Grip op informatieveilig gedrag

Hulpmiddel 3: bestuurlijke dialoogkaarten

Inleiding ‘Bestuurlijke dialoogkaarten’

Wie, wat, waarom?

Introductie

Deze dialoogkaarten helpen bij het ontwikkelen van een gezamenlijk kompas.
Door middel van stellingen, vragen en dilemma’s helpen de kaarten bij:

- Het helder krijgen van rollen en verantwoordelijkheden;
- Het stellen van prioriteiten;
- Een visie op de rol van gedrag en cultuur;
- Het bespreekbaar maken van verschillende perspectieven en belangen;
- Wederzijds begrip;
- Weten wat je van elkaar mag verwachten als het een keer misgaat.

Voor wie?

De dialoogkaarten zijn te gebruiken in het overleg tussen bestuurder, expert informatieveiligheid en directieleden en voor een dialoog binnen en met de Raad van Toezicht.

Input voor visievorming

De gesprekken met de dialoogkaarten kunnen de basis vormen voor de ontwikkeling van een gedeelde visie op informatieveiligheid en informatieveilig gedrag. Gebruik de opbrengsten uit de dialogen om richtinggevende uitgangspunten en bestuurlijke keuzes vast te leggen en hierover toezichthouders te informeren of raadplegen.

Waarover & hoe?

Niveaus

De dialoogkaarten zijn onderverdeeld in drie volwassenheidsniveaus:

- Starten: voor organisaties die bezig zijn de basis op orde te krijgen
- Groeien: voor organisaties die de basis willen doorontwikkelen
- Verdiepen: voor de gevorderde organisatie die meer diepgang wil

Thema’s dialoogkaarten

- Gedrag & cultuur
- Rollen & verwachtingen
- Leiderschap & voorbeeldgedrag
- Incidenten & leren
- Prioritering & schaarste
- Innovatie & informatieveiligheid
- Toezicht & verantwoording

Gebruik

- Reserveer per overleg 5–10 minuten tijdens het bestuurlijk overleg om een of meerdere dialoogkaarten te bespreken. Hierdoor ontstaat meer bestuurlijke betrokkenheid en betere besluitvorming
- Kies 2–3 dialoogkaarten passend bij het doel van het gesprek of actualiteit van dat moment
- Gebruik een stelling, vraag of dilemma als startpunt voor het gesprek

Gebruik de volgende pagina om je niveau te bepalen

Werken met de dialoogkaarten

Je kunt de dialoogkaarten naar eigen inzicht gebruiken. Kies per overleg één dialoogkaart en bespreek liever één vraag, stelling of dilemma grondig dan alle onderdelen oppervlakkig. Maak de keuze op basis van het doel van het gesprek, een actueel bestuurlijk vraagstuk, risico of besluit. Hieronder geven we een aantal voorbeelden van mogelijke werkvormen.

1

Perspectieven verkennen

*Gebruik een **stelling** om te verkennen in hoeverre er een gedeeld beeld bestaat van hoe te sturen op informatieveiligheid.*

2

Van inzicht naar actie

*Kies een **vraag** en bespreek welke bestuurlijke keuzes, investeringen of afspraken hieruit volgen.*

3

Het dilemma centraal

*Gebruik een **dilemma** om te verkennen welke belangen, risico's en waarden achter de verschillende antwoordmogelijkheden schuilgaan.*

4

De praktijktoets

Koppel een actuele ontwikkeling, innovatie, auditbevinding of incident aan een (onderdeel van een) dialoogkaart. Bespreek of de kaart nieuwe inzichten of handelingsopties oplevert.

Waar staat jullie organisatie nu?

Starten

"Grip op de basisvoorwaarden en beginselen van informatieveilig gedrag"

- Informatieveiligheid komt vooral op tafel bij incidenten of audits
- Er is nog weinig vastgelegd (rollen, afspraken, processen)
- Het gesprek met bestuur is onregelmatig en vaak ad hoc
- Er is beperkt zicht op risico's en prioriteiten

Groeien

"Grip op voortgang en een goede mix tussen mens, proces en techniek."

- Rollen, processen en beleid zijn grotendeels ingericht
- Er is periodiek overleg tussen expert(s) en bestuur
- Er wordt gerapporteerd over voortgang (bijv. KPI's, risico's)
- Het gesprek gaat nog vaak over wat er gebeurt, minder over wat het betekent

Verdiepen

"Grip op besturing en complexe samenwerkings-vraagstukken en waardewegingen."

- Informatieveiligheid is onderdeel van strategie en besluitvorming
- Bestuur en experts voeren een inhoudelijk, gelijkwaardig gesprek
- Keuzes worden gemaakt op basis van risico's, impact en ambitie
- Gedrag, cultuur en eigenaarschap krijgen proactief aandacht

Benut dit overzicht om je volwassenheidsniveau te bepalen

Starten: Gedrag & cultuur

Stelling

“Mensen maken fouten — dat hoort erbij”

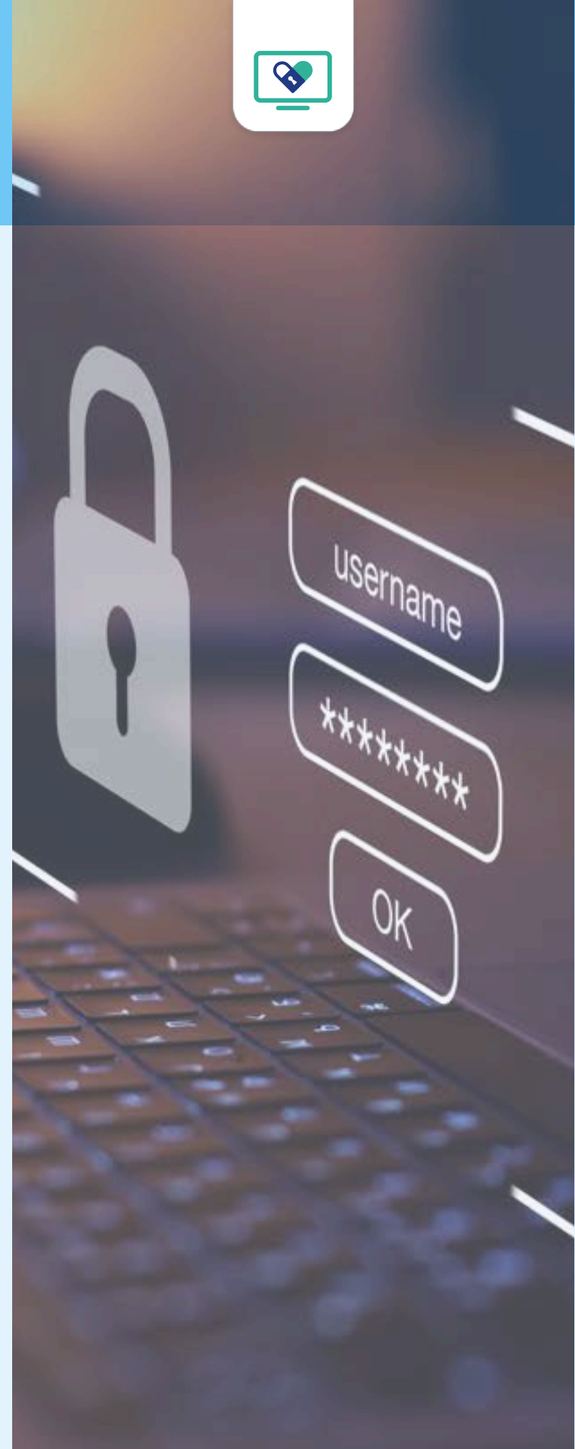
Vragen

1. Kunnen medewerkers informatieveiligheidsincidenten ergens melden en weten zij waar?
2. Melden medewerkers het als ze een fout hebben gemaakt in het omgaan met informatie?
3. Welke reactie op fouten stimuleert veilig gedrag?

Dilemma

Iemand lekt data en meldt dit niet. Wat doen we?

- Aanspreken: We benadrukken regels en verantwoordelijkheid
- Begrijpen: We onderzoeken waarom iemand niet meldt en leggen uit waarom melden belangrijk is
- Verbreden: We bedenken maatregelen als we zien dat dit vaker gebeurt



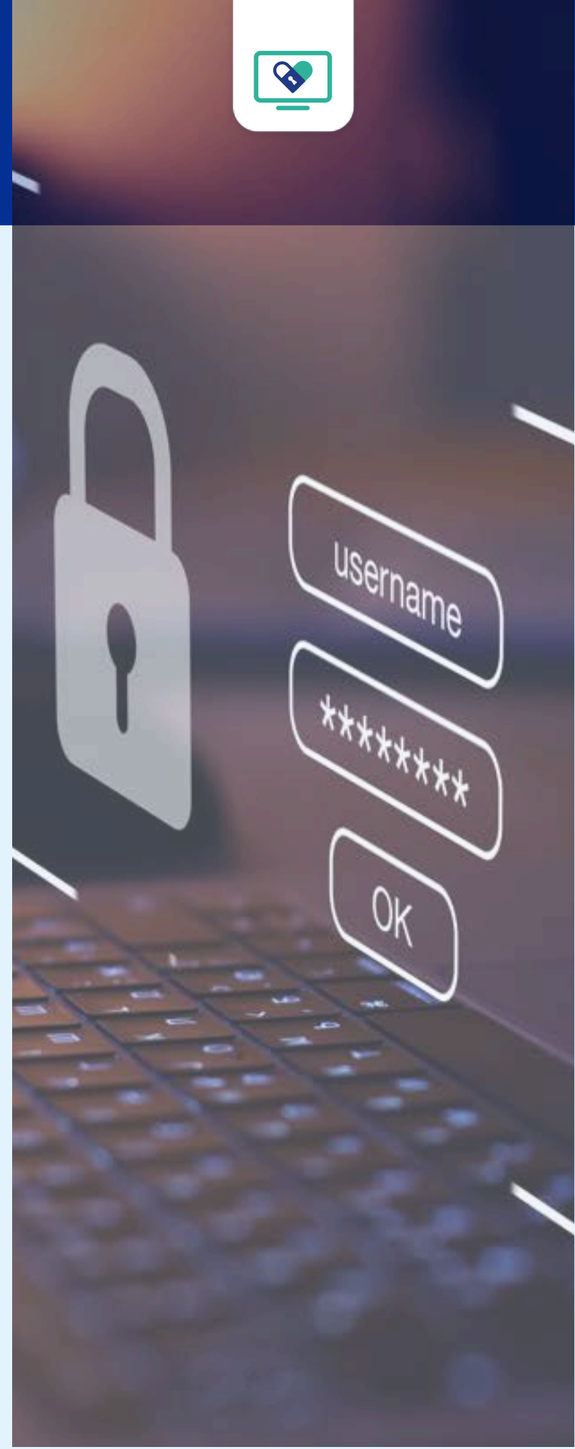
Gebruik de tookit ‘Melden datalek’ voor praktische tips om in actie te komen bij een datalek

Groeien: Gedrag & cultuur

Stelling
“Openheid over fouten helpt ons veiliger te werken”

Vragen
1. Hoe stimuleren we dat mensen incidenten melden?
2. Hoe voorkomen we dat mensen te makkelijk denken over het maken van een fout?
3. Hoe reageren leidinggevenden op fouten van medewerkers?

Dilemma
In een team zijn meerdere meldingen van een datalek, maar het leidt niet tot minder datalekken.
Wat doen we?
- Strakker sturen: Meer aandacht voor werkafspraken, impact en (gedrags)consequenties benoemen
- Teamleren stimuleren: Teams samen laten reflecteren op patronen en verbeteringen als vast agendapunt tijdens een werkoverleg
- Individuele aanpak: Een gesprek per persoon per datalek



Verdiepen: Gedrag & cultuur

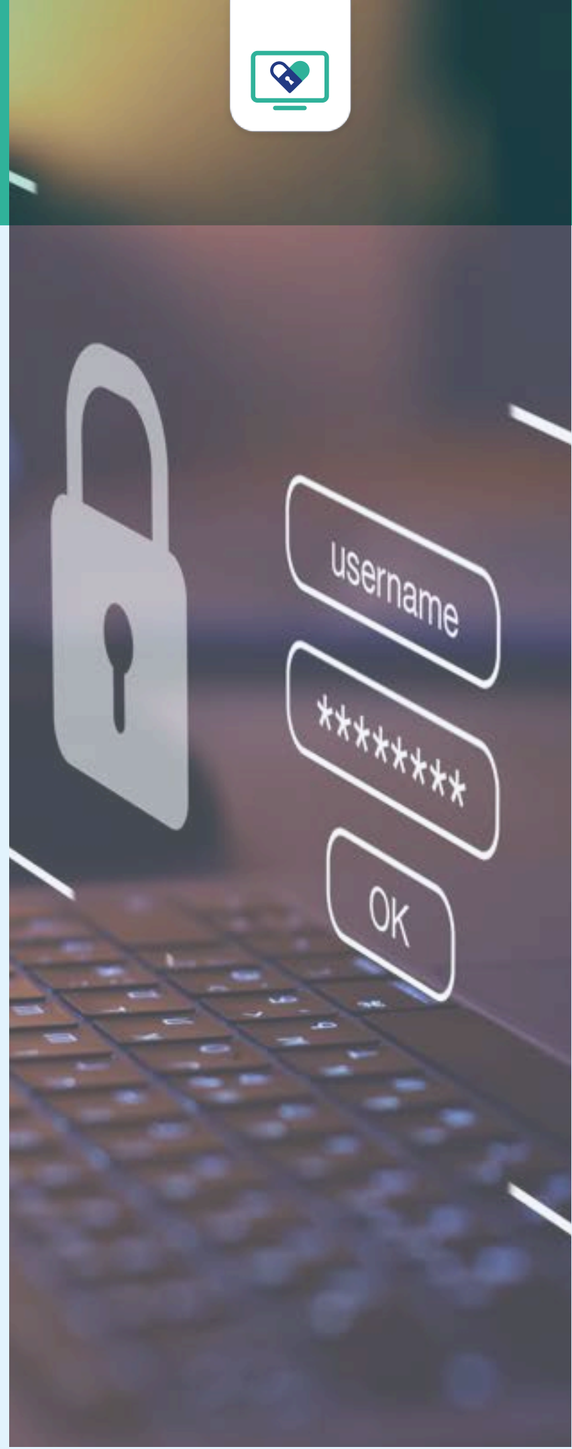
Stelling
“Onze cultuur bepaalt ons veiligheidsniveau”

Vragen

1. Welk gedrag belonen of sanctioneren we impliciet en welk gedrag expliciet?
2. Waar ervaren onze medewerkers spanning tussen veiligheid en andere waarden, zoals werkgeluk, gebruikersgemak en kwaliteit van zorg?
3. Welk voorbeeldgedrag willen we zien van leidinggevenden?

Dilemma
In delen van de organisatie omzeilen medewerkers de veiligheidsafspraken. Zij verdedigen dit gedrag door te zeggen dat het nodig is om goed werk te leveren. Wat doen we?

- Praktijk leidend: Teams krijgen ruimte om in de praktijk eigen afwegingen te maken
- Onderzoeken: We onderzoeken hoe veilig werken beter kan aansluiten op de praktijk
- Normeren: Veiligheid mag nooit zonder goedkeuring aan de kant geschoven worden



Starten: Rollen & verwachtingen

Stelling

“Het is bij ons duidelijk wie waarvoor verantwoordelijk is als het gaat over informatieveiligheid”

Vragen

1. Wie is bij ons verantwoordelijk voor informatieveiligheid?
2. Wat verwachten we van leidinggevenden?
3. Wat verwachten we van de CISO (of andere experts informatieveiligheid) en bestuurder(s)?

Dilemma

We zien dat medewerkers twijfelen of afwachten bij signalen van onveilig werken. Wat doen we?

- Aanspreken: We maken duidelijk waarom medewerkers elkaar actief moeten aanspreken
- Verduidelijken: We maken scherper waarom informatieveiligheid belangrijk is en wat we van medewerkers verwachten
- Ondersteunen: We helpen medewerkers om signalen bespreekbaar te maken

Groeien: Rollen & verwachtingen

Stelling

“Duidelijke verantwoordelijkheden leiden niet vanzelf tot goede samenwerking”

Vragen

1. Wat mogen we als bestuur en expert informatieveiligheid van elkaar verwachten (in het bestuurlijke gesprek)?
2. Wanneer schuurt het in onze samenwerking en hoe gaan we daar dan mee om?
3. Wat verwachten we van directieleden, managers en toezichthouders?

Dilemma

De expert informatieveiligheid geeft een negatief advies op basis van een risico-analyse, maar de bestuurder geeft prioriteit aan andere organisatiedoelen en legt het advies terzijde. Wat doen we?

- Veiligheid benadrukken: De expert informatieveiligheid blijft in beginsel actief aandacht vragen voor de risico’s
- Samen wegen: We investeren in een gezamenlijke weging en streven naar een gedeeld besluit
- Bestuurlijk besluiten: De bestuurder bepaalt welke prioriteiten voorrang krijgen en meldt dit bij toezichthouders

Deze kaart is ook geschikt voor toezichthouders

Verdiepen: Rollen & verwachtingen

Stelling

“Volwassen samenwerking vraagt om een duidelijke scheiding van uitvoeren, adviseren en besluiten”

Vragen

1. Wanneer is tegenspraak gewenst en wanneer wordt de expert informatieveiligheid te sturend?
2. Wanneer is een bestuurder voldoende betrokken op informatieveiligheid en wanneer wordt het micro-managen?
3. Hoe voorkomen we frustratie in de samenwerking?

Dilemma

De bestuurder raakt steeds meer betrokken bij inhoudelijke veiligheidsmaatregelen, terwijl de expert informatieveiligheid zich steeds nadrukkelijker uitspreekt over bestuurlijke keuzes. Wat doen we?

- Koesteren: Dit duidt op gedeeld eigenaarschap en begrip voor elkaars perspectief
- Rollen herijken: We herijken werkafspraken met daarbij mogelijk enige overlap in rollen
- Duidelijker begrenzen: Bestuurder en expert blijven strikt binnen hun eigen rol

Deze kaart is ook geschikt voor toezichthouders

Starten: Innovatie & informatieveiligheid

Stelling

“Informatieveiligheid en innovatie zitten elkaar soms in de weg”

Vragen

1. Hoe besteden we op dit moment aandacht aan informatieveiligheid bij innovatietrajecten?
2. Wanneer ervaren we dat de aandacht voor veiligheid innovatie vertraagt? Hoe kunnen we dat voorkomen?
3. Wie betrekt experts informatieveiligheid tijdens innovatietrajecten? En op welk moment?

Dilemma

Een team wil snel starten met een nieuwe AI-tool na positieve geluiden vanuit een andere organisatie.
Wat doen we?

- Toestaan: We laten het team starten en zien gaandeweg wat er nodig is.
- Beperken: We stellen minimale regels en laten het team dan experimenteren.
- Aanhouden: We moeten eerst beleid maken op AI en informatieveiligheid en daarna bepalen of deze tool binnen dit beleid past.

Groeien: Innovatie & informatieveiligheid

Stelling
“Informatieveiligheid moet innovatie ondersteunen, niet blokkeren”

Vragen

1. Hoe zorgen we dat innovaties snel én verantwoord kunnen starten?
2. Wanneer wordt informatieveiligheid een rem op innovatie en wanneer juist een versneller?
3. Wie maakt uiteindelijk de afweging tussen experimenteren en beheersen?

Dilemma
Een AI-toepassing lijkt veelbelovend voor de praktijk en sluit aan bij organisatiedoelen. Tegelijk weten we nog niet goed hoe betrouwbaar de leverancier is en hoe we medewerkers veilig met de toepassing laten werken. Wat doen we?

- Starten: We beginnen klein en monitoren actief
- Voorbereiden: We onderzoeken eerst leverancier, risico’s en begeleiding
- Uitstellen: We starten pas als landelijke richtlijnen of intern beleid verder zijn uitgewerkt

Verdiepen: Innovatie & informatieveiligheid

Stelling

“Informatieveiligheid versterkt innovatie”

Vragen

1. Hoe maken we innovatie tot een kans en versterker van informatieveiligheid?
2. Onder welke voorwaarden accepteren we bewust de risico’s van een innovatie?
3. Hoe borgen we in processen dat we onze keuzes goed kunnen uitleggen en verantwoorden?

Dilemma

Een AI-assistent verlaagt werkdruk sterk, maar kan niet risicoloos worden doorgevoerd. Toch besluiten we deze AI-assistent te gaan implementeren. Wat doen we?

- Extra investeren in monitoring: lerend evalueren en kort-cyclisch rapporteren
- Extra investeren in stakeholdermanagement: we benoemen dit in de rapportage aan de Raad van Toezicht en zorgen dat het voltallige directieteam achter dit besluit staat
- Extra investeren in verantwoording: we leggen ons besluit met de afwegingen grondig vast

Deze kaart is ook geschikt voor toezichthouders

Starten: Leiderschap & voorbeeldgedrag

Stelling
“Medewerkers kijken vooral naar het gedrag van leidinggevenden om hun eigen gedrag te verdedigen”

Vragen

1. Welk voorbeeldgedrag willen we zien van leidinggevenden?
2. Wanneer geven leidinggevenden onbedoeld een verkeerd signaal af?
3. Hoe maken we informatieveiligheid zichtbaar in het dagelijks werk?

Dilemma
Een team gebruikt tijdelijk een AI-chatbot die volgens de werkafspraken eigenlijk niet gebruikt mag worden. Het team geeft aan hierdoor sneller te kunnen werken en een belangrijke deadline te halen. Wat doen we?

- Gedogen: In uitzonderlijke situaties moet dit soms kunnen
- Samen bespreken: We onderzoeken waarom teams afwijken van afspraken
- Norm stellen: Teams en leidinggevenden horen werkafspraken consequent te volgen

Groeien: Leiderschap & voorbeeldgedrag

Stelling
“Voorbeeldgedrag van leiders bepaalt hoe serieus we informatieveiligheid nemen”

Vragen

1. Hoe krijgen we zicht op het voorbeeldgedrag van leidinggevenden?
2. Waar zit spanning tussen sturen op resultaat en sturen op veiligheid?
3. Hoe maken leidinggevenden veilig gedrag bespreekbaar in teams?

Dilemma
Een leidinggevende omzeilt werkafspraken ‘om het werk gedaan te krijgen’. Onder welke voorwaarden is dit acceptabel?

- Gezamenlijk gedragen: het team en de leidinggevende van de leidinggevende steunen de keuze
- Uitlegbaar: De afweging en risico’s zijn expliciet gemaakt
- Niet acceptabel: Leidinggevenden geven altijd het goede voorbeeld

Verdiepen: Leiderschap & voorbeeldgedrag

Stelling

“Goed leiderschap vraagt ook onder externe druk om duidelijke keuzes en voorbeeldgedrag”

Vragen

1. Welke waarden wegen het zwaarst in bestuurlijke afwegingen?
2. Hoe gaan we om met druk vanuit regionale samenwerking of ketenpartners?
3. Wanneer mag onze organisatie afwijken van eigen kaders of beleid?

Dilemma

Een bestuurder staat onder druk om mee te doen aan een regionale pilot voor gegevensuitwisseling. Hiervoor moet de organisatie afwijken van onderdelen van het eigen veiligheidsbeleid. Wat doen we?

- Meebewegen: Regionale samenwerking en innovatie krijgen prioriteit
- Regionaal leiderschap: Sturen op adoptie van ons beleid in de regio
- Grenzen stellen: We houden vast aan eigen kaders en beleid

Deze kaart is ook geschikt voor toezichthouders

Starten: Incidenten & leren

Stelling

“Als er iets misgaat, willen we het vooral snel oplossen”

Vragen

1. Wat doen we als er een incident plaatsvindt?
2. Wie moeten we altijd bij een incident betrekken?
3. Wanneer vinden we een incident echt opgelost?

Dilemma

Een incident is opgelost en de impact lijkt beperkt. Wat is de volgende stap?

- Afronden: We sluiten het incident af en gaan verder
- Intern bespreken: We bespreken wat we hiervan kunnen leren binnen het betrokken team
- Breder leren: We delen lessen actief met andere teams, locaties of externe partners

Groeien: Incidenten & leren

Stelling

“Terugkerende incidenten vragen om forse investeringen”

Vragen

1. Welke patronen zien we terug in incidenten?
2. Wat maakt het lastig om echt te veranderen op basis van incidenten?
3. Hoe bespreken we incidenten zonder direct schuldigen te zoeken?

Dilemma

Na het doorvoeren van verbetermaatregelen, is het aantal datalekken gehalveerd. Maar diverse medewerkers blijven het onveilige gedrag vertonen. Wat vraagt dit?

- Gerichter ingrijpen: We investeren in het aanpakken van het gedrag van de ‘achterblijvers’ en kijken naar wat teams van elkaar kunnen leren
- Herontwerpen: We onderzoeken of processen, systemen of verantwoordelijkheden fundamenteel anders moeten
- Accepteren: We erkennen dat je nooit alle medewerkers tot veilig gedrag kan bewegen.

Deze kaart is ook geschikt voor toezichthouders

Verdiepen: Incidenten & leren

Stelling

“Een lerende organisatie bespreekt kwetsbaarheden intern en extern - ook als daar nog geen oplossing voor is”

Vragen

1. Is onze governance en organisatiecultuur voldoende ingericht op permanent leren en verbeteren?
2. Wat willen we uitstralen in hoe we intern en extern handelen bij een incident?
3. Hoe zorgen we dat bestuur en toezicht actief leren van incidenten?

Dilemma

Incidenten ontstaan steeds vaker door afhankelijkheden in de regio, leverancierssketen of samenwerking met andere organisaties. Wat betekent dat voor onze lerende aanpak?

- Eigen organisatie versterken: We richten ons vooral op verbetering binnen de eigen organisatie
- Samen leren: We bespreken incidenten actief met ketenpartners en regionale samenwerkingen
- Samen organiseren: We investeren in een gezamenlijke aanpak van informatieveilig gedrag en investeren daar collectief in

Deze kaart is ook geschikt voor toezichthouders

Starten: Toezicht & verantwoording

Stelling

“Toezicht op informatieveiligheid ontstaat vaak pas bij incidenten of externe druk”

Vragen

1. Hoe informeren we toezichthouders en andere externe partijen over informatieveiligheid?
2. Wanneer informeren we tussentijds en wanneer gebruiken we de reguliere momenten voor verantwoording?
3. Welke informatie helpt toezichthouders om hun rol goed te vervullen?

Dilemma

Er lijkt sprake van een datalek, maar er is nog geen volledig beeld van oorzaak, impact en beheersing.
Wat doen we?

- Direct informeren: We brengen toezichthouders, patiënten of andere externe stakeholders vroegtijdig op de hoogte vanuit de kennis dat melden bij Autoriteit Persoonsgegevens verplicht is
- Eerst duiden: We informeren zodra oorzaak en impact beter in beeld zijn
- Alleen rapporteren: We bespreken dit bij de eerstvolgende reguliere rapportage

Groeien: Toezicht & verantwoording

Stelling

“Goed toezicht vraagt meer dan rapportages alleen”

Vragen

1. Hoe zorgen we dat toezichthouders en andere relevante externe partijen niet alleen cijfers zien, maar ook dilemma’s begrijpen?
2. Welke onderwerpen vragen om dialoog - naast rapportage?
3. Hoe bespreken we risico’s, onzekerheden en afwegingen met toezichthouders en externe stakeholders?

Dilemma

Directie en experts signaleren toenemende verschillen in de veiligheidscultuur tussen teams en hebben de indruk dat sommige leidinggevenden de werkafspraken minder strikt toepassen. Harde incidenten of KPI-afwijkingen zijn er nog niet. Wat doen we?

- Meenemen in reguliere rapportage: We benoemen de signalen kort in de voortgangsrapportage
- Verdiepende dialoog voeren: De signalen zijn aanleiding voor dialoog met toezichthouders
- Eerst verder duiden: We onderzoeken of de signalen wijzen op een structureel risico voordat we toezichthouders actief meenemen

Deze kaart is ook geschikt voor toezichthouders

Verdiepen: Toezicht & verantwoording

Stelling

“Volwassen toezicht vraagt om openheid over dilemma’s, onzekerheden en bewuste risico’s”

Vragen

1. Welke risico’s en dilemma’s vragen om actieve betrokkenheid van toezichthouders?
2. Hoe zorgen we dat toezicht niet alleen terugkijkt, maar ook helpt bij strategische keuzes?
3. Hoe expliciet zijn we over de risico’s die we bewust accepteren?

Dilemma

De organisatie wil versnellen op regionale samenwerking en gegevensuitwisseling. Bestuur en experts zien strategische kansen, maar weten ook dat niet alle risico’s volledig beheerst kunnen worden. Wat doen we?

- Actief meenemen: We betrekken toezichthouders vroegtijdig bij dilemma’s, onzekerheden en afwegingen
- Randvoorwaarden afspreken: We spreken met toezichthouders expliciet af welke risico’s acceptabel zijn en hoe we monitoren
- Beheersing centraal: We wachten met verdere stappen tot risico’s beter beheerst zijn

Deze kaart is ook geschikt voor toezichthouders

Starten: Prioritering & schaarste

Stelling
“Niet alles wat belangrijk is, kan tegelijk aandacht krijgen”

Vragen

1. Hoe bepalen we wat als eerste aandacht krijgt?
2. Wat moet minimaal op orde zijn op het gebied van informatieveiligheid?
3. Hoe en met wie bespreken we keuzes rondom veiligheid?

Dilemma
De organisatie weet dat medewerkers veiliger moeten werken, maar heeft onvoldoende tijd om alle teams tegelijk te ondersteunen. Wat doen we?

- Praktisch kiezen: We beginnen bij teams waar de grootste problemen zichtbaar zijn
- Risicogericht kiezen: We starten bij processen met de grootste impact op zorg en continuïteit
- Plan voor iedereen: We maken een planning zodat alle teams stap voor stap meegenomen worden

Groeien: Prioritering & schaarste

Stelling

“Het is verstandiger om enkele grote risico's goed aan te pakken dan te kiezen voor laaghangend fruit met beperkte impact”

Vragen

1. Welke organisatiedoelen zetten druk op informatieveiligheid?
2. Hoe expliciet maken we keuzes tussen veiligheid, werkdruk en innovatie?
3. Wanneer accepteren we tijdelijk verhoogde risico’s?

Dilemma

Door personeelstekorten en hoge werkdruk stellen diverse gezaghebbende collega’s voor om verbetermaatregelen voor informatieveiligheid opnieuw uit te stellen. Wat doen we?

- Balans zoeken: We zoeken naar verbeteringen die werkdruk én veiligheid ondersteunen
- Veiligheid prioriteren: We stellen andere organisatieontwikkelingen tijdelijk uit
- Risico accepteren: We accepteren tijdelijk hogere risico’s om de organisatie draaiende te houden

Deze kaart is ook geschikt voor toezichthouders

Verdiepen: Prioritering & schaarste

Stelling

"Door de steeds grotere afhankelijkheid van informatie, moeten we meer én gerichter gaan investeren in informatieveiligheid"

Vragen

1. Van welke leveranciers, systemen of samenwerkingen zijn we kritisch afhankelijk?
2. Welke risico's ontstaan door beperkte capaciteit, afhankelijkheden of regionale druk?
3. Welke afhankelijkheden vragen om gezamenlijke afspraken en investeringen, omdat we ze niet alleen kunnen beheersen?

Dilemma

Een kritieke leverancier of regionale voorziening voldoet niet volledig aan de eigen veiligheidsnormen, maar overstappen is nauwelijks haalbaar. Wat doen we?

- Eigen regie versterken: We investeren extra in monitoring, crisisvoorbereiding en eigen beheersmaatregelen
- Samen verbeteren: We zoeken gezamenlijk naar betere afspraken en voorzieningen
- Afhankelijkheid accepteren: We accepteren dat volledige controle en onafhankelijkheid niet realistisch zijn

Deze kaart is ook geschikt voor toezichthouders

Grip op informatieveilig gedrag

Aanvulling op hulpmiddel 3: Dialoogkaarten voor toezichthouders

Inleiding ‘Dialoogkaarten voor toezichthouders’

Wie, wat waarom?

Ook toezichthouders spelen een belangrijke rol in de digitale weerbaarheid van organisaties. Informatieveiligheid raakt direct aan de continuïteit van zorg, de kwaliteit van dienstverlening en de bestuurlijke verantwoordelijkheid. In de praktijk roept dit vragen op. Welke rol heb je als toezichthouder bij informatieveiligheid? Welke vragen kun en moet je stellen? Hoe houd je toezicht zonder op de stoel van het bestuur te gaan zitten? En hoe zorg je voor een goede samenwerking tussen Raad van Toezicht, bestuurder en expert informatieveiligheid?

Om deze gesprekken te ondersteunen zijn dialoogkaarten ontwikkeld over toezicht op informatieveiligheid. Deze vormen een aanvulling op de bestuurlijke dialoogkaarten en ondersteunen het gesprek tussen Raad van Toezicht, bestuurder en expert informatieveiligheid over risico’s, dilemma’s, governance, digitale weerbaarheid en bestuurlijke afwegingen.

Gebruik de dialoogkaarten op een manier die past bij het doel van het gesprek. Kies per overleg één kaart en bespreek liever één stelling, vraag of dilemma grondig dan alle onderdelen oppervlakkig. Laat de keuze aansluiten bij een actueel toezichtsvraagstuk, risico, incident of besluit. Hieronder staan enkele voorbeelden van mogelijke werkvormen.

Waarover en hoe?

Thema’s dialoogkaarten voor toezichthouders

- Het informeren van toezichthouders over informatieveiligheid
- Risicobereidheid & risico-afwegingen
- Incidenten, crisis & publieke verantwoording
- Kennis, deskundigheid & ontwikkeling

Over het gebruik van deze kaarten

- In de auditcommissie;
- Tijdens themabesprekingen over (informatie)veiligheid;
- Als reflectiemoment tussen Raad van Toezicht, bestuurder en experts informatieveiligheid.

Mogelijke werkvormen

- **Gedeeld beeld verkennen:** Gebruik een **stelling** om te verkennen in hoeverre binnen de Raad van Toezicht een gedeeld beeld bestaat over risico's, verantwoordelijkheden en prioriteiten.
- **Kritisch gesprek:** Kies één **vraag** van de kaart en bespreek welke aanvullende informatie, duiding of assurance nodig is om goed toezicht te kunnen houden.
- **Het dilemma centraal:** Gebruik uitsluitend het **dilemma**. Verken welke belangen, risico's en waarden een rol spelen en welke vragen dit oproept richting bestuurder of organisatie.

Deze kaarten zijn niet volwassenheidsniveau-afhankelijk

Dialoogkaart voor toezichthouders

Stelling

"Juist tijdens incidenten en crises moet duidelijk zijn wat toezichthouders van bestuur mogen verwachten"

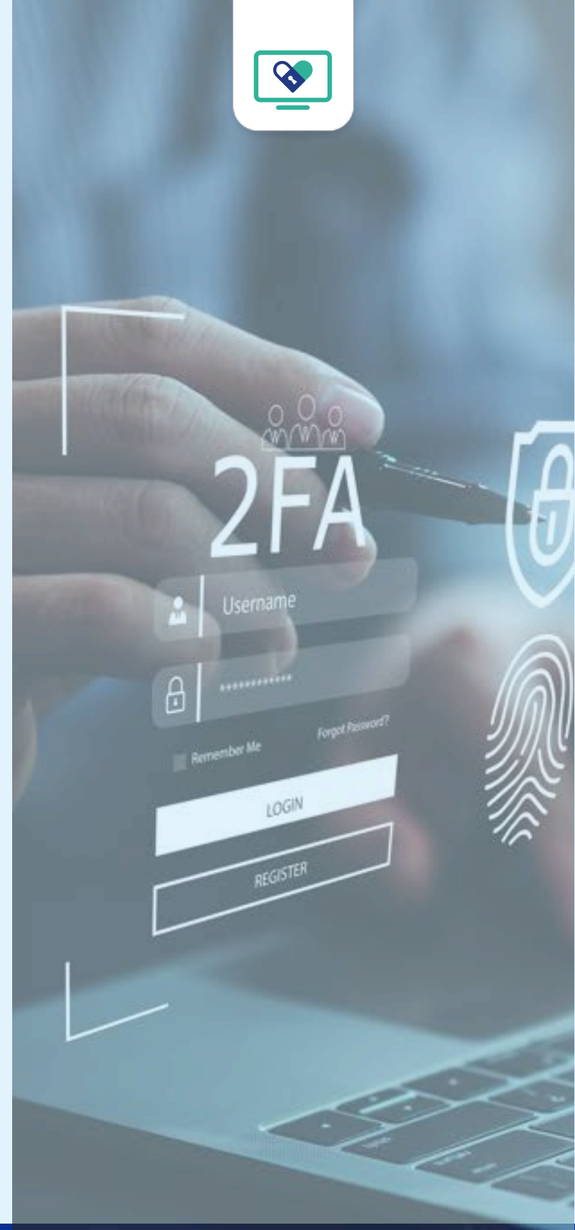
Vragen

1. Wanneer verwachten toezichthouders actief geïnformeerd te worden bij incidenten?
2. Welke rol wil de Raad van Toezicht spelen tijdens een crisis?
3. Wat is onze communicatiestrategie bij incidenten?

Dilemma

Tijdens een groot incident ontstaat maatschappelijke en regionale druk om snel duidelijkheid te geven, terwijl nog veel onzeker is. Wat doet de Raad van Toezicht?

- Bestuur ruimte geven: We vertrouwen op het crisisteam en de bestuurlijke aanpak
- Actief betrokken zijn: We zoeken actief afstemming met bestuur over keuzes en communicatie
- Interveniëren: We vragen indien nodig aanvullende maatregelen, externe ondersteuning of zetten in op extra toezicht



Het informeren van toezichthouders

Dialoogkaart voor toezichthouders

Stelling

“Toezicht op informatieveiligheid vraagt expliciete gesprekken over risicobereidheid, afhankelijkheden en strategische keuzes”

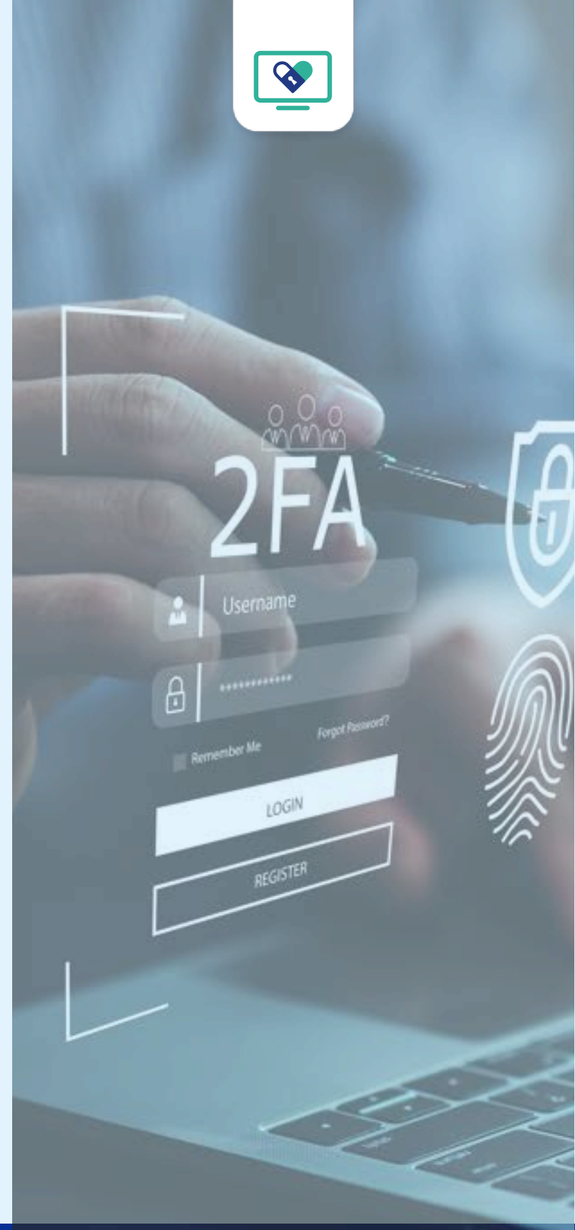
Vragen

1. Welke risico’s accepteert de organisatie bewust?
2. Hoe expliciet is de Raad van Toezicht betrokken bij strategische risico-afwegingen?
3. Wanneer wordt risicobereidheid onderdeel van strategie?

Dilemma

Een regionale samenwerking biedt grote strategische kansen, maar verhoogt ook structureel de afhankelijkheid en risico’s rond informatieveiligheid. Wat is de rol van de Raad van Toezicht?

- Beperkte rol: Pas als risico’s in strijd zijn met wettelijke normen, dient de raad geïnformeerd te worden
- Steunen: De bestuurder steunen nadat kritische vragen naar tevredenheid zijn beantwoord
- Kritische vriend: Kritisch bevragen en monitoren of maatregelen een goede balans bevatten van mens, techniek en proces



Risicobereidheid & risico-afwegingen

Dialoogkaart voor toezichthouders

Stelling

“Toezicht op informatieveiligheid gaat ook over cultuur, gedrag en risicobewustzijn”

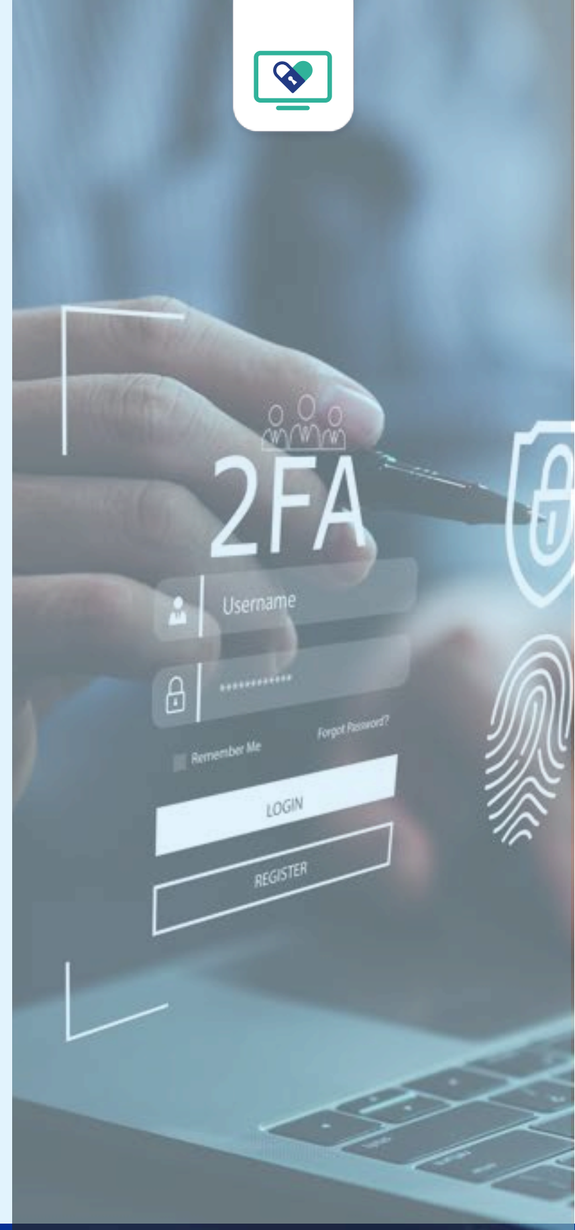
Vragen

1. Hoe bespreekbaar zijn risico’s en incidenten binnen de organisatie?
2. Hoe wordt omgegaan met signalen of slecht nieuws?
3. Hoe weet de Raad van Toezicht of de organisatie daadwerkelijk leert en verbetert?

Dilemma

Een bekend risico is nog niet opgelost, maar wordt bewust geaccepteerd vanwege strategische keuzes.

- De Raad van Toezicht accepteert deze afweging mits goed onderbouwd
- De Raad van Toezicht vraagt om aanvullende beheersmaatregelen
- De Raad van Toezicht vraagt om heroverweging van de strategische keuze



Incidenten, crisis & publieke verantwoording

Stelling

“Toezicht op informatieveiligheid vraagt kennis van technische trends, wet- en regelgeving en gedragsvraagstukken informatieveiligheid om de juiste vragen te stellen”

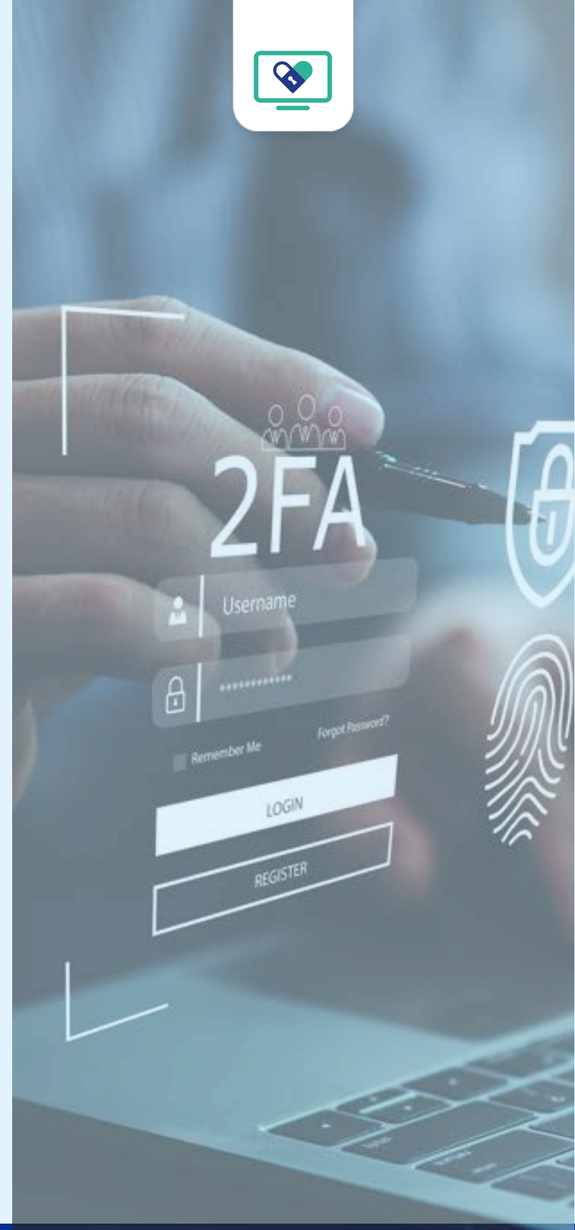
Vragen

1. Welke kennis hebben bestuurders en toezichthouders nodig om hun rol goed te vervullen?
2. Hoe blijven bestuur en toezicht voldoende op de hoogte van relevante ontwikkelingen?
3. Wanneer is externe deskundigheid of scholing nodig?

Dilemma

De organisatie staat voor complexe keuzes rond digitalisering en cyberveiligheid, terwijl bestuurders en toezichthouders beperkte kennis van informatieveiligheid hebben. Wat is gewenst?

- Vertrouwen op experts: We vertrouwen op rapportages en interne deskundigen
- Kennis versterken: Bestuurders en toezichthouders investeren actief in scholing en gezamenlijke verdieping
- Expertise organiseren: We voegen structureel extra deskundigheid toe aan bestuur, commissies of toezicht



Kennis, deskundigheid & ontwikkeling