

**TERUGBLIK**

---



WEBINAR DONDERDAG 3 APRIL 2025

# Goed voorbereid op NIS2 en Cyberbeveiligingswet

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 ►](#)

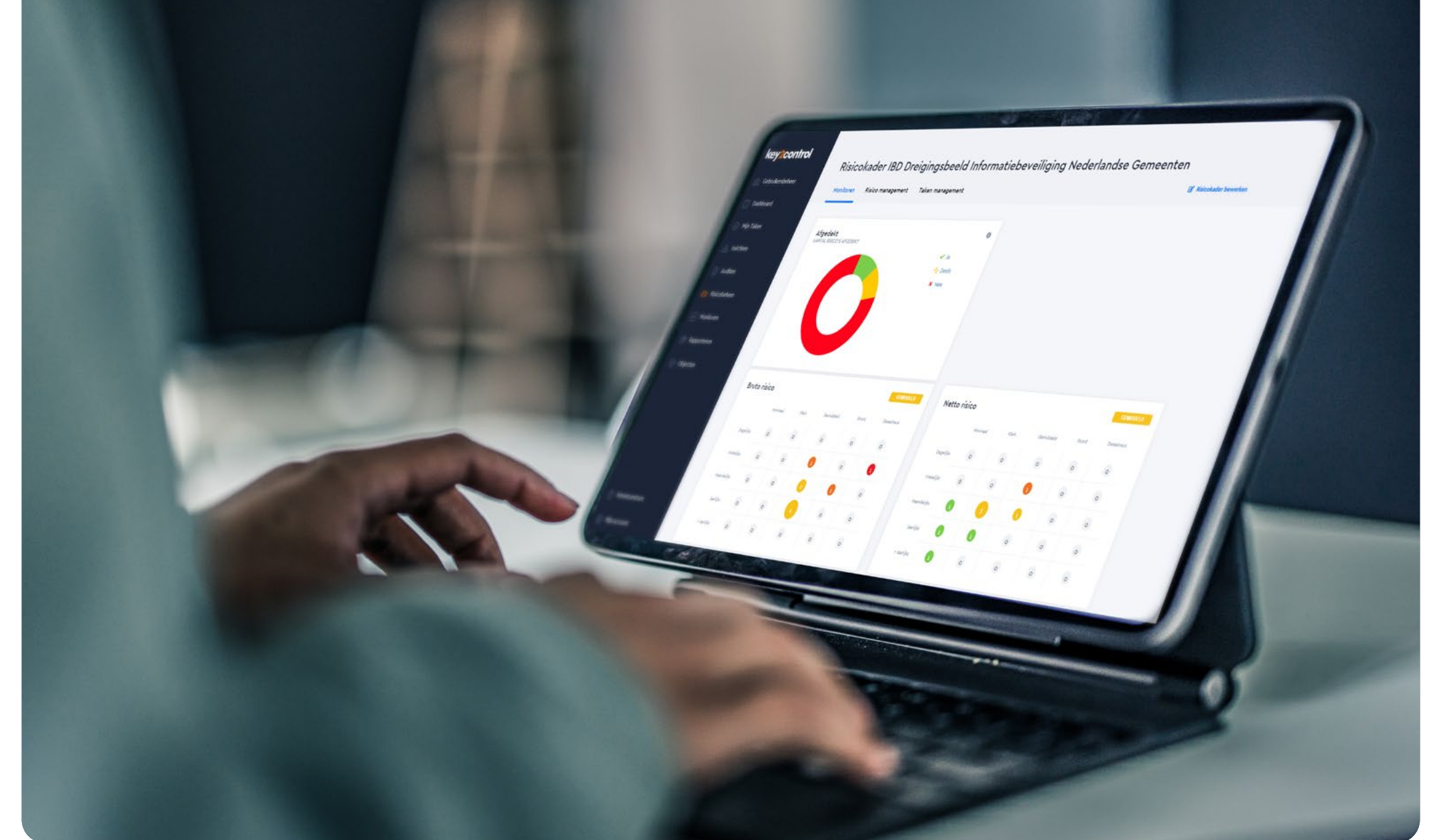


# Waarom is aandacht voor de NIS2 en Cyberbeveiligingswet van belang?

- Overheidsorganisaties krijgen te maken met strengere eisen voor cybersecurity en informatiebeveiliging.
- NIS2 verplicht overheidsorganisaties tot passende maatregelen, toezicht en melding van incidenten.

**RESULTAAT**  
Verbeterde digitale weerbaarheid en naleving wet- en regelgeving.

# 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.

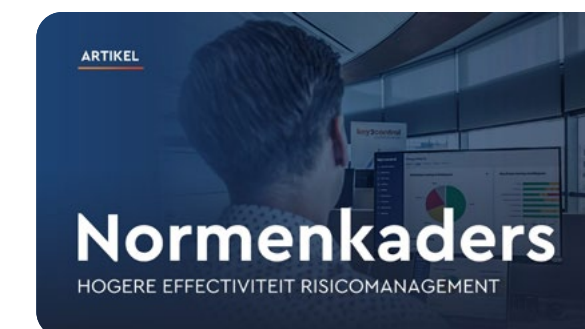
***"Gemeenten dreigen te bezwijken onder toenemende verantwoordingsdruk. Het gebruik van toetsbare normenkaders vermindert die druk: het voorwerk (monnikenwerk) is al gedaan."***

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 informatiebeveiliging?



## 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.

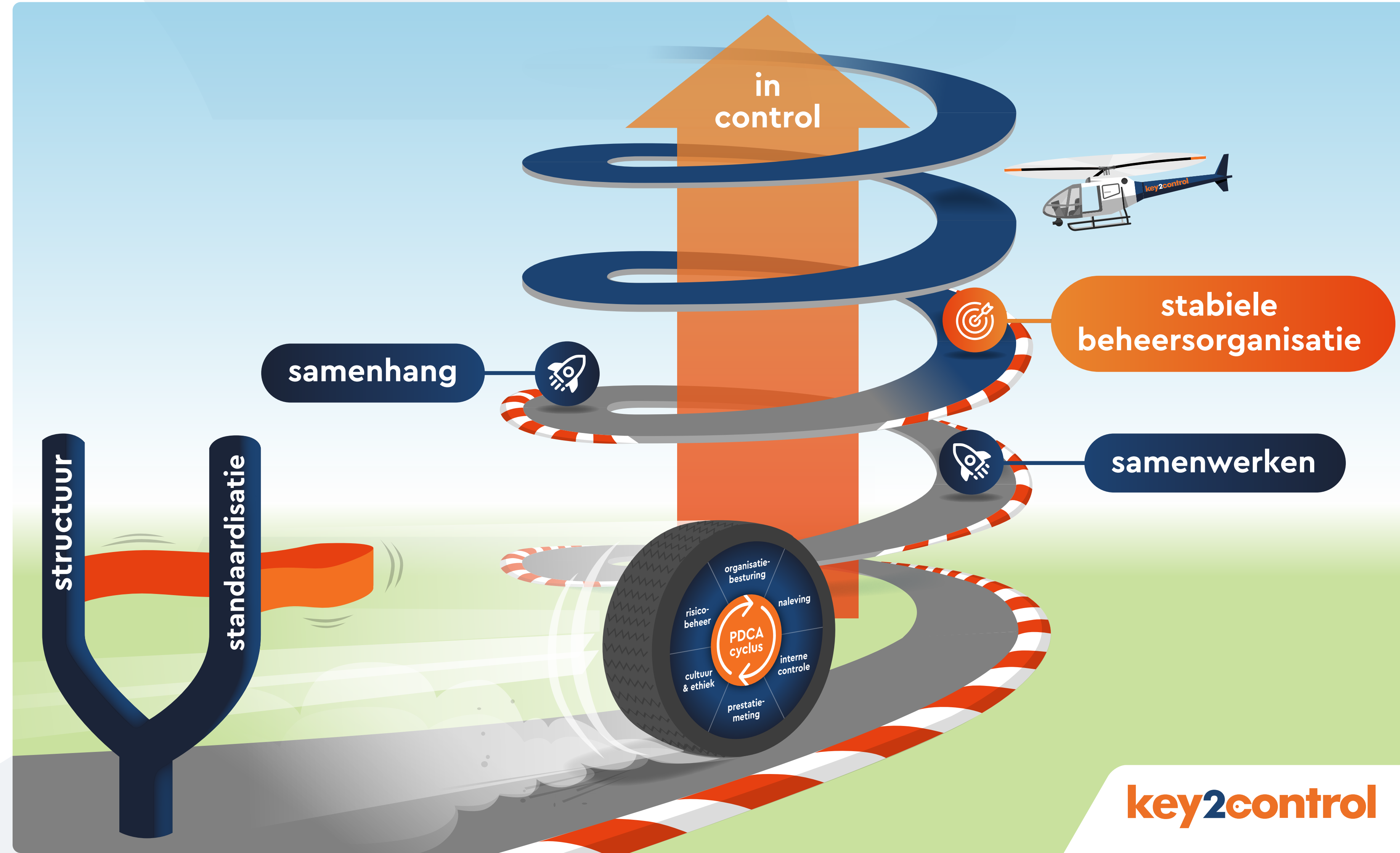
### HET GROTE VOORDEEL

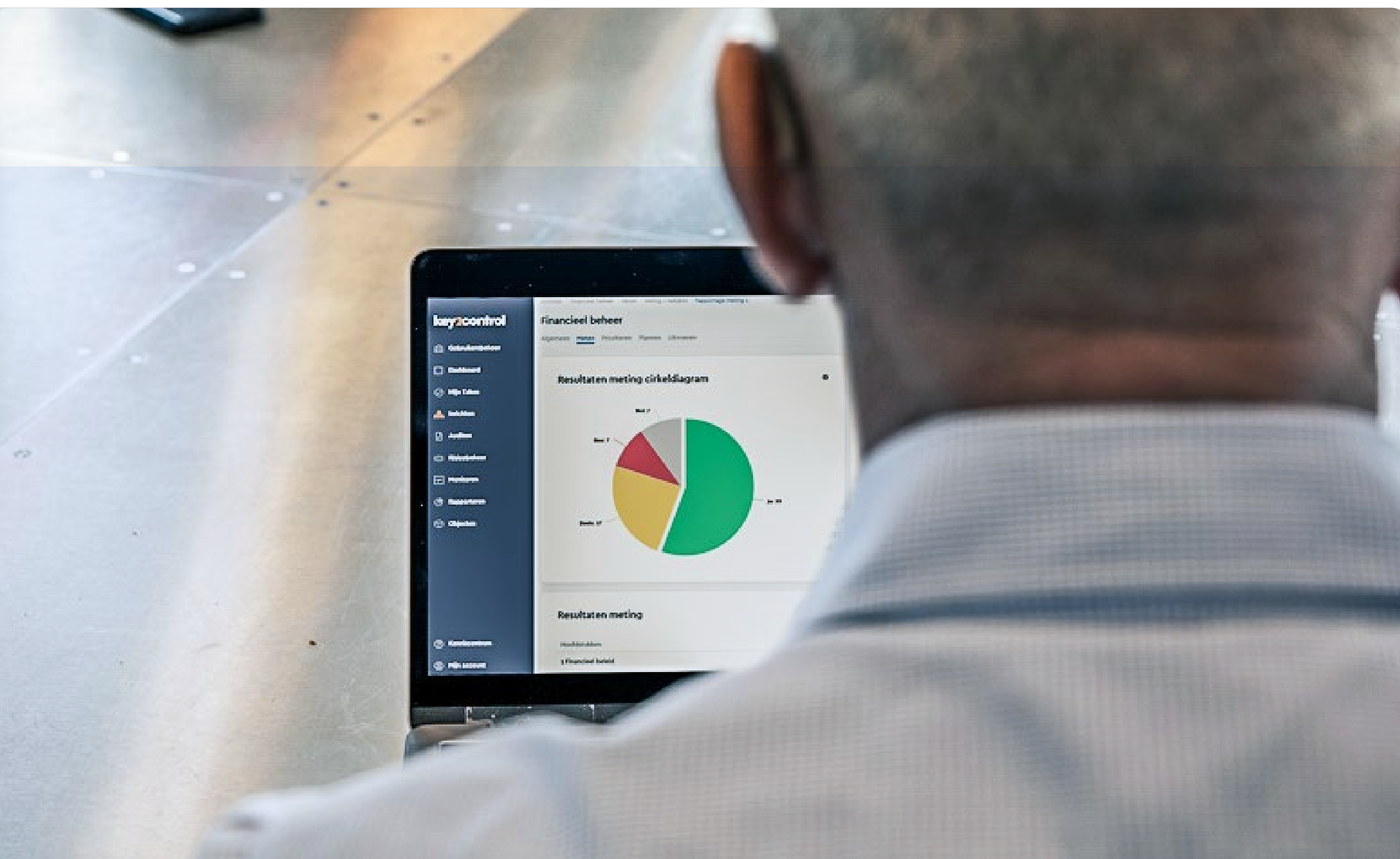
Normenkaders dienen als referentiekader voor de werkprocessen. Zijn alle elementen verweven in het werkproces?

# 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:

- Zorg voor een stabiele en professionele informatiebeveiligingsorganisatie met eigenaarschap, functioneel beheer en een goed werkend ISMS op basis van de PDCA-cyclus.
- Pas een risicogebaseerde aanpak toe: begin op tijd en focus op keyrisks.
- Vertaal keyrisks naar passende controls en kritieke applicaties.
- Versterk monitoring, meldprocedures en leveranciersmanagement.
- Investeer in bewustwording en alertheid bij medewerkers.
- Overweeg ISO27001-certificering als structurele stap naar volwassen informatiebeveiliging.

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

- Key2Control biedt één integrale oplossing voor cybersecurity: een softwaresysteem waarmee overheidsorganisaties risico's gestructureerd kunnen beheersen én aantoonbaar kunnen voldoen aan de eisen van NIS2 en de Cyberbeveiligingswet.

Meer weten?



lees artikel ►



# Vraag en antwoord

## Vraag

**"Als je het risicokader NIS2 invult in de software, heb je meteen een NIS2 GAP?"**

## Antwoord

In feite wel, want in de Key2Control software is een NIS2 Compliance risicokader met 47 voorgedefinieerde dreigingen opgenomen die gemapt is aan de BIO-normen. Daarmee krijg je inzicht in de voor jouw organisatie relevante keyrisks.

## Vraag

**"Hoe verhoudt ENSIA zich tot NIS2 en de CBW?"**

## Antwoord

ENSIA blijft ook met de komst van NIS2 en de Cyberbeveiligingswet een belangrijk instrument voor verantwoording, vooral richting verplichte audits. De komst van NIS2 en CBW betekent echter een aanzienlijke verbreding en verdieping van de eisen aan informatiebeveiliging. De verwachting is dat toezichthouders meer en specifiekere inzicht zullen vragen in de wijze waarop risico's zijn geïdentificeerd, beheerst en gemonitord.

## Vraag

**"Welke eisen stelt NIS2 aan onze samenwerking met externe leveranciers en ketenpartners?"**

## Antwoord

NIS2 stelt expliciet dat organisaties niet alleen verantwoordelijk zijn voor hun interne informatiebeveiliging, maar ook voor risico's die voortkomen uit samenwerking met externe partijen. Dit betekent dat gemeenten de beveiliging in de gehele keten moeten borgen. Leveranciersmanagement wordt daarmee een strategisch onderdeel van het ISMS.

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)