke opdracht: het samen vaststellen van wat de organisatie als kroonjuweel beschouwt, het bepalen van de risicobereidheid en het bewaken dat maatregelen echt worden uitgevoerd. De bestuurder zorgt voor duidelijke prioriteiten, voldoende middelen en een goed werkende governance, zodat de lijn (ondersteund door de CISO) en de organisatie het beveiligingsniveau kunnen realiseren én borgen. Ook wordt van de bestuurder verwacht dat hij of zij periodiek toetst of de resterende risico's acceptabel zijn en waar bijsturing nodig is.

De lijn (ondersteund door de CISO) vertaalt deze bestuurlijke keuzes naar een concrete uitwerking: het in kaart brengen van de kroonjuwelen, het actualiseren van toprisico's, het vastleggen en monitoren van maatregelen en het borgen dat risico's structureel worden gevolgd en gerapporteerd. De uitwerking hieronder beschrijft hoe deze taken invulling krijgen.

Driver 1: De kroonjuwelen beschermen	
Bestuurlijke vragen	**Kern Prestatie Indicatoren (KPI's)**
1. Wat zijn onze kroonjuwelen? 2. Wat zijn de belangrijkste dreigingen? 3. Hoe hebben we onze ICT-omgeving onder controle? 4. Hoe waarborgen we onze weerbaarheid? 5. Is ons restrisico acceptabel? 6. Zijn middelen en governance op orde?	1. Overzicht ICT-inventaris is volledig en actueel. 2. Lijst met kroonjuwelen en toprisico's is actueel en vastgesteld. 3. Maatregelen per kroonjuweel zijn vastgesteld en worden opgevolgd. 4. Restrisico is inzichtelijk en in lijn met de risicobereidheid. 5. Auditplan op toprisico's wordt volgens planning uitgevoerd. 6. Middelen en capaciteit zijn toereikend voor uitvoering van maatregelen.

Uitwerking: Acties voor de lijn (ondersteund door de CISO)

KPI's	Acties / Taken
KPI 1	- Complete en actuele ICT-assetinventaris (incl. cloud, OT, extern). - Proces om schaduw-ICT te identificeren en af te bouwen. - Regelmatige herijking van kritieke systemen, koppelingen en afhankelijkheden. - Toepassing van informatieclassificatie waar relevant.
KPI 2	- Identificeren en actualiseren van de kroonjuwelen en toprisico's (minimaal jaarlijks). - In kaart brengen welke systemen, processen en gegevens onderdeel zijn van elk kroonjuweel. - Periodiek beoordelen van opkomende technologische risico's (zoals cryptografie- en AI-ontwikkelingen) en deze meenemen in het dreigingsbeeld. - Betrekken van bestuurder en afdelings-MT's bij bepaling van toprisico's. - Integreren van risico's uit auditverslagen en eerdere onderzoeken. - Vastleggen van toprisico's als basis voor KPI-sturing en periodieke herijking en registratie daarvan in het risicoregister.
KPI 3	- Vaststellen van preventieve, detectieve en herstelmaatregelen per kroonjuweel. - Aansluiting bij BIO2-maatregelen en vastlegging in SoA/VvT.[7] - Periodieke beoordeling van de effectiviteit van maatregelen. - Signaleren van knelpunten (capaciteit, budget, techniek, leveranciers). - Integreren van bevindingen uit audits en eerdere risicoanalyses in de maatregelpakketten.
KPI 4	- Uitvoeren van risicoanalyses per bedrijfskritisch IV-assets. - Actueel houden van risico-acceptaties (incl. einddatums). - Inzichtelijk maken van restrisico en vergelijking met risk appetite. - Opvolgen en vastleggen van benodigde mitigerende acties.

KPI 5	- Actueel auditplan met focus op toprisico's en relevante maatregelen.
	- Opnemen van minimaal één onafhankelijke audit per toprisico-maatregel (derde partij).
	- Bijhouden van overzicht uitgevoerde audits van de afgelopen twee jaar.
	- Per audit: belangrijkste bevindingen/adviezen + status opvolging.
	- Overzicht van geplande audits:
	  ○ Voorgaande auditbevindingen meenemen.
	  ○ Aansluiten op actuele toprisico's.
	  ○ Vastleggen, opvolgen en periodiek actualiseren van auditbevindingen in het ISMS, inclusief status, risico-impact en verantwoordelijke eigenaar.

KPI 6	- Structureel inzicht in benodigde capaciteit, expertise en middelen. - Tijdige signalering van tekortkomingen of afhankelijkheden. - Onderbouwde voorstellen voor aanvullende middelen of prioritering.

Bestuurlijk sturingskader (KPI-tabel) met daarin opgenomen voorgestelde normen:

KPI	Onderwerp	Norm	Bestuurlijk risico	Escalatiepunt	Status (G/O/R)[8]
1	ICT-inventaris volledig en actueel	100% van systemen, koppelingen, cloud- en OT-omgevingen bekend en geregistreerd	Onbekende systemen worden niet gepatcht of bewaakt → verhoogde kans op cyberincidenten en uitval van kritieke dienstverlening	>5% onbekende of schaduw-ICT → bestuurlijke bijsturing op prioriteit en capaciteit	

[7] *Statement of Applicability of Verklaring van Toepasselijkhied betreft een cruciaal document dat aangeeft welke beveiligingsmaatregelen van toepassing zijn.*

[8] *G/O/R: versimpelde weergave van de mate van informatiebeveiligingsniveau in stoplichtkleur: Groen/Oranje/Rood.*

2	Kroonjuwelen en toprisico's vastgesteld	Jaarlijks vastgesteld door bestuurder en proceseigenaren	Verkeerde prioriteiten: maatregelen op randzaken i.p.v. kernprocessen → verhoogd risico op verstoring publieke taak	Geen bestuurlijke accordering binnen 3 maanden → gesprek op directieniveau	
3	Maatregelen per kroonjuweel vastgesteld en opgevolgd	≥90% van maatregelen per kroonjuweel uitgevoerd volgens planning	Onvoldoende bescherming van kroonjuwelen → hoge kans op uitval van kritieke dienstverlening	Achterstand >20% → herprioritering of extra middelen door bestuur	
4	Restrisico inzichtelijk en in lijn met risicobereidheid	100% van de risicoacceptaties vastgelegd met eigenaar en einddatum	Ongecontroleerde risico's → bestuurlijke aansprakelijkheid en non-compliance (BIO2/NIS2)	Verlopen risicoacceptaties of "stille" restrisico's → directe bestuurlijke besluitvorming	
5	Auditplan op toprisico's uitgevoerd volgens planning	Auditplan op toprisico's uitgevoerd conform planning	Onvoldoende zicht op werking van maatregelen → tekortschietende beheersing en verantwoording	Auditachterstand of kritieke bevinding zonder opvolging → escalatie naar MT/bestuur	
6	Middelen en capaciteit toereikend	Benodigde capaciteit en middelen zijn structureel geborgd	Onvoldoende uitvoeringskracht → maatregelen blijven liggen, risico's nemen toe	Structureel tekort zonder besluit → bestuurlijke afweging over prioriteit en budget	

4.2 Driver 2: Kijk verder dan de eigen organisatie

Organisaties functioneren steeds meer in een netwerk van ketenpartners, leveranciers, leveranciers van cloudoplossingen en andere (externe) dienstverleners. Daarmee verschuift een groot deel van de risico's naar buiten de eigen muren, terwijl de impact bij de organisatie zelf voelbaar blijft. Het beheersen van deze afhankelijkheden is essentieel om continuïteit, integriteit en vertrouwelijkheid van de dienstverlening te waarborgen. Hiervoor is het van belang dat de organisatie goede afspraken maakt met leveranciers en ketenpartners, in lijn met de BIO2 en aanvullende kaders. Daarbij worden leveranciersrisico's regelmatig gemonitord en beoordeeld, en wordt geborgd dat contracten duidelijke verplichtingen bevatten voor leveranciers om te voldoen aan actuele beveiligingseisen.

Voor bestuurders betekent dit dat zij moeten borgen dat keten- en leveranciersrisico's structureel worden meegenomen in besluitvorming, contractering en governance. Zij bepalen de risicobereidheid in de keten, zorgen dat beveiligingsafspraken worden vastgesteld en nageleefd, en zien toe op periodieke herbeoordeling van kritieke leveranciers. Ook is het aan de bestuurder om prioriteit te geven aan transparantie in afhankelijkheden en voldoende middelen beschikbaar te stellen om toezicht, audits en monitoring in de keten uit te voeren.

De uitwerking van de lijn (ondersteund door de CISO) richt zich op het inzichtelijk maken van afhankelijkheden, de beheersing van leveranciers- en ketenrisico's en het borgen dat beveiliging structureel onderdeel is van alle keten- en contractafspraken.

Driver 2: Kijk verder dan de eigen organisatie	
Bestuurlijke vragen	**Kern Prestatie Indicatoren (KPI's)**
1. Hoe borgen we security in de keten? 2. Hoe brengen we onze afhankelijkheden in beeld? 3. Hoe beheersen we leveranciers- en ketenrisico's? 4. Zijn contracten en afspraken voldoende beveiligd?	1. Leveranciers-, cloud- en ketenoverzicht is volledig en actueel. 2. Nieuwe contracten bevatten passende en toegepaste beveiligingseisen. 3. Bestaande contracten zijn herijkt conform actuele beveiligingseisen. 4. Leveranciers zijn geclassificeerd op risico en periodiek herbeoordeeld. 5. Ketenrisico's zijn in beeld en worden gerapporteerd. 6. Audit- en monitoringsafspraken met kritieke leveranciers worden uitgevoerd. 7. Ketenpartners, contactpersonen en verantwoordelijkheden zijn actueel.

Uitwerking: Acties voor de lijn (ondersteund door de CISO)

KPI's	**Acties / Taken**
KPI 1	- Volledige en actuele inventarisatie van leveranciers, cloudpartijen, dienstverleners en ketenpartners (incl. afhankelijkheden en ketenassets). - In kaart brengen van technische afhankelijkheden en mogelijke single points of failure. - Actief opsporen en registreren van niet-bekende of informele leveranciersafspraken (schaduwafspraken).
KPI 2	- Beoordelen van nieuwe aanbestedingen, inkopen en uitbestedingen op securityrisico's. - Opnemen van passende beveiligingseisen, zoals auditrechten, hardening, monitoring, incidentmeldplicht, data-locatie, bewaartermijnen en compliance. - Gebruik van de ICO-Wizard voor het samenstellen van informatieveiligheidseisen bij aanbestedingen en (nieuwe of continuerende) contracten (aanbevolen door BZK en EZK binnen de Roadmap Digitaal Veilige Hard- en Software (DVHS)). - Toepassen van security-by-design en security-by-default in nieuwe contracten en diensten.
KPI 3	- Systematische herijking van bestaande contracten volgens een vastgesteld plan. - Controleren of contracten voldoen aan actuele BIO2-vereisten voor leveranciers en cloud. - Bijstellen van afspraken over beveiliging, privacy en bewaartermijnen (AVG/Archiefwet).
KPI 4	- Classificeren en prioriteren van leveranciers op basis van risico (kritiek, hoog, middel, laag). - Minimaal jaarlijkse herbeoordeling van kritieke leveranciers; vaker als risico's of omstandigheden wijzigen. - Meewegen van geopolitieke risico's, datalocatie en vervangbaarheid. - Opstellen van exit-strategie of uitwijkscenario's voor kritieke leveranciers.
KPI 5	- Uitvoeren en actualiseren van ketenrisicoanalyses (incl. IV-koppelingen en ketenprocessen). - Integreren van informatieclassificatie in de ketencontext. - Structurele rapportage van ketenrisico's aan bestuurder; inclusief afhankelijkheden, trends en opvolging.
KPI 6	- Opstellen en uitvoeren van audit- en monitoringsafspraken voor kritieke leveranciers. - Uitvoeren van audits (intern/extern), controles en technische tests waar relevant.

	- Vastleggen en opvolgen van bevindingen binnen het ISMS.
KPI 7	- Actueel overzicht van ketenpartners, contactpersonen, verantwoordelijkheden en hun rollen in beheer, security en escalatie opstellen en onderhouden. - Ketenverantwoordelijkheden en keteneigenaarschap vastleggen in beleid. - Afspraken, documentatie en rapportages bijwerken in het ISMS en richting MT/bestuur.

Bestuurlijk sturingskader (KPI-tabel) met daarin opgenomen voorgestelde normen:

KPI	Onderwerp	Norm	Bestuurlijk risico	Escalatiepunt	Status (G/O/R)
1	Leveranciers-, cloud- en ketenoverzicht volledig en actueel	100% van de kritieke leveranciers, cloudpartijen en ketenpartners geïdentificeerd	Afhankelijkheden zijn onzichtbaar → ongecontroleerde uitval in de keten en verstoring van publieke dienstverlening	Onbekende kritieke leverancier of cloudpartij → directe bestuurlijke escalatie	
2	Nieuwe contracten met passende beveiligingseisen	Nieuwe contracten 100%; bestaande contracten 80% binnen 12 maanden geactualiseerd (tenzij onevenredige kosten)	Geen afdwingbare maatregelen en geen auditrecht → non-compliance met BIO2/NIS2 en onvoldoende grip op leveranciers	Contract met hoge kriticiteit zonder beveiligingsclausules → bestuurlijke besluitvorming	
3	Bestaande contracten herijkt conform actuele eisen	Herijking uitgevoerd volgens vastgesteld plan	Verouderde contractafspraken → verhoogd risico op datalekken, uitval en juridische aansprakelijkheid	Afwijking van herijkingsplanning bij kritieke contracten → escalatie naar MT/bestuur	
4	Leveranciers geclassificeerd en periodiek herbeoordeeld	100% kritieke leveranciers minimaal jaarlijks beoordeeld	Verstoring bij leverancier leidt tot uitval van publieke dienstverlening	Leverancier met hoog risico zonder verbeterplan → bestuurlijke escalatie	
5	Ketenrisico's in beeld en gerapporteerd	Ketenrisicoanalyses actueel en periodiek gerapporteerd aan bestuurder	Onvoldoende zicht op ketenafhankelijkheden → verlies van regie en verhoogd maatschappelijk risico	Geen actuele ketenrisicoanalyse of rapportage → escalatie naar directie/bestuur	
6	Audit- en monitorings afspraken met kritieke leveranciers uitgevoerd	Audit- en monitoringsafspraken uitgevoerd conform planning	Onvoldoende toezicht op leveranciers → tekortschietende beheersing en verantwoording	Auditachterstand of kritieke bevinding zonder opvolging → escalatie naar MT/bestuur	
7	Ketenpartners, contactpersonen en verantwoordelijkheden actueel	Overzicht ketenpartners, contactpersonen en verantwoordelijkheden actueel	Onduidelijke verantwoordelijkheden → trage incidentrespons en bestuurlijke onzekerheid	Ontbrekende of verouderde ketenafspraken bij kritieke ketens → bestuurlijke escalatie	

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

Het blijvend veilig houden van systemen vraagt om continu onderhoud, tijdige vernieuwing en het structureel oplossen van kwetsbaarheden. Technische schuld[9], verouderde technologie en nieuwe dreigingen kunnen de betrouwbaarheid van de dienstverlening onder druk zetten wanneer zij niet actief worden gemanaged. Deze driver richt zich op het borgen van een stabiel, robuust en toekomstbestendig beveiligingsniveau. Hierbij is het van belang dat de organisatie tijdig security-updates uitvoert binnen het IV-landschap om nieuwe technische bedreigingen het hoofd te kunnen bieden, verouderde software tijdig te vervangen en de veiligheid van systemen regelmatig te beoordelen.

De bestuurder heeft daarbij de taak om te zorgen dat veilig beheer een integraal onderdeel is van de reguliere bedrijfsvoering. Dit betekent het vaststellen van duidelijke prioriteiten, het organiseren van voldoende middelen en capaciteit, en het bewaken dat risico's door veroudering, kwetsbaarheden of afhankelijkheden in cloud- en platformsystemen tijdig worden aangepakt. Bovendien bepaalt de bestuurder de risicobereidheid voor kritieke systemen en stuurt op structurele modernisering en vervanging wanneer dat noodzakelijk is. Daarmee creëert het bestuur de randvoorwaarden waarbinnen systemen duurzaam en aantoonbaar veilig kunnen blijven functioneren.

De uitwerking door de lijn (ondersteund door de CISO) beschrijft hoe dit in de praktijk wordt ingevuld, met focus op patching, kwetsbaarhedenbeheer, lifecycle-management, systeem-hardening en het beheersen van cloud-, netwerk- en cryptografierisico's.

Driver 3: Zorg dat wat veilig is, ook veilig blijft	
Bestuurlijke vragen	**Kern Prestatie Indicatoren (KPI's)**
1. Hoe houden we onze systemen veilig en up-to-date? 2. Hoe beperken we technische schuld en borgen we tijdige vernieuwing van systemen? 3. Hoe borgen we veilige internet- en cloudservices? 4. Hoe beheersen we kwetsbaarheden en misbruikrisico's? 5. Hoe zorgen we dat kritieke systemen structureel beschermd blijven?	1. Kwetsbaarheden en patches worden tijdig en aantoonbaar opgelost. 2. Internetgerichte diensten voldoen aan veilige standaarden en worden periodiek getoetst. 3. Systeemveiligheid en risicobeheersing voor nieuwe en bestaande systemen is aantoonbaar en actueel. 4. Afbouw van technische schuld voor verouderde systemen en bescherming van nieuwe systemen wordt systematisch uitgevoerd. 5. Kritieke systemen en omgevingen zijn duidelijk geïdentificeerd en actueel. 6. Cloud-, netwerk- en platformrisico's zijn in beeld en worden beheerst. 7. Cryptografie- en sleutelbeheer zijn geborgd op organisatieniveau.

Uitwerking: Acties voor de lijn (ondersteund door de CISO)

KPI's	**Acties / Taken**
KPI 1	- Patchmanagementproces op basis van risico, ernst en exploitatiekans. - Tijdig toepassen van patches om misbruik van kwetsbaarheden in verouderde systemen te voorkomen. - Overzicht en monitoring van patchstatus voor alle systemen (incl. cloud, OT en internetgerichte diensten).

[9] *Technische schuld staat hier voor verouderde? soft- en hardware waardoor er toenemende risico's zijn dat kwetsbaarheden door bijvoorbeeld hackers of andere actoren worden benut.*

	- Hardening, gecontroleerde software-installatie (whitelisting) en antimalware borgen de basisveiligheid.
KPI 2	- Web- en maildiensten voldoen aan de standaarden van Forum Standaardisatie (incl. internet.nl-score). - Periodieke technische toetsing op TLS, DMARC, DKIM/SPF en veilig configureren van alle diensten die in aanraking komen met het internet.
KPI 3	- Inzicht in systeemveiligheid, inclusief risico's door veroudering, end-of-life-systemen, niet-patchbare kwetsbaarheden en benodigde vernieuwingen per bedrijfskritische IV-asset. - Analyse van kosten en mogelijkheden om kwetsbaarheden en zwakke plekken op te lossen. - Integreren van auditbevindingen en leveranciersadviezen, accordering door management.
KPI 4	- Risicogebaseerd levenscyclus- en moderniseringsplan voor systemen opstellen en uitvoeren (onderhoud, vervanging, migratie, uitfasering). - Zwakke plekken planmatig wegnemen via vervanging, migratie of hardening. - Voortgang en knelpunten bewaken en periodiek rapporteren. - Segmentatie en scheiding van omgevingen toepassen om risico's te beperken.
KPI 5	- Volledig en actueel overzicht van kritieke systemen, afhankelijkheden en koppelingen. - Periodieke herijking bij wijzigingen in processen, organisatie of leveranciers. - Vastleggen van single points of failure en ketenafhankelijkheden.
KPI 6	- Risico's in cloud, netwerkarchitectuur en platforms periodiek beoordelen. - Scheiding tussen beheer- en gebruiksomgevingen en passende hardening toepassen. - Toetsing van cloudleveranciers op beveiliging, datalocatie en compliance. - Registratie en opvolging van risico's door configuratiefouten of kwetsbaarheden.
KPI 7	- Cryptografiebeleid en sleutelbeheerproces vaststellen en onderhouden. - Veilige sleutelopslag, rotatie en toegangsbeheer toepassen. - Periodieke beoordeling van cryptografische instellingen, incl. voorbereiden op toekomstige (post-quantum) risico's. - Rapporteren van afwijkingen en verbeteracties.

Bestuurlijk sturingskader (KPI-tabel) met daarin opgenomen voorgestelde normen:

KPI	Onderwerp	Norm	Bestuurlijk risico	Escalatiepunt	Status (G/O/R)
1	Patchmanagement en basisbeveiliging	100% Kritieke kwetsbaarheden gepatcht binnen vastgestelde termijnen op basis van risico	Misbruik van bekende kwetsbaarheden → verhoogde kans op cyberincidenten en uitval van dienstverlening	Overschrijding patchtermijnen bij kritieke systemen → bestuurlijke bijsturing op prioriteit en capaciteit	
2	Beveiliging web- en maildiensten	100% Web- en maildiensten voldoen aan standaarden Forum Standaardisatie	Onvoldoende beveiligde internetdiensten → verhoogd risico op misbruik, phishing en datalekken	Structurele non-compliance met standaarden → escalatie naar MT/bestuur	
3	Inzicht in systeemveiligheid en veroudering	Inzicht in risico's, EOL/EOS en niet-patchbare kwetsbaarheden per kritisch IV-asset	Verouderde of kwetsbare systemen blijven in gebruik → verhoogd risico op uitval en aansprakelijkheid	Kritiek IV-asset met niet-geaccepteerd restrisico → bestuurlijke besluitvorming	

4	Levenscyclus- en moderniseringsplanning	Risicogebaseerd levenscyclus- en moderniseringsplan vastgesteld en uitgevoerd	Achterstallige vernieuwing → structurele kwetsbaarheden en verlies van beheersbaarheid	Structurele vertraging of knelpunt zonder besluit → escalatie naar bestuur	
5	Overzicht kritieke systemen en afhankelijkheden	100% van de kritieke systemen, koppelingen en afhankelijkheden is bekend en actueel	Onbekende afhankelijkheden → ongecontroleerde uitval en ketenproblemen	Onbekende critical dependency of SPOF → bestuurlijke escalatie	
6	Beveiliging cloud en architectuur	Cloud-, netwerk- en platformrisico's periodiek beoordeeld en opgevolgd	Architectuur- of configuratiefouten → verhoogd risico op datalekken en verstoring	Kritiek risico zonder mitigerende maatregel → escalatie naar MT/bestuur	
7	Cryptografie en sleutelbeheer	Cryptografiebeleid en sleutelbeheer geïmplementeerd en periodiek beoordeeld	Onvoldoende cryptografische bescherming → verlies van vertrouwelijkheid en integriteit	Ernstige afwijking in cryptografie of sleutelbeheer → directe bestuurlijke escalatie	

4.4 Driver 4: Identity & Access Management

Effectief Identity & Access Management (IAM) is cruciaal om te waarborgen dat alleen bevoegde personen toegang hebben tot systemen en gegevens. Onjuiste of verouderde rechten vormen een direct risico op datalekken, misbruik en verstoring van de dienstverlening. IAM is daarom een basisvoorwaarde voor digitale veiligheid en continuïteit. Hierbij is het van belang dat de organisatie zorgt voor strikte toegangscontrole en verhoogde eisen hanteert voor systemen die onderdeel zijn van de kroonjuwelen of waarin gevoelige gegevens worden verwerkt. Daarnaast creëert de organisatie een klimaat waarin medewerkers zich veilig voelen om incidenten te melden, ook wanneer hun eigen gedrag daarbij een rol heeft gespeeld.

De bestuurder borgt dat IAM organisatiebreed, actueel en risicogericht is ingericht. Dit betekent sturen op heldere kaders voor identificatie en autorisatie, het verplicht toepassen van sterke authenticatie en het beperken van bijzondere bevoegdheden. Ook veilige (thuis)werkplekken en externe toegang moeten blijvend worden geborgd, evenals het tijdig melden en opvolgen van incidenten en afwijkingen.

De uitwerking door de lijn (ondersteund door de CISO) richt zich vooral op het periodiek beoordelen van toegangsrechten, het beheersen van beheer- en bijzondere bevoegdheden, sterke authenticatie en het aantoonbaar maken van afwijkingen en opvolging daarvan.

Driver 4: Identity & Access Management (IAM)	
Bestuurlijke vragen	**Kern Prestatie Indicatoren (KPI's)**
1. Hebben alleen bevoegde personen toegang tot systemen en gegevens? 2. Zijn toegangsrechten juist, noodzakelijk en actueel?	1. Identiteiten van alle gebruikers zijn betrouwbaar vastgesteld en actueel. 2. Toegangsrechten sluiten aan bij rol, functie en gevoeligheid en worden periodiek beoordeeld.

3. Worden toegangsrechten aangepast bij in-, door- en uitstroom van medewerkers? 4. Zijn beheer- en bijzondere bevoegdheden voldoende ingeperkt en verantwoord? 5. Is sterke authenticatie verplicht toegepast waar dit nodig is? 6. Is externe toegang veilig, tijdelijk en verantwoord ingericht? 7. Voldoen werkplekken en mobiele apparaten aan de eisen voor veilige toegang?	3. Beheer- en bijzondere bevoegdheden zijn beperkt tot noodzakelijke gebruikers en verantwoord vastgelegd. 4. Sterke authenticatie is verplicht toegepast waar vereist. 5. Werkplekken en mobiele apparaten voldoen aan vastgestelde beveiligingseisen voor toegang. 6. Externe toegang is tijdelijk, noodzakelijk en in lijn met vastgestelde voorwaarden.

Uitwerking: Acties voor de lijn (ondersteund door de CISO)

KPI's	Acties / Taken
KPI 1	- Vaststellen van kaders voor identificatie, registratie en beëindiging van identiteiten. - Zorgen voor aantoonbare actualiteit, uniciteit en herleidbaarheid van identiteiten. - Inzicht verschaffen in afwijkingen in identity-registraties en de oplossingsstatus.
KPI 2	- Vaststellen van een organisatiebreed autorisatiekader op basis van rol, functie en gevoeligheid. - Periodiek laten vaststellen van de juistheid van toegangsrechten. - Inzicht verschaffen in vervallen of onnodige toegangsrechten en de opvolging daarvan.
KPI 3	- Vaststellen van wat onder bijzondere en beheerbevoegdheden valt en wie deze mogen hebben. - Periodiek laten beoordelen van de noodzakelijkheid van bijzondere bevoegdheden. - Inzicht geven in afwijkingen in bevoegdheden en de mate van opvolging.
KPI 4	- Vaststellen waar sterke authenticatie verplicht moet zijn. - Aantoonbaar maken dat sterke authenticatie is toegepast op alle relevante systemen. - Inzicht geven in afwijkingen en de opvolging daarvan.
KPI 5	- Vaststellen van beveiligingseisen voor werkplekken en mobiele apparaten. - Aantonen welke werkplekken en apparaten aan deze eisen voldoen. - Inzicht geven in afwijkingen en de status van opvolging.
KPI 6	- Vaststellen van kaders voor veilige, tijdelijke en noodzakelijke externe toegang. - Aantonen dat externe toegang voldoet aan deze kaders. - Inzicht verschaffen in afwijkingen in externe toegang en de opvolging daarvan.

Bestuurlijk sturingskader (KPI-tabel) met daarin opgenomen voorgestelde normen:

KPI	Onderwerp	Norm	Bestuurlijk risico	Escalatiepunt	Status (G/O/R)
1	Betrouwbare en actuele identiteiten	100% van de gebruikersidentiteit en is betrouwbaar vastgesteld, actueel en herleidbaar	Onjuiste of verouderde identiteiten → onbevoegde toegang tot systemen en gegevens	Onverklaarde of niet-beëindigde identiteiten → bestuurlijke escalatie	
2	Juistheid en actualiteit toegangsrechten	100% Toegangs-rechten sluiten aan bij rol, functie en gevoeligheid en worden periodiek beoordeeld	Onnodige of foutieve toegangsrechten → verhoogd risico op misbruik en datalekken	Structurele afwijkingen zonder opvolging → escalatie naar MT/bestuur	
3	Beheer- en bijzondere bevoegdheden	100% van de beheer- en bijzondere bevoegdheden is	Overmatige privileges → verhoogd risico op	Beheerrechten zonder verantwoording of herbeoordeling →	

		beperkt tot noodzakelijke gebruikers en vastgelegd	grootschalige schade of misbruik	directe bestuurlijke escalatie	
4	Sterke authenticatie verplicht toegepast	100% van de systemen waarvoor sterke authenticatie vereist is, maakt hiervan gebruik	Zwakke authenticatie → verhoogde kans op accountmisbruik en datalekken	Afwijkingen bij kritieke systemen → escalatie naar MT/bestuur	
5	Veilige werkplekken en mobiele apparaten	Werkplekken en mobiele apparaten voldoen aan vastgestelde beveiligingseisen	Onveilige eindpunten → ongeautoriseerde toegang en dataverlies	Structurele afwijkingen zonder herstel → bestuurlijke bijsturing	
6	Veilige en tijdelijke externe toegang	100% van de externe toegang is tijdelijk, noodzakelijk en conform vastgestelde kaders	Ongecontroleerde externe toegang → verhoogd risico op inbreuk en datalekken	Externe toegang buiten kaders of zonder einddatum → bestuurlijke escalatie	

4.5 Driver 5: Afscherming, detectie, monitoring en response

Een robuuste beveiligingsarchitectuur vereist dat verstoringen en aanvallen tijdig worden voorkomen, gedetecteerd en opgevolgd. Dit vraagt om adequate afscherming aan de buitenrand en effectieve segmentatie van systeemdomeinen met verschillende risicoprofielen, zodat incidenten zich niet ongehinderd binnen het netwerk kunnen verspreiden. Zonder passende detectie en monitoring bestaat het risico dat dreigingen onopgemerkt blijven, met negatieve gevolgen voor de dienstverlening en continuïteit. Hierbij is het van belang dat de organisatie applicaties met een verhoogd risicoprofiel, waaronder de kroonjuwelen, door middel van segmentatie beschermt om domino-effecten te voorkomen en zorgt voor passende detectie-, monitoring- en responsvoorzieningen (CERT- en SOC-diensten). Daarbij is aandacht voor de continuïteit van de organisatie essentieel.

Bestuurders hebben hierbij de taak om te borgen dat systeemsegmentatie, logging en monitoring structureel op orde zijn. Dit betekent sturen op aansluiting bij Security Operations Center (SOC)- en Computer Emergency Response Team (CERT)-voorzieningen, het opvolgen van hun adviezen en het beschikbaar maken van middelen voor tijdige detectie en adequate response. Ook het stimuleren van meldingsbereidheid en het bewaken van opvolgtijden is een essentieel onderdeel van bestuurlijk toezicht.

De uitwerking door de lijn (ondersteund door de CISO) richt zich vooral op het realiseren van effectieve systeemsegmentatie, volledige logging van kritieke systemen, een goed functionerende SOC/SIEM-omgeving (Security Operations Center en Security Information en Event Managment), de opvolging van CERT-adviezen en het tijdig detecteren en afhandelen van access-gerelateerde afwijkingen en incidenten.

Driver 5: Afscherming, detectie, monitoring en response	
Bestuurlijke vragen	**Kern Prestatie Indicatoren (KPI's)**
1. Hoe voorkomen we verspreiding van verstoringen en aanvallen? 2. Is onze systeemsegmentatie op orde voor kroonjuwelen en ketens?	1. Netwerk- en systeemscheiding is actueel, effectief en aantoonbaar in werking. 2. Kritieke systemen zijn volledig aangesloten op centrale logging en monitoring.

3. Is monitoring volledig en effectief ingericht? 4. Worden systeem-, netwerk- en beveiligingsdreigingen tijdig gedetecteerd en opgevolgd? 5. Worden access-gerelateerde afwijkingen en misbruik tijdig herkend en adequaat afgehandeld?	3. SOC/SIEM-functie is ingericht en operationeel volgens vastgestelde normen. 4. CERT-aansluiting functioneert en adviezen worden tijdig verwerkt. 5. Monitoring- en detectiecapaciteit dekt alle kroonjuwelen en relevante ketenverbindingen. 6. Verbeterplannen voor segmentatie, logging en monitoring worden aantoonbaar uitgevoerd. 7. Afwijkingen, misbruik en incidenten rond access worden gedetecteerd en adequaat afgehandeld.

Uitwerking: Acties voor de lijn (ondersteund door de CISO)

KPI's	**Acties / Taken**
KPI 1	- Segmentatie uitvoeren op basis van BIO2, incl. zones, beveiligingsniveaus en scheiding van toprisico-segmenten. - Ketenverbindingen versleutelen met passende encryptie (TLS/VPN). - Periodiek netwerkconfiguraties scannen op kwetsbaarheden en bevindingen verwerken in verbeterplannen. - Documentatie van segmentatie actueel houden, inclusief logische, fysieke en cloudcomponenten. - Jaarlijkse onafhankelijke toetsing van effectiviteit van segmentatie en toegangsbarrières.
KPI 2	- Dekking van logging bijhouden voor alle kritieke systemen. - Logopslag, transport en vernietiging inrichten conform BIO2. - Kwaliteitsnormen voor logging toepassen (clock synchronisatie, integriteit, volledigheid). - Logbewaartermijnen vastleggen en technisch afdwingen volgens BIO2-eisen. - Controleren of alle kroonjuwelen logging genereren die bruikbaar zijn voor detectie.
KPI 3	- SOC 24/7 inrichten conform NCSC/IBD/CERT-adviezen, inclusief escalatieprocedures. - SIEM-configuratie actualiseren op basis van dreigingsbeeld, IOCs en tactieken. - Use-cases beheren: periodiek reviewen, testen en aanvullen voor o.a. privilege abuse, laterale beweging, datadoorvoer, malware-indicatoren en AI-gedetecteerde anomalieën. - Monitoringcapaciteit uitbreiden voor DDoS-detectie, TLS-analyse, VPN-analyse en netwerkanomalieën. - Responstijden (detectie → triage → actie) meten en tijdig escaleren bij afwijkingen.
KPI 4	- CERT-feed continu monitoren en automatisch integreren in SIEM waar mogelijk. - CERT-adviezen classificeren naar urgentie en impact op de kroonjuwelen. - Patch- en mitigatieprocessen koppelen aan CERT-richtlijnen en security-releasemanagement. - CERT-communicatie testen via periodieke oefening (tabletop en technische oefening). - Overzicht bijhouden van openstaande CERT-acties en rapporteren aan CISO/CIO.
KPI 5	- Detectieregels toepassen op alle zones waarin de kroonjuwelen staan, incl. OT, cloud, SaaS en ketenpartners. - Ketenverbindingen monitoren op afwijkende datapatronen, latency, encryptieproblemen of ongeautoriseerde endpoints. - Integratie met leveranciers en ketenpartners vastleggen (log-uitwisseling, incidentmeldingen, gezamenlijke detectie). - End-to-end zichtbaarheid realiseren van netwerkpad naar kroonjuwelen (flow logs, IDS/IPS, endpoint telemetry). - Periodiek toetsen of elke kroonjuweel een volledig detectieprofiel heeft.
KPI 6	- Gedefinieerde manco's in segmentatie en monitoring in een verbeterplan onderbrengen. - Planning, afhankelijkheden en risico's expliciet maken en voortgang periodiek rapporteren. - Remediatie koppelen aan lifecyclebeheer van infrastructuur en cloudplatformen. - Voor elk verbeterpunt een eigenaar, deadline en acceptatiecriteria vastleggen.

	- Afronding van maatregelen toetsen op effectiviteit (audit, penetratietest, config-controle).
KPI 7	- Verdachte inlogpogingen, afwijkend accountgedrag en signalen van misbruik worden herkend en beoordeeld. - Access-gerelateerde incidenten worden tijdig gemeld en behandeld volgens vastgestelde afspraken. - Afhandeling vindt plaats binnen de daarvoor vastgestelde doorlooptijden. - Trends in meldingsbereidheid, type incidenten en afhandelingstijden worden periodiek gerapporteerd.

Bestuurlijk sturingskader (KPI-tabel) met daarin opgenomen voorgestelde normen:

KPI	Onderwerp	Norm	Bestuurlijk risico	Escalatiepunt	Status (G/O/R)
1	Netwerk- en systeemscheiding	Netwerk- en systeemscheiding is actueel, effectief en aantoonbaar in werking	Onvoldoende segmentatie → snelle verspreiding van aanvallen en verstoring van kroonjuwelen	Kritieke segmentatie-afwijking of falende scheiding → directe bestuurlijke escalatie	
2	Logging van kritieke systemen	100% Kritieke systemen zijn volledig aangesloten op centrale logging en monitoring	Ontbrekende logging → incidenten worden niet of te laat gedetecteerd en onderzocht	Kritiek systeem zonder logging → escalatie naar MT/bestuur	
3	SOC/SIEM-functie operationeel	SOC/SIEM-functie ingericht en operationeel volgens vastgestelde normen	Onvoldoende detectie en respons → langdurige onopgemerkte aanvallen en grotere schade	Structureel niet voldoen aan SOC/SIEM-normen → bestuurlijke bijsturing	
4	CERT-aansluiting en opvolging	CERT-aansluiting functioneert en adviezen worden tijdig verwerkt	Relevante dreigingsinformatie wordt niet benut → verhoogd risico op bekende aanvallen	Niet-opgevolgd urgent CERT-advies → bestuurlijke escalatie	
5	Detectiedekking kroonjuwelen en ketens	100% Monitoring- en detectiecapaciteit dekt alle kroonjuwelen en relevante ketenverbindingen	Beperkte zichtbaarheid → aanvallen op kroonjuwelen blijven onopgemerkt	Kroonjuweel of kritieke ketenverbinding zonder detectiedekking → directe bestuurlijke escalatie	
6	Verbeterplannen segmentatie en monitoring	Verbeterplannen voor segmentatie, logging en monitoring worden uitgevoerd conform planning	Bekende tekortkomingen blijven bestaan → structurele kwetsbaarheden en herhaalde incidenten	Structurele vertraging of ontbrekende besluitvorming → escalatie naar bestuur	
7	Detectie en afhandeling access-incidenten	Afwijkingen, misbruik en incidenten rond access worden tijdig gedetecteerd en afgehandeld	Accountmisbruik blijft onopgemerkt → datalekken en verlies van vertrouwen	Overschrijding vastgestelde afhandeltijden of herhaald misbruik → escalatie naar MT/bestuur	

4.6 Driver 6: Effectief handelen bij incidenten en crisissen

Incidenten en crisissen kunnen de continuïteit van de organisatie ernstig verstoren. Effectief handelen vraagt daarom om betrouwbare back-ups, duidelijke herstelafspraken, een goed georganiseerde crisisstructuur en regelmatig geoefende procedures. Alleen wanneer deze processen aantoonbaar werken, kan de organisatie tijdig reageren op uitval, ransomware of andere ernstige verstoringen. Hierbij is het van belang dat de organisatie zorgt voor betrouwbare back-ups, duidelijke herstelafspraken, een goed georganiseerde crisisstructuur en regelmatig geoefende procedures.

Bestuurders hebben hierbij de verantwoordelijkheid om te borgen dat incident- en crisisbeheer structureel is ingericht, bestuurlijk is vastgesteld en periodiek wordt getest. Zij bepalen de randvoorwaarden, zoals middelen, prioriteiten en besluitvormingskaders, en zien erop toe dat meld- en escalatiemechanismen functioneren in de praktijk.

De uitwerking door de lijn (ondersteund door de CISO) richt zich op het aantoonbaar effectief maken van back-up en herstel, het organiseren en actualiseren van de crisisstructuur, het uitvoeren van realistische oefeningen én het borgen dat meldingen, escalaties en ketenafstemming tijdig plaatsvinden.

Driver 6: Effectief handelen bij incidenten en crisissen	
Bestuurlijke vragen	**Kern Prestatie Indicatoren (KPI's)**
1. Zijn we voorbereid om effectief te handelen bij incidenten en crisissen? 2. Kunnen we onze diensten altijd herstellen, ook bij grote uitval of ransomware? 3. Zijn back-up, uitwijk en continuïteit aantoonbaar geborgd? 4. Zijn meld- en escalatieprocessen bekend en functioneren ze in praktijk?	1. Back-up- en herstelvoorzieningen zijn volledig en aantoonbaar effectief. 2. Continuïteits- en crisisplannen zijn actueel, compleet en bestuurlijk vastgesteld. 3. Oefeningen voor incident- en crisisrespons worden periodiek uitgevoerd en opgevolgd. 4. Meld- en escalatieprocedures functioneren en worden tijdig nageleefd. 5. Ingerichte en operationele afstemming over afhankelijkheden met ketenpartners over meldingen, herstel en continuïteit is geïntegreerd in de crisisprocessen. Deze worden periodiek gezamenlijk getest.

Uitwerking: Acties voor de lijn (ondersteund door de CISO)

KPI's	**Acties / Taken**
KPI 1	- Back-up- en herstelplan actueel houden, inclusief uitwijkmogelijkheden en ransomware-resilience. - Regelmatig hersteltesten uitvoeren voor kritieke systemen, inclusief meetpunten (bijv. hersteltijd, dataverlies). - Scheiding van back-ups waarborgen (offline, immutable of logisch gescheiden). - Afstemming van RTO/RPO met proceseigenaren periodiek herbevestigen en aanpassen waar nodig. - Back-upketen testen: applicatie <> database <>infrastructuur <> ketenpartners.
KPI 2	- Crisisorganisatie organiseren en borgen: rollen, verantwoordelijkheden, bereikbaarheid, escalatie. - Scenario's opnemen voor ICT-uitval, ransomware, afpersing, datadiefstal en uitwijk. - Beleidsuitgangspunten vastleggen voor afpersings- of betaalbeslissingen, vooraf bestuurlijk afgestemd. - Plannen actualiseren na incidenten, nieuwe dreigingen, auditbevindingen of reorganisaties. - Integratie van communicatieplannen (intern, keten, media, openbaar bestuur).

KPI 3	- Jaarlijks tabletop- en technische hersteltesten organiseren voor back-up, uitwijk en crisismanagement. - Realistische ransomware-oefeningen uitvoeren (isolatie, herstel, communicatie, besluitvorming). - Leerpunten direct verwerken in plannen, draaiboeken en procedures. - Betrokkenheid van bestuur en proceseigenaren borgen in scenario's. - Vastleggen van oefenresultaten en rapporteren over verbeterimplementatie.
KPI 4	- Meldplichten borgen (bijv. datalekken, ketenmeldingen, wettelijke verplichtingen). - Interne meldprocedure regelmatig testen en bewustzijn verhogen binnen de organisatie. - Ketenpartners informeren bij relevante incidenten en dreigingen. - Aansluiting op CSIRT/CERT actief gebruiken voor meldingen en dreigingsinformatie. - Escalatielijnen continuïteitstesten (24/7 bereikbaarheid, opvolgingstijd, triage).
KPI 5	- Continuïteitseisen (RTO/RPO) en herstelafspraken afstemmen met ketenpartners en leveranciers. - Ketenbrede herstel- en oefenscenario's organiseren en evalueren. - Afhankelijkheden en uitwijkroutes documenteren, inclusief cloud- en netwerkverbindingen. - Incidentdelen en dreigingsinformatie betrouwbaar en tijdig uitwisselen binnen wettelijke kaders. - Afstemming periodiek toetsen op volledigheid en effectiviteit.

Bestuurlijk sturingskader (KPI-tabel) met daarin opgenomen voorgestelde normen:

KPI	Onderwerp	Norm	Bestuurlijk risico	Escalatiepunt	Status (G/O/R)
1	Back-up- en herstelvoorziening en	Back-up- en herstelvoor-zieningen zijn aantoonbaar effectief voor alle kritieke systemen	Onvoldoende herstelcapaciteit → langdurige uitval van publieke dienstverlening en maatschappelijke ontwrichting	Mislukte hersteltest of onhaalbare RTO/RPO bij kritisch systeem → directe bestuurlijke escalatie	
2	Continuïteits- en crisisplannen	100% Continuïteits- en crisisplannen zijn actueel, compleet en bestuurlijk vastgesteld	Onvoldoende voorbereiding → chaotische besluitvorming en verlies van regie tijdens crisis	Ontbrekende of verouderde plannen → escalatie naar bestuur	
3	Oefeningen incident- en crisisrespons	Incident- en crisisrespons wordt periodiek geoefend en opgevolgd	Ongetrainde organisatie → vertraagde respons en vergrote impact van incidenten	Geen oefening uitgevoerd of leerpunten niet opgevolgd → escalatie naar MT/bestuur	
4	Meld- en escalatieprocessen	Meld- en escalatieprocedures functioneren en worden tijdig nageleefd	Te late of onjuiste meldingen → juridische gevolgen, toezichtmaatregele n en reputatieschade	Overschrijding meldtermijnen of falende escalatie → directe bestuurlijke escalatie	
5	Ketenafstemming bij incidenten en herstel	Afstemming met ketenpartners over meldingen, herstel en continuïteit is ingericht en periodiek getest	Ketenfalen → herstel vertraagt of faalt ondanks interne maatregelen	Ontbrekende of niet-geteste ketenafspraken → bestuurlijke escalatie	

4.7 Driver 7: Meet, leer en stuur bij

Een volwassen beveiligingsorganisatie ontwikkelt zich continu. Dat vraagt om structurele meting van volwassenheid, regelmatige toetsing van processen en gedrag, en het vertalen van leerpunten naar concrete verbeteringen. Door systematisch te meten, te leren en bij te sturen, blijft de organisatie in lijn met veranderende risico's, technologie en ketenafhankelijkheden. De organisatie meet de kwaliteit van securityprocessen met self-assesments. De organisatie houdt alle medewerkers scherp op feitelijk security-gedrag, bijvoorbeeld met behulp van Red teaming. Red teaming is een voorbeeld van een geavanceerde beveiligingstest waarbij een gesimuleerde, realistische aanval wordt uitgevoerd op de systemen, processen en fysieke beveiliging van een organisatie door het rode team. Audits ondersteunen daarbij de verplichting om de opzet, het bestaan en de werking van maatregelen aan te tonen. De organisatie verwerkt bevindingen in het ISMS en zorgt dat de PDCA-cyclus aantoonbaar wordt doorlopen en dat risico's en verbeterpunten structureel met management en bestuur worden gedeeld[10].

Bestuurders borgen dat governance en de PDCA-cyclus effectief functioneren, dat bevindingen worden opgevolgd en dat eigenaarschap is verankerd. Audits helpen daarbij aan te tonen dat beveiligingsmaatregelen werken. Bestuurders zorgen voor duidelijke mandaten, transparante rapportagelijnen en een cultuur waarin leren en verbeteren vanzelfsprekend is. Het risicoregister en het ISMS vormen daarbij de centrale bronnen voor sturing, doordat zij risico's, bevindingen en voortgang van verbetermaatregelen gestructureerd inzichtelijk maken.

Voor het meten van volwassenheid kan gebruik worden gemaakt van verschillende instrumenten, zoals het BIO-Self Assessment (BIO-SA), het Privacy-Self Assessment (PriSA), het NBA-model van NOREA of - voor gemeenten - ENSIA. Veel organisaties beschikken daarnaast over een ISMS-pakket dat relevante vragen al bevat en daarmee als basis voor deze driver kan worden benut.

De uitwerking door de lijn (ondersteund door de CISO) richt zich vooral op het uitvoeren van deze metingen, het analyseren van bevindingen en het vertalen daarvan naar aantoonbare verbeteringen.

Driver 7: Meet, leer en stuur bij	
Bestuurlijke vragen	**Kern Prestatie Indicatoren (KPI's)**
1. Is er een cultuur van eigenaarschap en verantwoord gedrag in de organisatie? 2. Groeien onze beveiligings- en privacyprocessen mee met veranderende risico's? 3. Zijn onze governance en PDCA-cyclus effectief ingericht? 4. Leren we structureel van testen, incidenten en praktijkervaring?	1. Volwassenheid van informatie- en privacybescherming voldoet aan het vereiste niveau en groeit aantoonbaar. 2. Periodieke testen van gedrag, processen en systemen (o.a. phishing en red teaming) worden uitgevoerd en opgevolgd. 3. Management ontvangt structureel inzicht in risico's, bevindingen en leerresultaten uit toetsen en incidenten. 4. Governance, rollen, mandaat en rapportagelijnen zijn helder ingericht en worden nageleefd. 5. De PDCA-cyclus voor IB&P is aantoonbaar doorlopen en leidt tot verbeteringen.

[10] Via de website www.basisbeveiling.nl kan de status achterhaald worden of belangrijke organisaties de digitale basisveiligheid op orde hebben. Dat is noodzakelijk voor beschikbaarheid, integriteit en vertrouwelijkheid van onlinedienstverlening.

	6. Leermiddelen en bewustwording worden aantoonbaar benut door medewerkers en bestuurders. 7. Bestuurder-CISO-gespreksverslag is actueel.

Uitwerking: Acties voor de lijn (ondersteund door de CISO)

KPI's	Acties / Taken
KPI 1	- Jaarlijkse meting van IB-volwassenheid en P-volwassenheid uitvoeren volgens vastgesteld raamwerk. - Maturiteitsdoelen afstemmen met management en opnemen in jaarplan. - Beoordelen of processen meegroeien met risico's, technologische ontwikkelingen en ketenafhankelijkheden. - Gap-analyse uitvoeren en verbetermaatregelen prioriteren voor technische en organisatorische controles. - Meting, bevindingen en verbetermaatregelen vastleggen in het ISMS. - Voortgang periodiek rapporteren aan bestuur en proceseigenaren.
KPI 2	- Phishing-acties en social engineering-campagnes uitvoeren voor verschillende doelgroepen. - Red teaming inzetten om de weerbaarheid van ICT-systemen, processen en menselijk handelen te testen. - Procesmatig testen uitvoeren op key controls en kwetsbare stappen. - Bevindingen klasseren naar ernst en gebruiken voor directe verbetering van processen, techniek en gedrag. - Effectiviteit van verbetermaatregelen later opnieuw toetsen (retest).
KPI 3	- Resultaten van phishing, red teaming en andere toetsen expliciet rapporteren. - Incidenten door menselijke fouten of ontbrekende controles afzonderlijk inzichtelijk maken. - Trends, patronen en terugkerende tekortkomingen signaleren en duiden. - Confronterende leerpunten opnemen in managementrapportages. - Effectiviteit van maatregelen en restrisico's structureel terugkoppelen. - Relevante risico's en bevindingen opnemen in het risicoregister en opvolging borgen via het ISMS.
KPI 4	- Formeel governance-kader borgen: rol CISO, onafhankelijkheid, bevoegdheden. - Mandaat, verantwoordelijkheden en escalatiepaden vastleggen en periodiek toetsen. - Heldere rapportagelijnen richting CIO, bestuur en audit-/risicocomités. - Verantwoordelijkheden voor IB&P beleggen bij proceseigenaren, inclusief risicoacceptatie. - Overzicht bijhouden van overlegstructuren, besluitvorming en actielijsten.
KPI 5	- Jaarplan opstellen met maatregelen, prioriteiten, risico's en KPI's (Plan). - Uitvoering borgen in projecten, beheerprocessen en awarenessprogramma's (Do). - Audits, metingen, testen en incidentanalyses uitvoeren en beoordelen (Check). - Verbetermaatregelen implementeren, risico's herbeoordelen en processen bijstellen (Act). - Resultaten documenteren als bewijslast en input voor volgende cyclus. - Alle stappen van de PDCA-cyclus aantoonbaar vastleggen in het ISMS, inclusief koppeling aan het risicoregister.
KPI 6	- E-learning, workshops, simulaties en instructies aanbieden voor alle functies. - Deelname en voltooiing monitoren en rapporteren. - Aanbod afstemmen op toetsresultaten, risico's en incidentpatronen. - Bewustwording verankeren in onboarding, projectstartups en verandertrajecten. - Effectiviteit van trainingen periodiek evalueren en optimaliseren.
KPI 7	- Vastlegging van besluiten, risico's en prioriteiten. - Risico's actualiseren in het risicoregister en koppelen aan verantwoordelijke proceseigenaren. - Actualisatie en opvolging monitoren via het ISMS. - Tijdige updates richting bestuur en afdelings-MT's.

Bestuurlijk sturingskader (KPI-tabel) met daarin opgenomen voorgestelde normen:

KPI	Onderwerp	Norm	Bestuurlijk risico	Escalatiepunt	Status (G/O/R)
1	Volwassenheid IB & Privacy	Volwassenheid van informatie- en privacybescherming wordt jaarlijks gemeten en groeit aantoonbaar conform vastgestelde doelen	Beveiliging en privacy groeien niet mee met risico's → structurele kwetsbaarheden en bestuurlijke verrassingen	Geen aantoonbare groei of achterblijvende volwassenheid → escalatie naar bestuur	
2	Periodieke testen (phishing, red teaming)	Periodieke testen van gedrag, processen en systemen worden uitgevoerd en opgevolgd	Ongeteste weerbaarheid → schijnveiligheid en verhoogde kans op succesvolle aanvallen	Geen testen uitgevoerd of bevindingen niet opgevolgd → escalatie naar MT/bestuur	
3	Managementinzicht en leerresultaten	Management ontvangt structureel inzicht in risico's, bevindingen en leerresultaten	Bestuur mist zicht op echte risico's → verkeerde prioriteiten en onvoldoende sturing	Structurele rapportage ontbreekt of is onvoldoende → bestuurlijke escalatie	
4	Governance en verantwoordelijkheden	Governance, rollen, mandaat en rapportagelijnen zijn helder ingericht en nageleefd	Onduidelijke verantwoordelijkheden → falende besluitvorming en toezicht	Afwijkingen in governance of mandaat → escalatie naar bestuur	
5	PDCA-cyclus IB&P	PDCA-cyclus voor IB&P is aantoonbaar doorlopen en leidt tot verbeteringen	Geen structurele verbetering → herhaling van incidenten en bevindingen	PDCA niet aantoonbaar of verbeteringen blijven uit → escalatie naar MT/bestuur	
6	Bewustwording en leermiddelen	Leermiddelen en bewustwording worden aantoonbaar benut door medewerkers en bestuurders	Onvoldoende veiligheidsbewustzijn → menselijk falen blijft dominante oorzaak	Structureel lage deelname of effectiviteit → bestuurlijke bijsturing	
7	Bestuurder-CISO-gespreksverslag	Bestuurder-CISO-gespreksverslag is actueel en vastgelegd	Onvoldoende bestuurlijke dialoog → gebrek aan eigenaarschap en regie	Gespreksverslag ontbreekt of is verouderd → verplicht agenderen in bestuursoverleg	

Bijlage 1: Voorbeeld Opdrachtbrieven aan de CISO en de Lijn

Opzet en gebruik van de voorbeeld-opdrachtbrieven

Na het eerste gesprek tussen bestuurder en CISO en de vaststelling van het jaarprioriteitenoverzicht geeft de bestuurder twee formele opdrachten:

Opdracht 1 – aan de CISO

Adviseren, ondersteunen en monitoren

Opdracht 2 – aan de lijn

Verantwoordelijkheid nemen en organiseren / implementeren

Toelichting bij het gebruik van deze voorbeeld-opdrachtbrieven

- Pas de brieven aan aan de eigen organisatie, cultuur en samenwerkingsvorm
- Voeg concrete data, namen en functies toe
- Verstuur beide brieven gelijktijdig
- Overweeg een gezamenlijke kick-off met CISO en MT's om de samenwerking te bespreken
- Maak expliciet dat u als bestuurder beide partijen aanspreekt op hun rol
- Beoordeel of deze schriftelijke opdrachtbrieven nog passend zijn wanneer al is gestart

Hierna volgen voorbeelden van beide opdrachtbrieven.

Brief 1 – Opdracht aan de CISO

Aan: [naam CISO]
Van: [naam bestuurder]
Datum: [datum]

Beste [naam CISO],

Naar aanleiding van ons gesprek op [datum] over de sturing van informatieveiligheid geef ik je hierbij formeel opdracht. In deze opdracht vervul je de rol van coördinator, adviseur en ondersteuner van de organisatie.

Jouw opdracht

Je ondersteunt de organisatie bij het verbeteren van informatieveiligheid door de volgende taken uit te voeren:

1. Ontwikkelen van het dashboard
   - Zet het statusoverzicht om naar een werkbaar KPI-dashboard
   - Zorg dat alle afdelingen met het dashboard kunnen werken
   - Lever periodieke rapportages aan bestuur en directie

2. Adviseren en ondersteunen van de lijn
   - Help afdelings-MT's bij het begrijpen en toepassen van de 7 drivers
   - Adviseer over passende maatregelen en prioriteiten
   - Ondersteun bij het verzamelen en duiden van informatie
   - Deel kennis, expertise en best practices

3. Monitoren en rapporteren

- Monitor de voortgang per afdeling
- Signaleer risico's en knelpunten
- Rapporteer trends en ontwikkelingen
- Adviseer over verbeterpunten

4. Coördineren
   - Organiseer kwartaaloverleggen met de lijn-MT's
   - Faciliteer kennisdeling tussen afdelingen
   - Zorg voor een consistente en uniforme aanpak organisatiebreed
   - Belangrijke aandachtspunten
   - Je bent en blijft adviseur; je draagt geen lijnverantwoordelijkheid
   - De afdelings-MT's nemen zelf de besluiten
   - Escaleer naar mij wanneer MT's hun verantwoordelijkheid niet nemen
   - Wees kritisch, maar constructief in je adviezen

5. Planning
   - Dashboard gereed: [datum]
   - Eerste kwartaalrapportage: [datum]
   - Elk kwartaal: bespreking met het directieteam

Succes met deze opdracht. Ik ben beschikbaar voor overleg wanneer nodig.

Met vriendelijke groet,
[Naam bestuurder]
Bijlage: Concept statusoverzicht KPI's

Brief 2 – Opdracht aan de lijn

Aan: Leden van de afdelings-MT's
Van: [naam bestuurder]
Datum: [datum]

Geachte leden van de afdelings-MT's,

Informatieveiligheid is essentieel voor onze dienstverlening. Als afdelings-MT bent u verantwoordelijk voor informatieveiligheid binnen uw eigen domein. Met deze brief maak ik die verantwoordelijkheid expliciet en geef ik u een concrete opdracht.

Uw verantwoordelijkheid

Als lijnmanagement bent u verantwoordelijk voor:

- Het identificeren van risico's binnen uw domein
- Het nemen van besluiten over maatregelen en prioriteiten
- Het implementeren van informatiebeveiligingsmaatregelen
- Het accepteren van risico's binnen de gestelde kaders

De CISO coördineert, adviseert en ondersteunt u, maar de verantwoordelijkheid en beslissingsbevoegdheid blijven bij u.

Uw opdracht

Concreet vraag ik u om het volgende:

1. Kwartaalupdate van het dashboard
   - Werk elk kwartaal de status van uw afdeling bij
   - Verzamel hiervoor de benodigde informatie
   - Laat u hierbij ondersteunen door de CISO
   - Deadline: binnen één week na afloop van het kwartaal

2. Kwartaalbespreking in uw MT
   - Bespreek de 7 drivers en bijbehorende KPI's
   - Identificeer risico's en knelpunten
   - Bepaal prioriteiten en maatregelen
   - Neem besluiten over de aanpak van verbeteringen

3. Implementatie en opvolging
   - Wijs eigenaren toe aan acties
   - Monitor de voortgang
   - Zorg voor voldoende middelen en tijd
   - Escaleer naar het directieteam bij structurele knelpunten

4. Deelname aan organisatiebreed overleg
   - Neem elk kwartaal deel aan overleg met de CISO en andere MT's
   - Deel ervaringen en leer van elkaar
   - Draag bij aan organisatiebrede samenhang

Ondersteuning die u krijgt

De CISO ondersteunt u met:

- Advies over risico's en maatregelen
- Inhoudelijke kennis van standaarden en best practices
- Ondersteuning bij het verzamelen van informatie
- Monitoring en rapportage
- Coördinatie met andere afdelingen

Beschikbare ondersteuning:

- [Naam CISO] – [e-mail] – [telefoonnummer]
- [Naam IB-adviseur] – [e-mail] – [telefoonnummer]

Verwachtingen

Ik verwacht dat u:

- Deze verantwoordelijkheid serieus neemt
- Voldoende tijd en aandacht besteedt aan informatieveiligheid
- Actief gebruikmaakt van de beschikbare ondersteuning
- Tijdig knelpunten signaleert
- Besluiten neemt en verantwoordelijkheden niet doorschuift naar de CISO

Planning

- Kick-offbijeenkomst: [datum]
- Dashboard operationeel: [datum]
- Eerste kwartaalupdate: [datum]
- Eerste kwartaalbespreking per MT: [datum]

Informatieveiligheid is geen uitsluitend IT-onderwerp, maar een integraal onderdeel van goed management. Ik reken op uw commitment.

Januari 2026

Met vriendelijke groet,
[Naam bestuurder]
CC: CISO, Directieteam