
PvIB
Platform voor
InformatieBeveiliging
21 november 2024
ISMS:
een papieren tijger
of
een tijger in de tank?
Visie & werkwijze ISMS
in het publieke domein
key2control

Even voorstellen

Bart Suers

Gerrit Goud

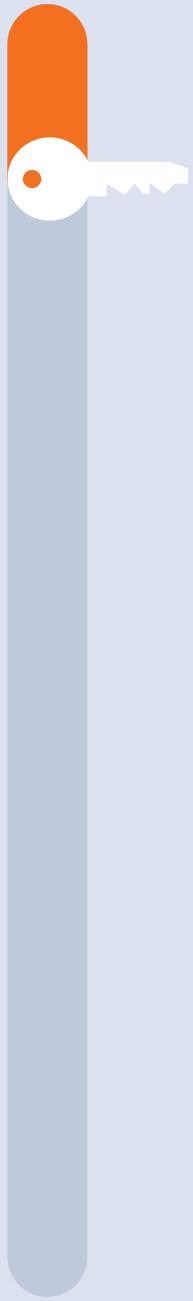
key2control

Key2Control

- 100% Nederlands software- en contentbedrijf
- Continu verbeteren, beheersen en verantwoorden van bedrijfsprocessen
- Compliance-, risk-, auditmanagement
- Focus op gemeenten & lokale overheid


key2control

Inhoudsopgave



key2control

Vraag:

Wie van jullie is werkzaam in de publieke sector?

key2control

Wat speelt er in de publieke sector?

Tijdlijn

Jaar	Ontwikkeling
2025	BIO 2 (op basis van ISO27002: 2022) en NIS2 zullen in Q4 in werking treden

Handreiking BIO2.0-opmaat

De kolomkoppen met rechts bovenin een rode driehoek bevatten e

Control-nr.	Control-soort	BBN van control	Control-titel	Maatregel-nummer	BBN van maatregel	Overheidsmaatregel	Verantwoordelijke(n)
5.35	Organisatorisch	1	Onafhankelijke beoordeling van informatiebeveiliging	5.35.1	2	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier
5.35	Organisatorisch	1	Onafhankelijke beoordeling van informatiebeveiliging	5.35.2	2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier

ISMS wordt verplicht in de publieke sector (overheidsmaatregel: norm 5.35).
Overheid heeft een zorgplicht, documentatieplicht, meldplicht en toezicht.

key2control

Inhoudsopgave

key2control

Wat is een ISMS?

- Het doel van een ISMS is het verbeteren van informatiebeveiliging via een procesmatige aanpak, ondersteund door het management.
- De basis van een ISMS ligt in het interne beheersingsproces.
- Het beheersingsproces zorgt voor tijdige bijsturing en verantwoording van beveiligingsmaatregelen.
- De PDCA-cyclus is de motor en bepaalt in combinatie met de governance de slagkracht van dit proces.

key2control

Voordelen van een effectief ISMS

- Voor alle betrokkenen een steunpilaar voor de organisatie.
- Zorgt voor structuur en standaardisatie in beheersing.
- Audittrail geschikt voor toezicht en audits.
- Borgt kennis binnen de organisatie.
- Minder kwetsbaar bij uitval van sleutelfunctionarissen.
- Stimuleert samenwerking tussen verschillende disciplines en afdelingen.
- Draagt bij aan professionalisering en groei naar volwassenheid.

key2control

Voorwaarden voor een effectief ISMS

- **A tool is for a fool**
- Software alleen is niet genoeg voor succes; visie en inzet zijn essentieel.
- Eenvoud voorkomt complexiteit en bevordert gebruik.
- Maak het proces toegankelijk, begrijpelijk en gebruikersvriendelijk voor iedereen.
- Focus op bewustwording en de zachte kant van interne beheersing zoals cultuur en integriteit (mensfactor).

Inhoudsopgave

key2control

Stelling 1:

"Interne beheersing is het vermogen dat een organisatie in staat stelt doelstellingen op een betrouwbare wijze te realiseren, onzekerheden aan te pakken en integer te handelen."

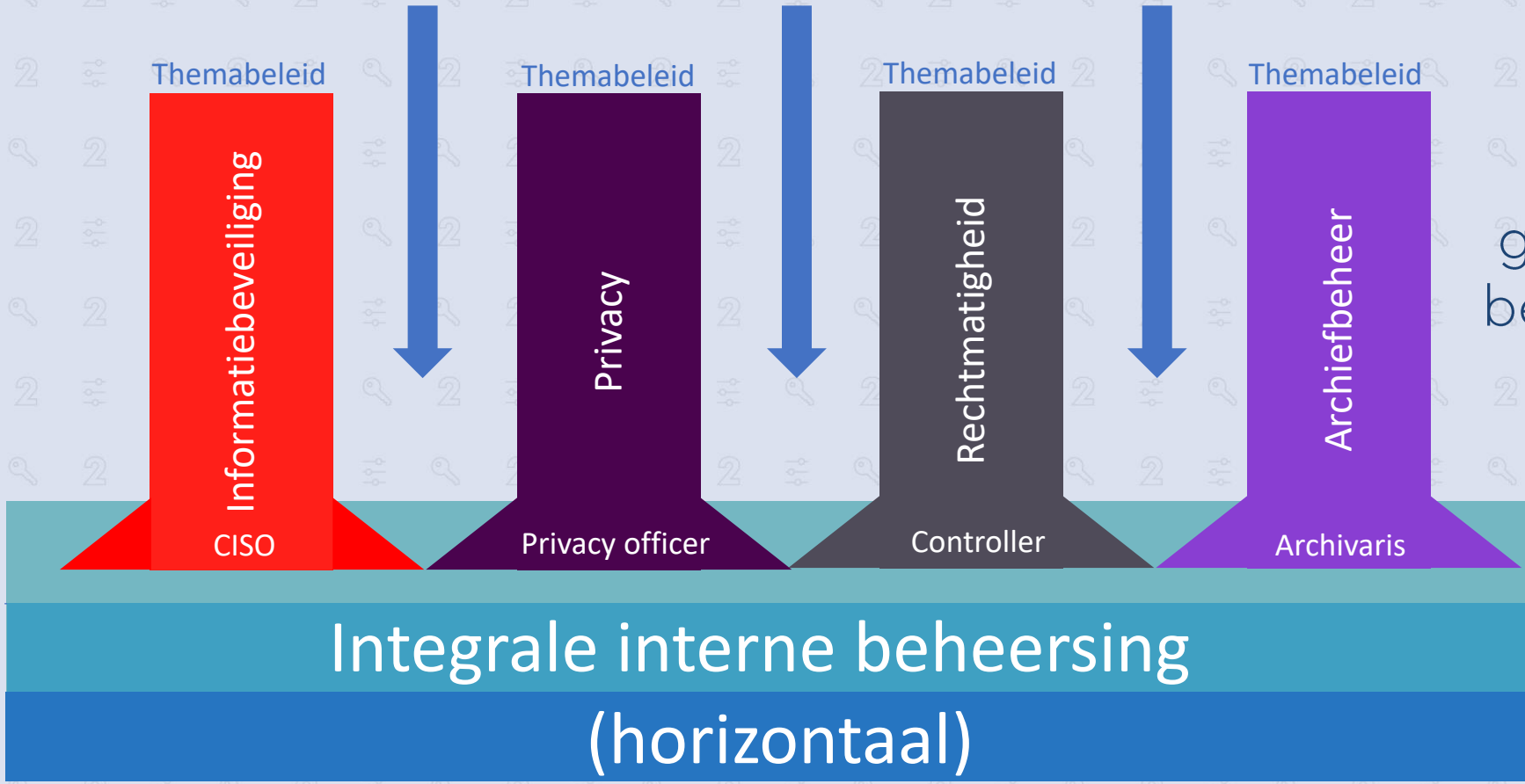
key2control

De basis voor interne beheersing

- Governance: rolverdeling interne beheersing volgens het drielijnenmodel (zelfsturend en corrigerend instrument)
- Doelstellingen: bedrijfs- en daarvan afgeleide beheersdoelstellingen
- Betrouwbaar: voorspelbare uitkomsten, relatief weinig verrassingen
- Risicobeheer: sturen op keyrisks en keycontrols
- Integer: houding & gedrag en compliance

key2control

Integrale interne beheersing



Elk thema maakt gebruik van dezelfde beheersingsprincipes.

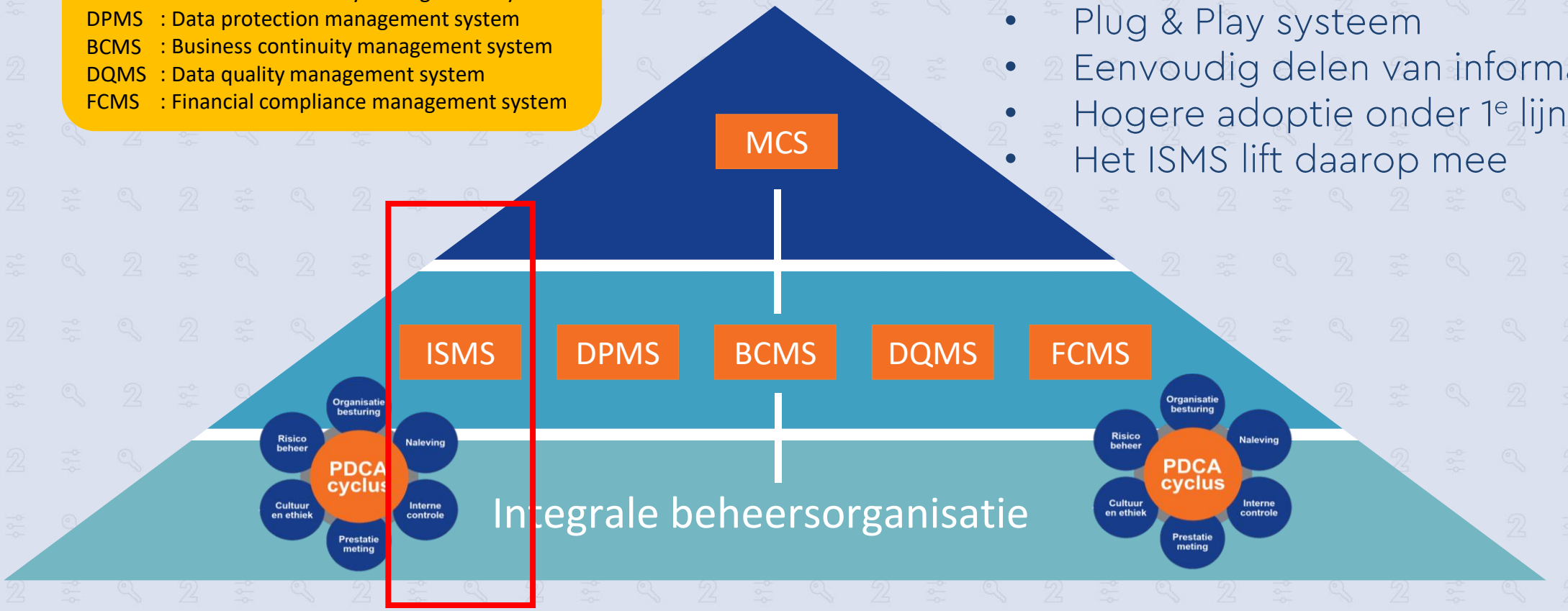
key2control

ISMS als onderdeel van een MCS

MCS : Management control system
ISMS : Information security management system
DPMS : Data protection management system
BCMS : Business continuity management system
DQMS : Data quality management system
FCMS : Financial compliance management system

Voordelen:

- Plug & Play systeem
- Eenvoudig delen van informatie en kennis
- Hogere adoptie onder 1e lijn gebruikers
- Het ISMS lift daarop mee



Geen silo-specifieke applicatie maar één integraal beheersingssysteem voor alle te beheersen thema's.

key2control

Stelling 2:

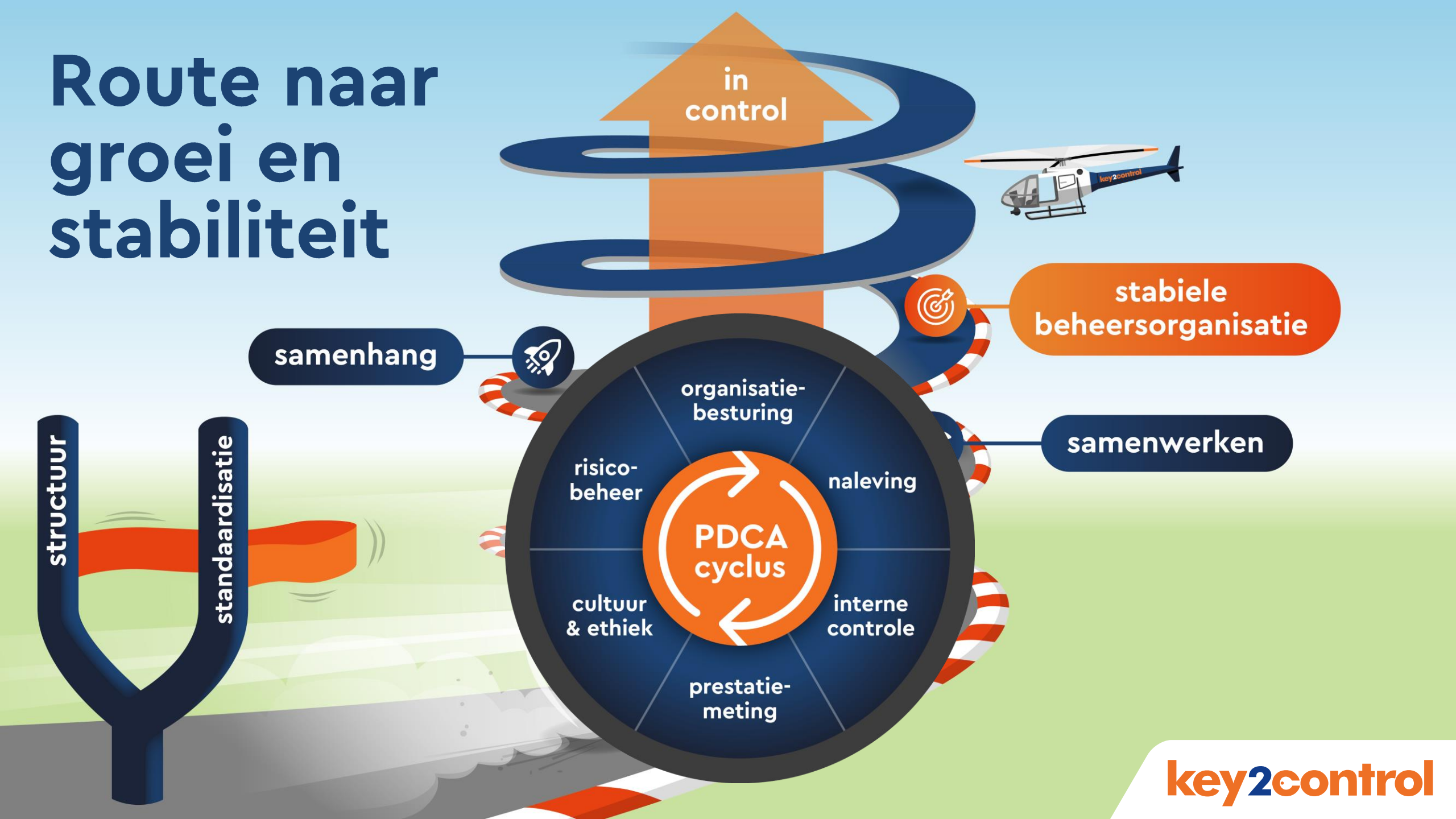
"Het beheersingsproces (de tijger) borgt de inhoud (bewijs)".

key2control

Helicopterview op informatiebeveiliging leidt tot...

key2control

Route naar groei en stabiliteit



key2control

Volwassenheidsniveau (visie, ambitie)

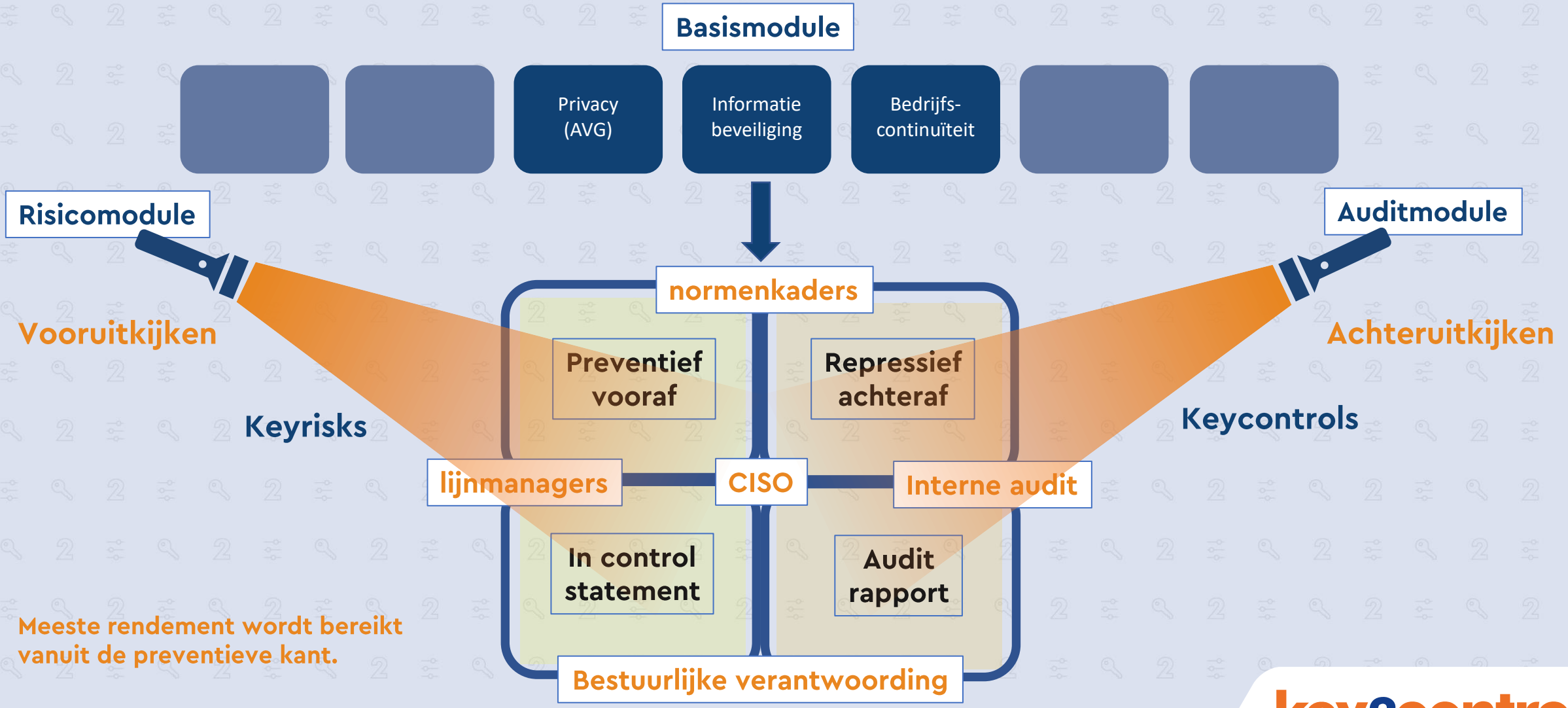
Een ISMS kan starten bij niveau 1, biedt structuur en standaardisatie, en laat gebruikers groeien met visie en ambitie..

key2control

Inhoudsopgave

key2control

Beheersingsmodel voor ISMS



Meeste rendement wordt bereikt vanuit de preventieve kant.

key2control

Risicogebaseerde aanpak

Op operationeel niveau

1. Aan welke eisen moet ik voldoen?

Vaststellen opzet en bestaan vanuit de 1e lijn

2. In hoeverre voldoe ik aan die eisen?

Risk management by exception vanuit de 2e lijn

3. Welke risico's loop ik als ik niet voldoe?

4. Waar moet ik me op focussen om te sturen?

Toetsen werking vanuit de 3e lijn

5. Zijn mijn beheersmaatregelen effectief?

Instrumenten in de PDCA-cyclus

- Toetsbare normen
- Zelf-evaluatie
- Gap-analyse
- Risicokader "Keyrisks"
- Key controls
- Toetsen
- Audit-module

key2control

Inhoudsopgave

key2control

Aanpak uitrol ISMS

- Denk groot met visie en ambitie, maar start klein en deel successen.
- Begin met een zelfevaluatie op basis van de baseline; deel resultaten, verbeter en herhaal jaarlijks (ungoing cyclisch verbeterproces).
- Focus op haalbare verbeteringen, overtuig anderen en creëer bewustwording.
- Volg de data: inventariseer, vaak opgeslagen in de cloud (gemeenten).
- Identificeer kritieke systemen, classificeer data, organiseer eigenaarschap
- Betrek ambassadeurs en richt een overlegstructuur in.
- Werk van generiek naar specifiek; vermijd direct de diepte in te gaan.
- Professionaliseer functioneel applicatiebeheer als poortwachters van applicaties en data.

Relatie tussen CISO en FAB

- Primair: follow the data.
- CISO is centraal aanspreekpunt op het gebied van informatiebeveiliging voor FAB
- De keten is zo sterk als de zwakste schakel.
- Professionaliseer FAB.
- Samenwerking en uitwisseling beveiligingsinformatie tussen FAB en CISO is cruciaal.

key2control

Inhoudsopgave

key2control

Korte impressie

In 15 klikken

- Voorbeeld zelfevaluatie BIO
- Verklaring van toepasselijkheid
- Status uitgezette maatregelen
- Uitvoeringstaken
- Risicoanalyse
- Risicokaart
- Dashboard

key2control

Meer weten?

Bekijk onze website
www.key2control.nl

Meld je aan voor onze gratis kenniswebinars
www.key2control.nl/webinarkalender

Lees onze blogs over interne beheersingsthema's
https://key2control.nl/category/blogs/

key2control

Inhoudsopgave

key2control

Een papieren tijger?
Ja!
overheid heeft een documentatieplicht.

Tijger in de tank?
ja!
Overheid heeft een zorgplicht, meldplicht en extern toezicht (NIS2).

key2control

Dank voor jullie belangstelling!

Bart Suers MScBA
Directeur
bart.suers@key2control.nl
06 - 52 45 14 50

www.key2control.nl

Drs. Gerrit Goud RA
Senior Consultant
gerrit.goud@key2control.nl
06 - 54 33 51 64

www.key2control.nl

key2control