

**TERUGBLIK**

---



WEBINAR DONDERDAG 6 FEBRUARI 2025

# Risicomangement en BIO2

**key2control**

Heb je vragen over het webinar, de normenkaders of onze aanpak?

Neem contact op met:

**Bart Suers**  
Directeur Key2Control  
+31 (0)6 52 451 450

[e-mail ►](#)



**Gerrit Goud**  
Senior Consultant  
+31 (0)6 5433 5164

[e-mail ►](#)



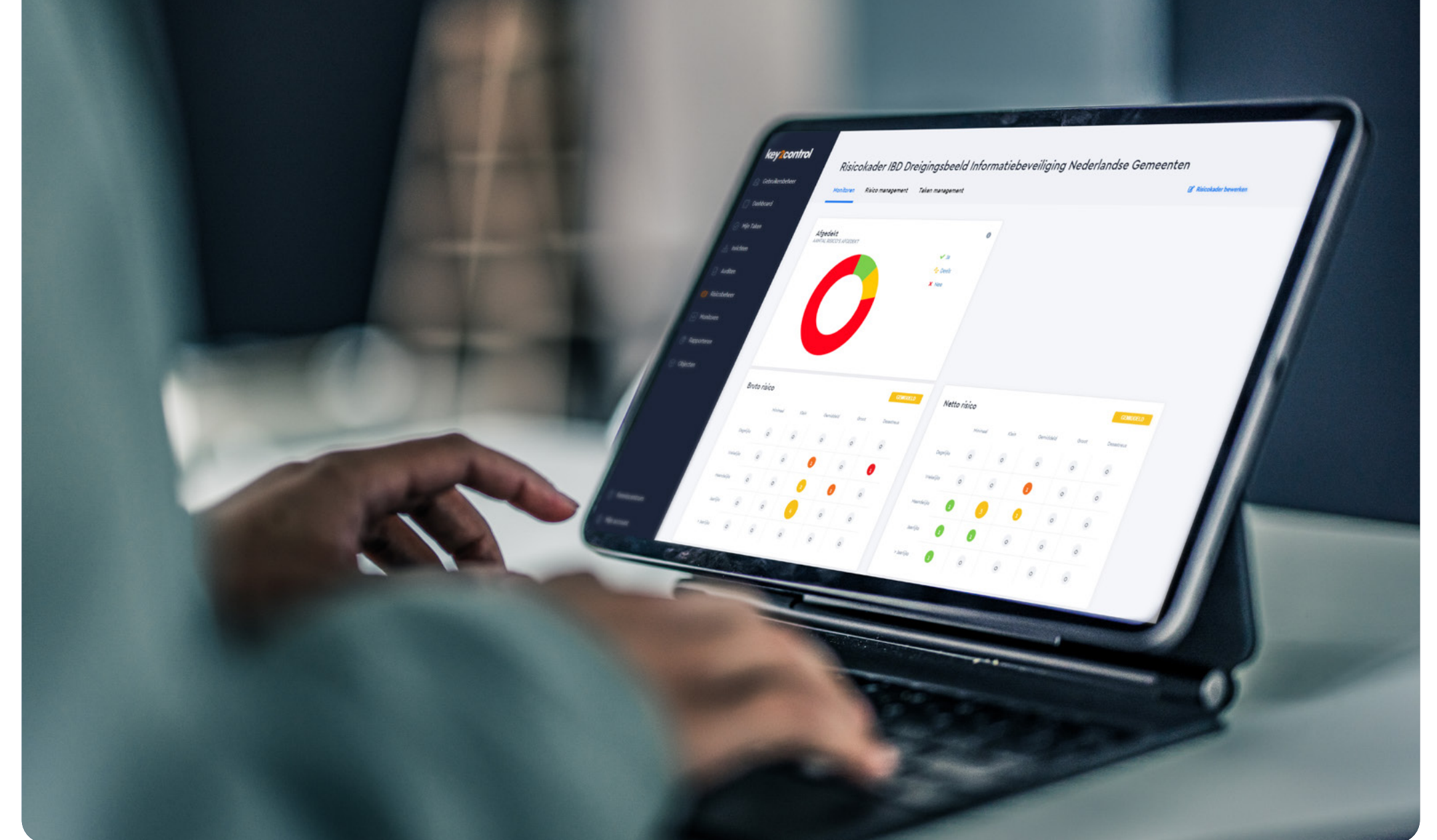
# Waarom is aandacht voor risicomanagement en de BIO2 van belang?

- BIO2 introduceert aangescherpte kaders voor informatieveiligheid, waardoor overheidsorganisaties hun werkwijze moeten aanpassen om te voldoen aan de ENSIA-audit 2025.
- Een werkend ISMS is voor lokale overheden verplicht met de komst van de nieuwe BIO2, waarbij er wordt uitgegaan van de NEN-EN-ISO/IEC 20071 norm.

## RESULTAAT

Een effectieve implementatie van de nieuwe BIO2 leidt tot een verbeterde informatiebeveiliging en risicobeheersing.

# Waarom toetsbare normenkaders in de Key2Control software?



- **Borging van kennis op één centrale plek**
  - > Gemotiveerd inzicht in de mate van beheersing en de wijze van verbetering.
- **Normenkaders zijn toekomstbestendig en stabiel**
  - > Normenkaders beschrijven de 'wat-vraag': aan welke eisen moet je voldoen? In tegenstelling tot het beschrijven van processen. Werkprocessen zijn veel dynamischer. Dat betekent dat wanneer binnen de organisatie iets verandert, de werkprocessen mee moeten veranderen. Dit heeft betrekking op de 'hoe-vraag': op welke manier voldoet de organisatie aan de eisen?
- **Gestandaardiseerde aanpak**
  - > Alle normenkaders zijn op dezelfde manier opgebouwd.
  - > Ingebed in het beheersingsproces.
  - > Dit resulteert in kwaliteitsverbetering en efficiënt werken.
  - > Normenkaders zijn laagdrempelig. Dit helpt om de 1e lijn te betrekken bij interne beheersing op een begrijpelijke en logische manier. De normenkaders vormen een gemeenschappelijke taal voor de 1<sup>e</sup>, 2<sup>e</sup> en 3<sup>e</sup> lijn.

**RESULTAAT**  
De normenkaders vormen een gemeenschappelijke taal voor de 1<sup>e</sup>, 2<sup>e</sup> en 3<sup>e</sup> lijn van waaruit samenwerking ontstaat.

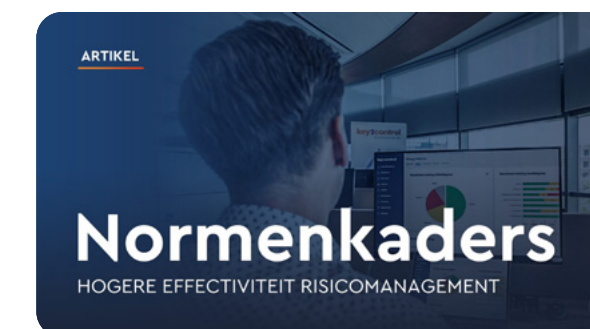
***"Gemeenten dreigen te bezwijken onder toenemende verantwoordingsdruk. Het gebruik van toetsbare normenkaders vermindert die druk: het voorwerk (monnikenwerk) is al gedaan."***

Lees ook onze artikelen over de meerwaarde van normenkaders:



**De 6 grote voordelen van toetsbare normenkaders**

[lees artikel ►](#)



**Hoe normenkaders bijdragen aan hogere effectiviteit**

[lees artikel ►](#)

# Visie van Key2Control op Risicomanagement en BIO2



## Helikopterview op interne beheersing van bedrijfsprocessen

De paden van het doolhof staan beschreven in werkprocessen. Die paden kunnen telkens veranderen, dat is de dynamiek van werkprocessen. Maar wanneer je ín het doolhof staat, heb je geen overzicht. Daardoor is het moeilijk om te bepalen of je het goed doet als organisatie. Zijn er brandhaardjes? Dat zie je niet direct. Behalve vanuit de helikopter. Je kijkt vanuit een hoger niveau, het bedrijfsproces niveau. Dankzij de normenkaders weet je aan welke eisen je moet voldoen. Als je weet waar je niet aan voldoet, kun je daar iets van vinden en daarop actie ondernemen.

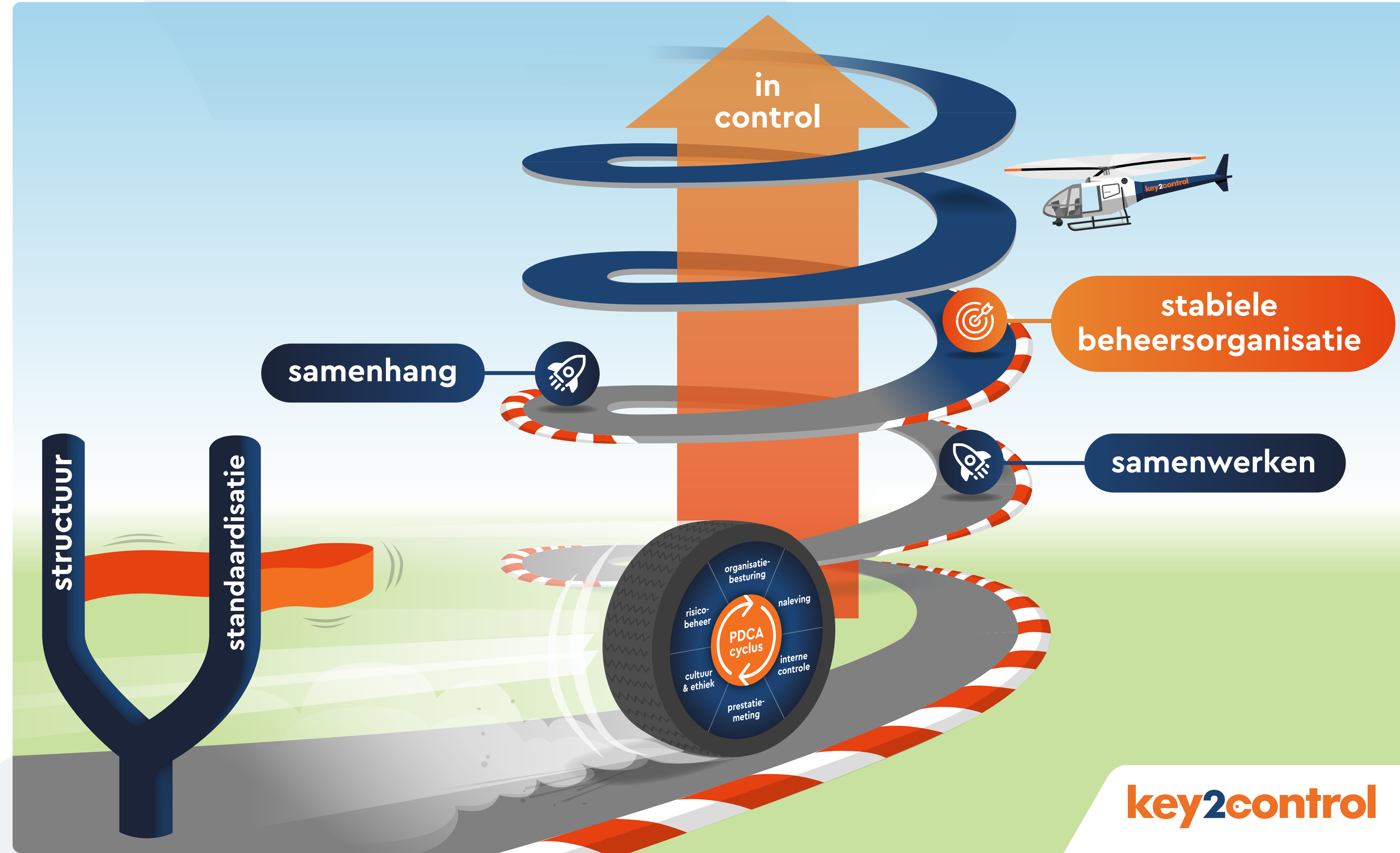
### GROOT VOORDEEL

Normenkaders dienen als referentiekader voor de werkprocessen. Zijn alle elementen verweven in het werkproces?

# Route naar groei en stabiliteit

## Key2Control beheersingsmodel

Onze software wordt afgebeeld als de katapult, die biedt standaardisatie, structuur en ondersteuning om een stabiele beheersorganisatie te realiseren. Een stabiele beheersorganisatie betekent: een voorspelbare uitkomst en betrouwbare uitvoeringskwaliteit. De software helpt om vanuit het proces te denken. Het proces borgt de inhoud. Hierdoor ben je minder kwetsbaar voor bijvoorbeeld uitval van medewerkers. Grip krijgen wordt door deze werkwijze veel eenvoudiger. De Plan Do Check Act cyclus is de basis, het proces.





# Heldere rapportages

Rapportages bieden managementinformatie. De Key2Control rapportages maak je écht met een paar muisklikken en tonen meteen hoe je er als organisatie voor staat zonder dat je de inhoud hoeft te kennen. Je ziet meteen of de organisatie grip heeft en of alles beheersbaar is. Het doel is om als organisatie bewustwording te creëren en samen te kunnen staan voor datgene wat samen bereikt is. In de praktijk betekent dit het wij-gevoel creëren door samenwerken en samenhang. Wanneer je van elkaar weet waar je mee bezig bent, bereik je als organisatie een hoger niveau van volwassenheid.



# Belangrijkste lessen uit het webinar:

- Een risicogebaseerde aanpak en samenwerking tussen disciplines vergroten de beheersbaarheid en effectiviteit van informatiebeveiliging.
- Werk als CISO samen met functioneel applicatiebeheerders (FAB) om systemen, data en informatiebeveiliging effectief te beheersen.
- Begin niet met risicomanagement: het is een middel geen doel op zich en vereist integratie. Een 'gemanaged' volwassenheidsniveau moet worden geïmplementeerd wanneer de organisatie er klaar voor is.
- Begin klein en haalbaar, creëer bewustwording, betrek ambassadeurs en richt een overlegstructuur in en professionaliseer functioneel applicatiebeheer door data te inventariseren, kritieke systemen te identificeren en eigenaarschap te organiseren.
- Het bestuur kan niet meer wegduiken, aangezien de BIO2 hen verantwoordelijk maakt voor naleving van deze norm.
- Een goed functionerend ISMS maakt ENSIA minder relevant.

**Wat is de grootste meerwaarde/het concrete resultaat van de Key2Control software voor dit onderwerp?**

- Key2Control ondersteunt overheidsorganisaties bij het opzetten en beheren van een ISMS, waardoor de BIO2 en risicomanagement optimaal worden geïmplementeerd.

Meer weten?



Versterkte informatiebeveiliging dankzij de BIO2

[lees artikel ►](#)



Hoe een BIO2 implementatie leidt tot een fitte organisatie

[lees artikel ►](#)



# Vraag en antwoord

## Vraag

"Zijn er in de software mogelijkheden om verschillende afdelingen in een organisatie te vergelijken?"

## Antwoord

Ja. De BIO2 is een normenkader om informatiebeveiliging op organisatieniveau te beheersen, verbeteren en verantwoorden. In Key2Control kun je dat inrichten door de BIO maatregelen per afdeling uit te zetten of per afdeling / team aparte metingen uit te voeren. Daarmee behoud je als organisatie flexibiliteit over de inrichting en uitvoering.

## Vraag

"Hoe begin ik met deze nieuwe normen, want het zijn 2 normenkaders?"

## Antwoord

Begin met de verplichte overheidsmaatregelen als volwassenheidsniveau voor risicomanagement nog niet is bereikt. Denk na over de inzet van risicomanagement in een latere fase. Bespreek de uitkomsten van de metingen, zo creëer je draagvlak. Laat het jaarplan vervolgens door het management vaststellen zo borg je het mandaat voor verbetering. Maak periodiek een voortgangsrapportage waarin je constateert wat er gebeurt. Zo maak je het zichtbaar en hou je de organisatie bij de les.

## Vraag

"Wat is de belangrijkste tip die je kunt meegeven?"

## Antwoord

De CISO is centraal aanspreekpunt op het gebied van informatiebeveiliging voor Functioneel Applicatiebeheer en aanjager van het professionaliseren van functioneel applicatiebeheer (FAB) als poortwachters van applicaties en data. Dus "follow the data". Samenwerking en uitwisseling beveiligingsinformatie tussen FAB en CISO is dus cruciaal.

Het webinar is afgesloten met een korte demo van de Key2Control software.

Wil jij ook een demo?

[Demo aanvragen ▶](#)

Of neem direct contact op met Bart:



**Bart Suers**

Directeur

+31 (0)6 52 451 450

[e-mail ▶](#)

Key2Control B.V.  
Avenue Ceramique 222  
6221 KX Maastricht



[www.key2control.nl](http://www.key2control.nl)