mbo digitaal

NETWERK Informatiebeveiliging en Privacy

Governance IB&P in het mbo 2023

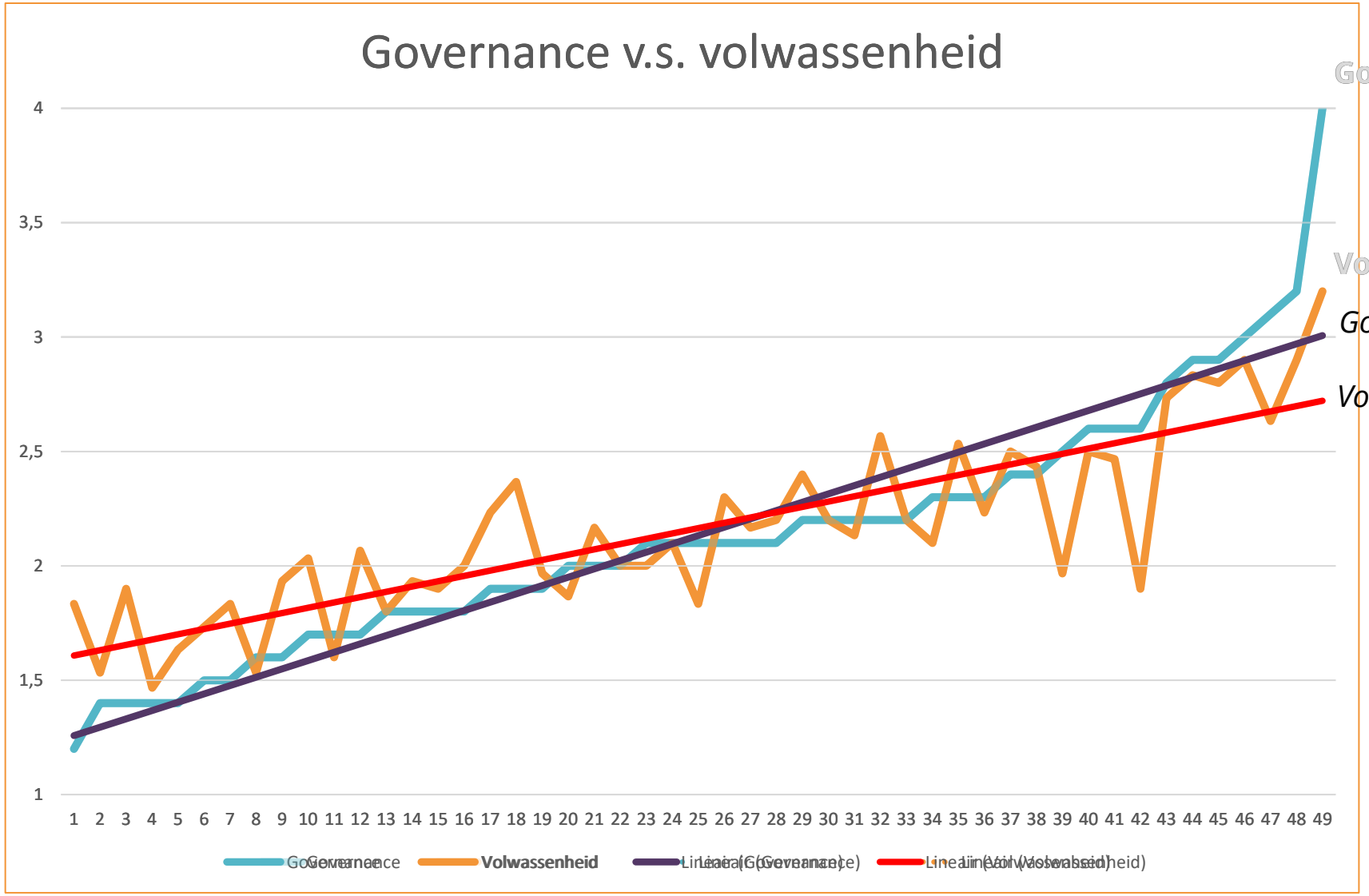
8 maart 2024

Van toekijken naar control

Victor Meerloo

14-03-2024

NBA nulmeting 2022 mbo



Governance

Volwassenheid

Governance

Volwassenheid

NBA-Volwassenheid

- Governance
- Processen
- Technische weerbaarheid

Het onderzoek governance van informatieveiligheid

- December 23 Uitvraag 55 instellingen
- Deelnemers 44 van de 55 instellingen!
  - 44 Bestuurders
  - 44 IBP-functionarissen
- Onderzoek **Hoe** is de governance georganiseerd
  - Gemeenschappelijke basis
  - Organisatie in het mbo
  - Leerpunten

Governance

CODE GOED BESTUUR MBO 2020

College van bestuur verantwoordelijk is voor het bereiken van de strategische doelstellingen.

➡ dus ook *Strategisch Risicomanagement*

Governance van informatiebeveiliging

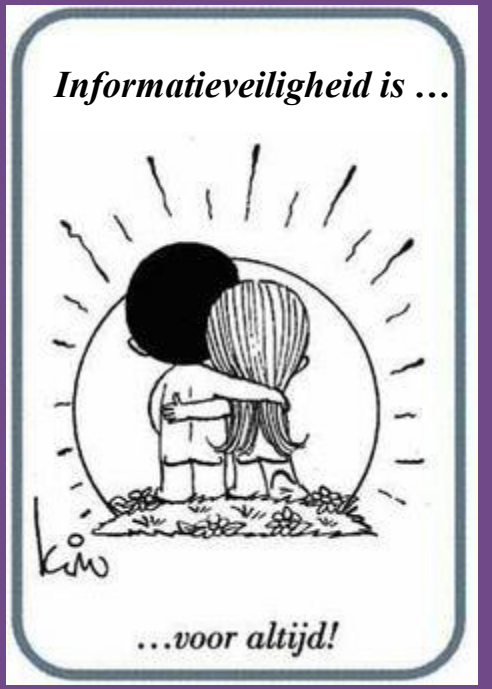
De sturing op informatiebeveiliging binnen een organisatie, waarbij de bestuurder eindverantwoordelijk is voor het risicomanagement.

CODE
GOED BESTUUR
MBO 2020

Informatieveiligheid is…

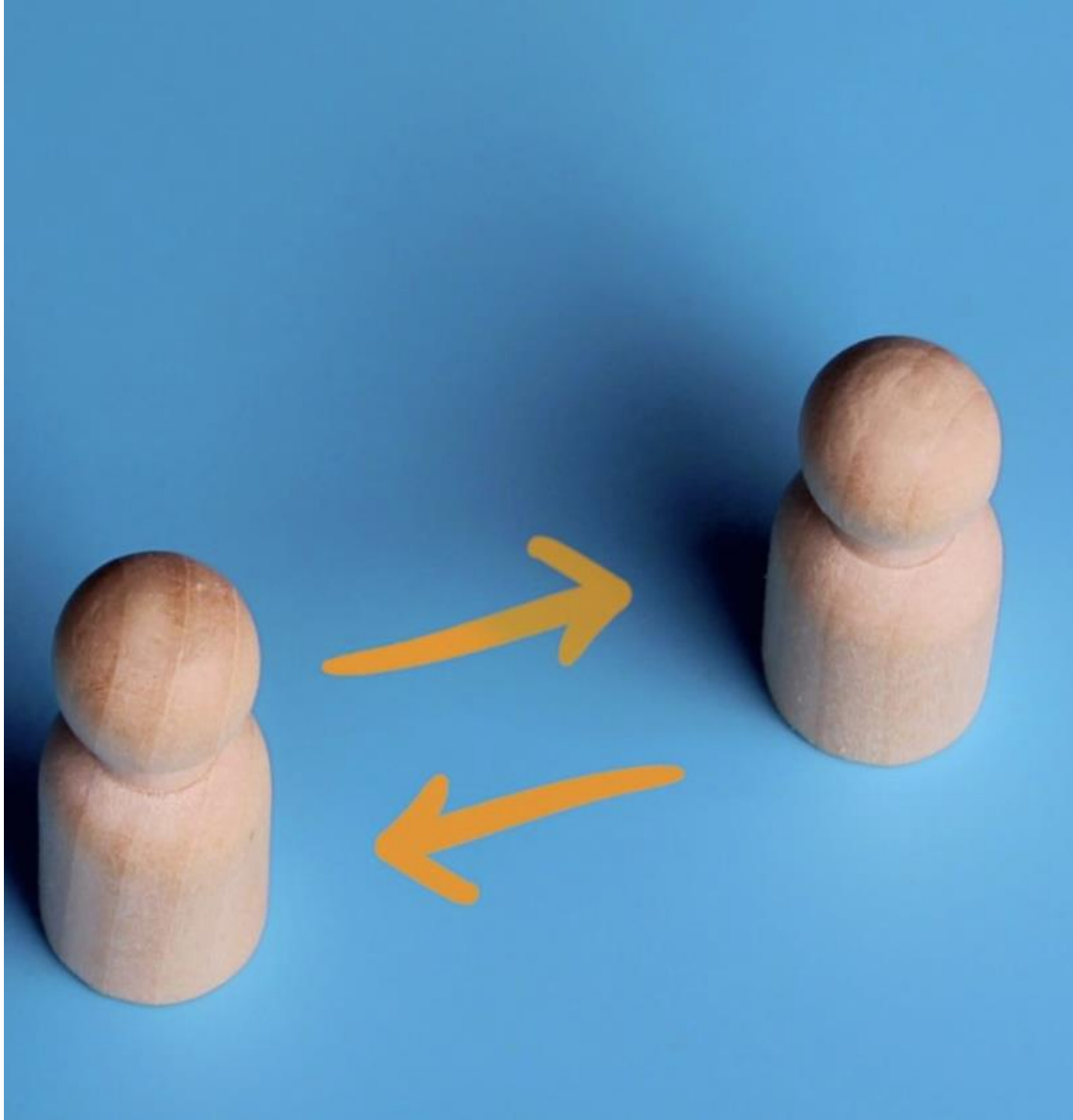
Informatieveiligheid = Risicomanagement

- NBA-kader (best practice)
- Operationeel risicomanagement

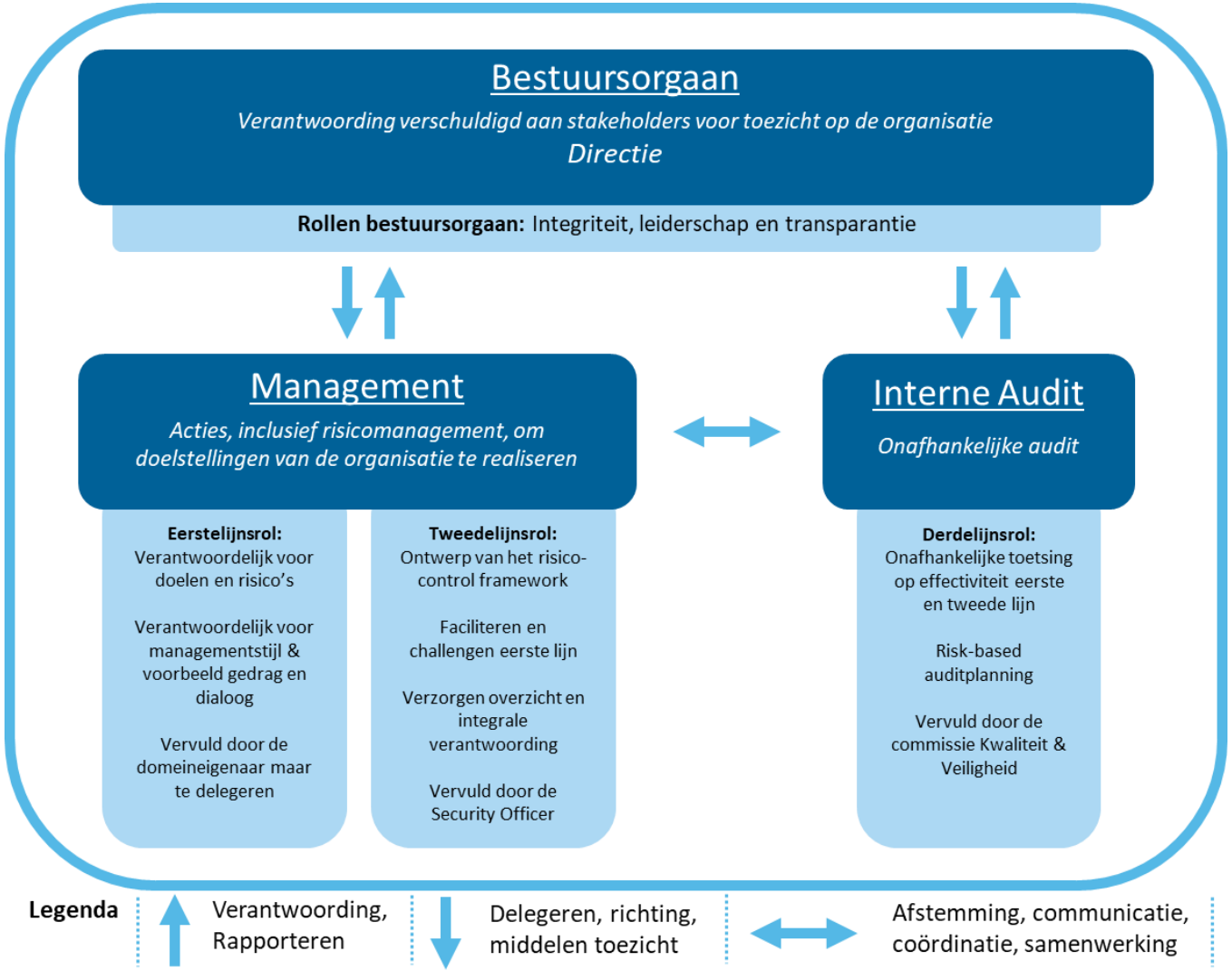


Risico gerichte aanpak

- Besluitvorming onder onzekerheid
- Hulpmiddel om te prioriteren
- Schade minimaliseren!
- **Communicatiemiddel!**



3-lines model risicomanagement



1e lijn – domeineigenaar

- risico-eigenaar

2e lijn – IBP-functionaris

- eigenaar ISMS (PDCA)
- ondersteuning 1e lijn
- overzicht / integrale verantwoording

3e lijn – Interne audit

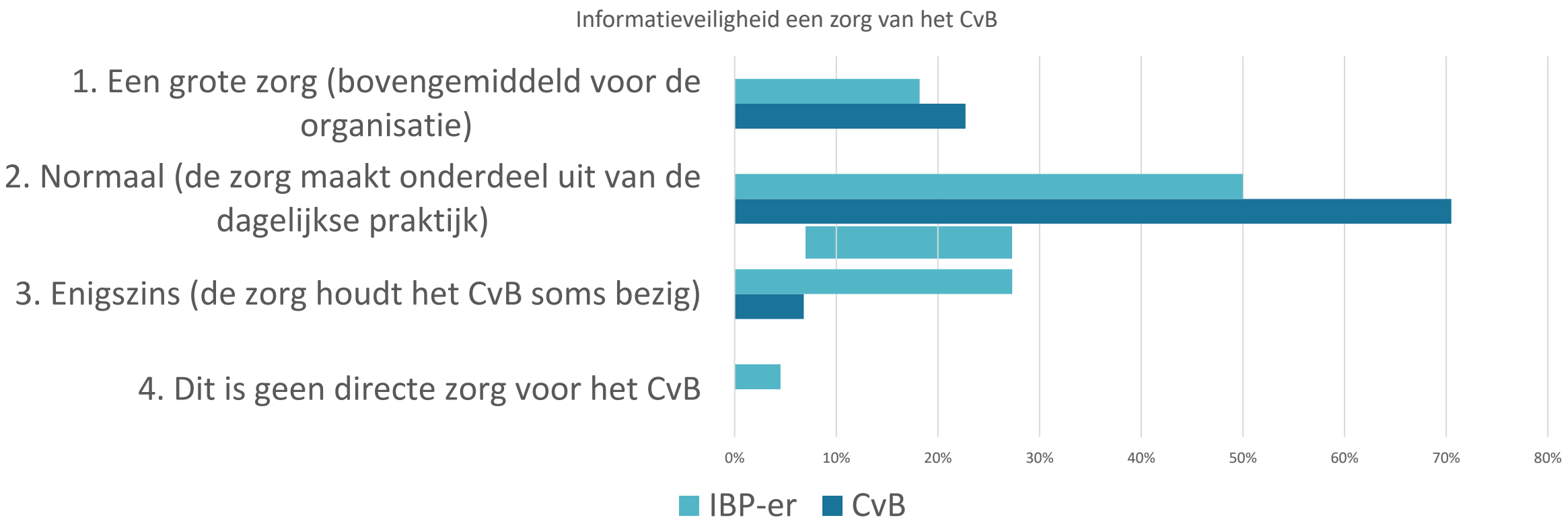
- onafhankelijk
- risico gebaseerd

Resultaten onderzoek

- De zorg rond informatieveiligheid bij CvB
- De rol van de bestuurder
- Risicogerichte aanpak
- Risico-eigenaarschap (v.s. 3-lines model)
- De rol van de IBP-functionaris
- Positie van de IBP-functionaris
- Eigenschappen top 3 instellingen

De zorg rond informatieveiligheid bij CvB

In hoeverre zijn onderwerpen als cyberveiligheid, kwetsbaarheden, verbeteren van awareness bij studenten en medewerkers een zorg voor het CvB?



Bespreektip!

Ga als IBP-functionaris het gesprek aan met de bestuurder om de zorg over en het belang van het onderwerp informatieveiligheid met elkaar te bespreken.

De rol van de bestuurder

mbo digitaal

Welke rol ziet het CvB voor het CvB weggelegd op het gebied van informatiebeveiliging en privacy?

Rol van de bestuurder	Bestuurder	IBP-er	verschil
a) Zich informeren	5,00	4,56	0,44
b) Richtinggevend (strategisch)	4,80	4,19	0,61
c) Kaderstellend (beleid en bevoegdheden)	4,86	4,37	0,49
d) Sturend / bijsturend (tactisch)	3,89	3,30	0,59
e) Evaluerend / kritische reflectie	4,45	4,12	0,33
f) Controlerend	3,68	3,44	0,24
g) Stimulerend	4,45	3,91	0,54
h) Voorbeeld functie	4,86	4,35	0,51
i) Vertegenwoordigende functie (stakeholders)	4,09	3,77	0,32

>> De bestuurder schat zijn rol altijd zwaarder in dan de IBP denkt over de bestuurder

Een gesprek tussen de bestuurder en de IBP-functionaris zou het beeld over de betrokkenheid van de bestuurder meer in balans kunnen brengen.

Risicogerichte aanpak

IBP-er

De instelling hanteert een risicogerichte aanpak ten aanzien van informatieveiligheid.

De instelling hanteert risicogerichte aanpak	Aantal	Relatief
01 - volledig mee eens	9	20%
02 - enigszins mee eens	21	48%
03 - niet eens - niet mee oneens	7	16%
04 - grotendeels mee oneens	6	14%
05 - volledig mee oneens	1	2%
Totaal	**44**	**100%**

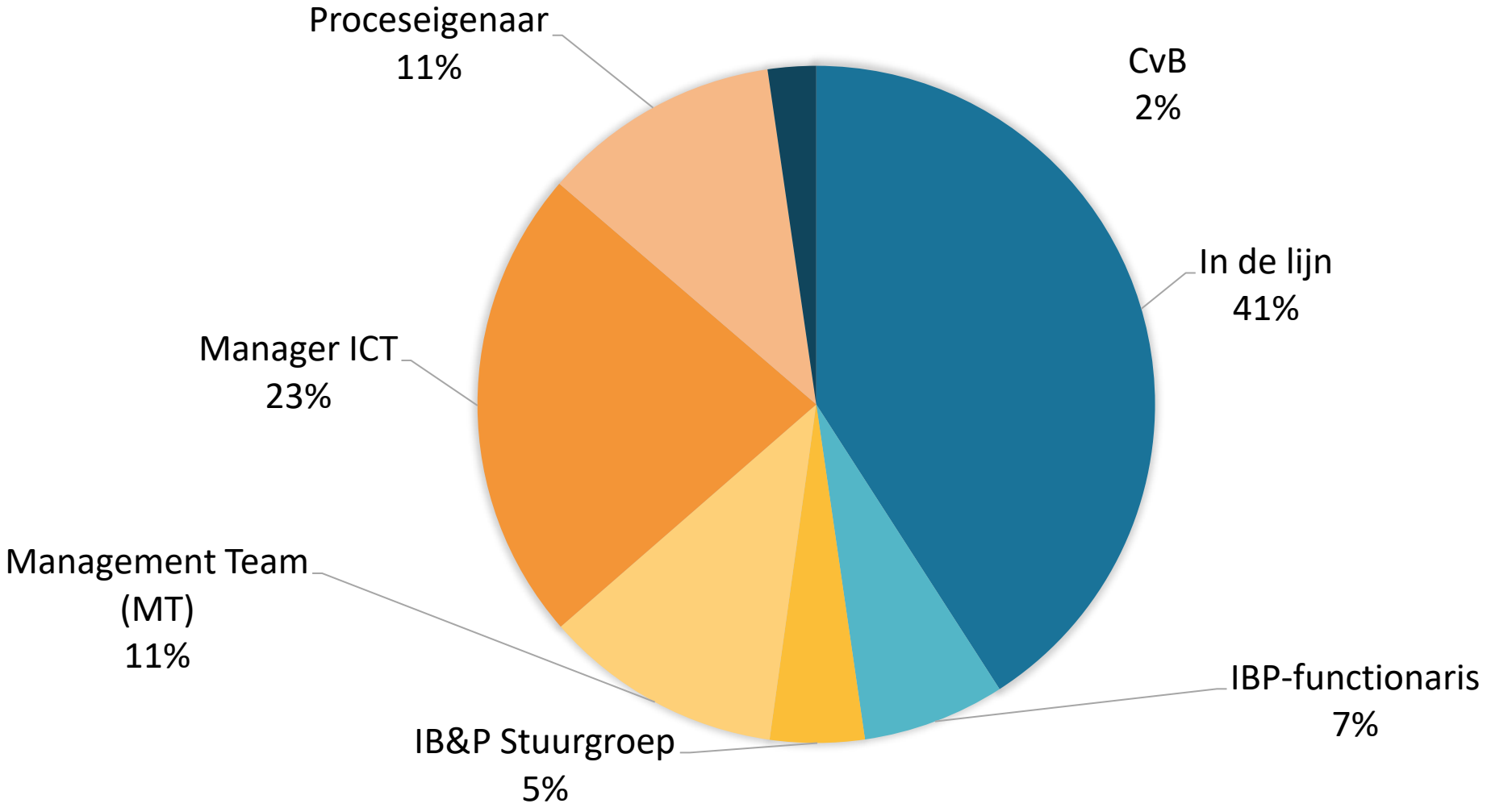
TrustBound grc platform

Bespreektip!

- *Bespreek de inschatting van de risico's en prioriteer acties o.b.v. risico*
- *Gebruik de GRC-applicaties voor een risico-gerichte aanpak.*
  - ✓ *Risicorapportages*
  - ✓ *Voortgang taken (beheersmaatregelen)*

Risico-eigenaarschap (v.s. 3-lines model)

Waar is de verantwoordelijkheid belegd voor de uitvoering van beheersmaatregelen in de operationele bedrijfsprocessen?



De rol van de IBP-functionaris

mbo digitaal

Positionerig IBP-Functionaris	kolom 1: Veiligheid van de IB-functie (Information risk management)	kolom 2: Veiligheid van de ICT-functie (ICT beveiliging / cyber security)
rij 1: Strategisch en/of tactisch	traditionele CISO-rol CISO	ICT-beveiligingsmanager IB-mgr
rij 2: Tactische en/of operationeel	traditionele ISO-rol + optioneel Privacy Officer Rol. ISO	ICT-beveiligingsspecialist/beheerder NW-spec

De rol van de IBP-functionaris

mbo digitaal

Hoe positioneert het CvB de rol van de IBP-functionaris (verantwoordelijk voor het adviseren rond en toezicht houden op de uitvoering van het informatiebeveiligingsbeleid)?

Postionering IBP-functionaris		Kolom 1: Veiligheid van de IBP-functie		Kolom 2: Veiligheid van de ICT-functie	
positie		bestuurder	IBP-functionaris	bestuurder	IBP-functionaris
Rij 1: Strategisch en/of tactisch	Bestuurder	30%		16%	
	IBP-functionaris	CISO	31%	IB-mgr	13%
Rij 2: Tactisch en/of operationeel	Bestuurder	36%		13%	
	IBP-functionaris	ISO	40%	NW-spec	16%
Totalen kolommen	**Bestuurder**	66%		29%	
	IBP-functionaris		71%		29%

Markt

Evalueer de positie van de IBP-functionaris binnen de instelling. Welke positie wordt gekozen en hoe wordt deze onderbouwd. Bij een tactisch/operationele insteek, kijk hoe de strategisch/tactische positie wordt ingevuld.

Positie van de IBP-functionaris

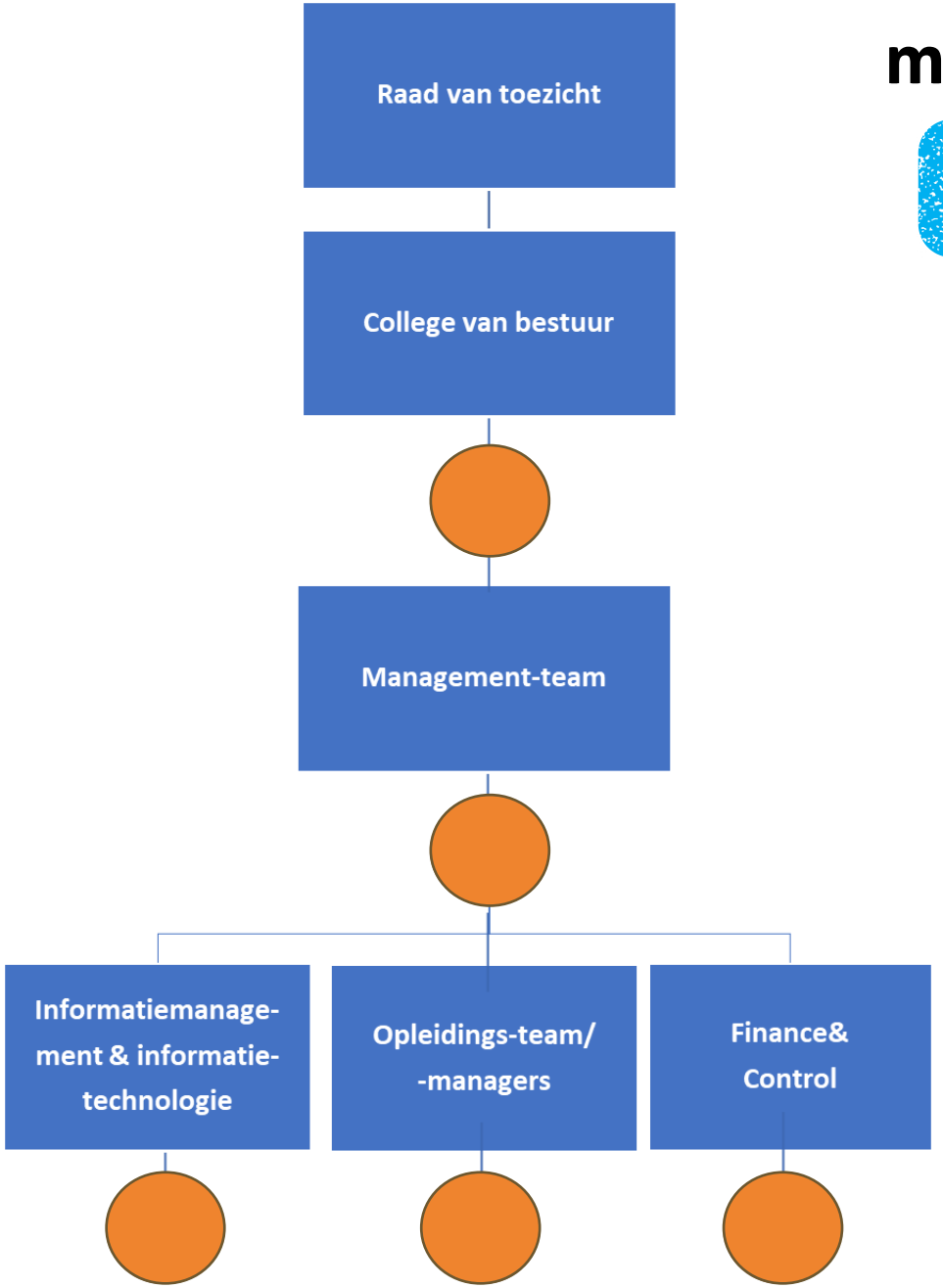
Waar in de organisatiestructuur is IBP-functionaris formeel geplaatst? Hiërarchisch valt deze onder....

mbo digitaal

IBP-er

45% IBP onder ICT?

- Conflict of interest?
- Dicht bij het vuur (techniek)
- Communicatie met de organisatie (ICT?)
- Onafhankelijk?



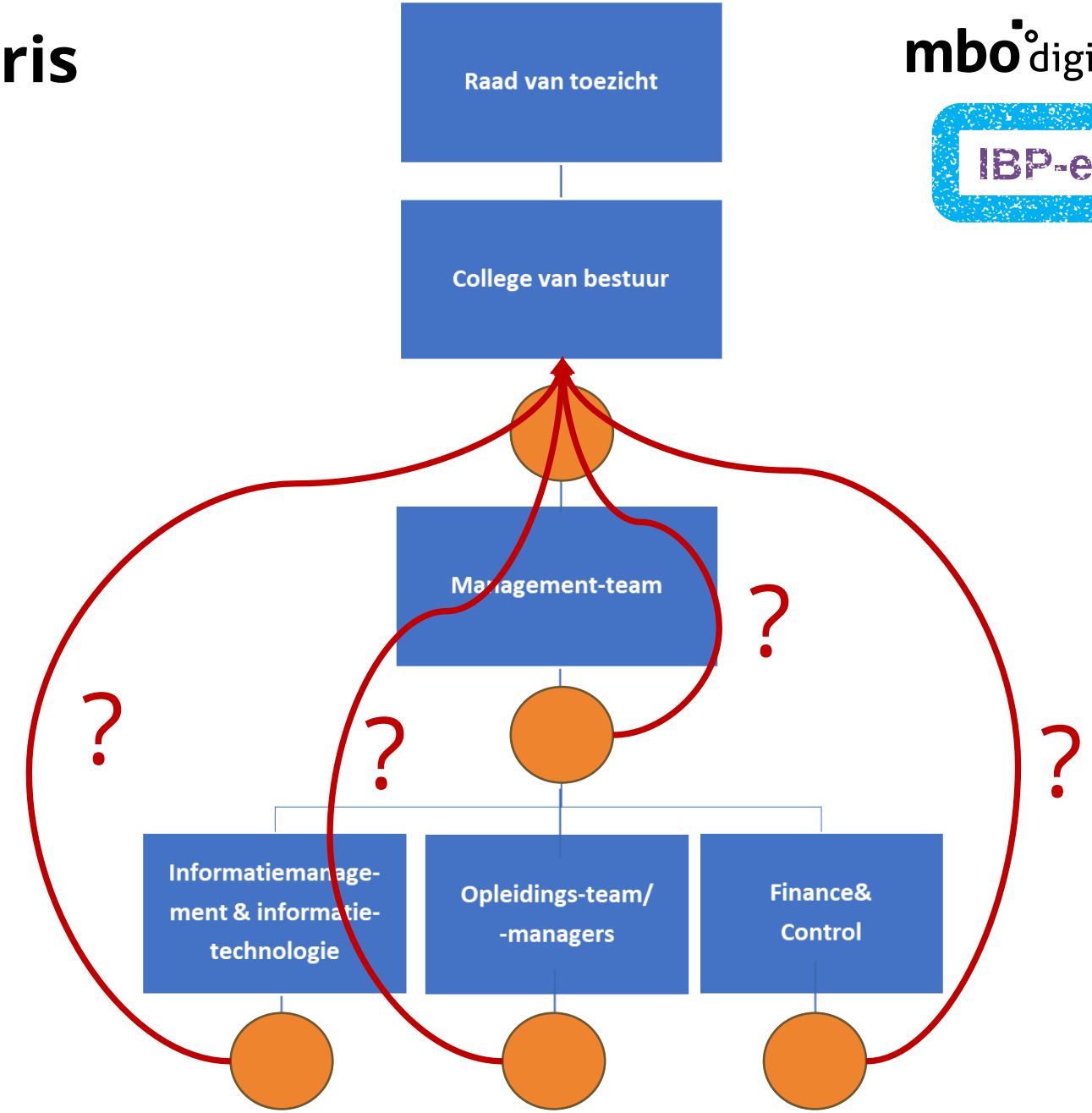
Positie van de IBP-functionaris

Verantwoording aan CvB

- Objectiviteit en onafhankelijkheid
- Strategische uitlijning
- Toegang tot middelen
- Prioriteitsstelling en risicomanagement
- Rapportage van beveiligingsstatus

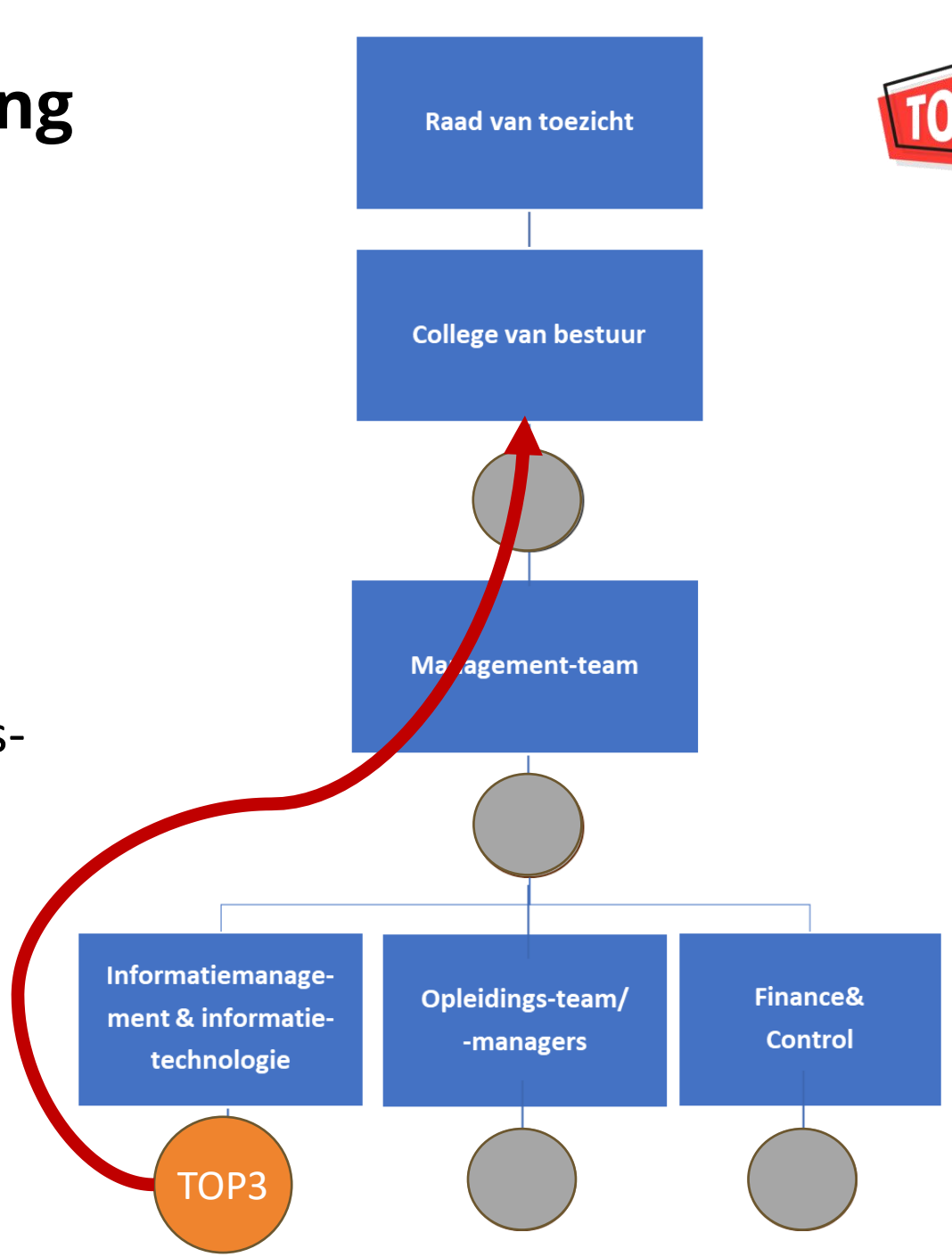
Onderzoek

52% IBP-functionaris met rechtstreekse lijn de bestuurder (los van positie) -> ***48%*** *dus niet.*



Top-3 instellingen NBA 0-meting

- Opvallend! IBP hiërarchisch onder ICT
- Directe lijn met CvB
- Volwassenheid NBA = 3 (van 5) op IBP en 2,9 op governance.
- Hoge betrokkenheid bestuurder
- Verantwoordelijkheden belegd bij proces-/domeineigenaren
- Duidelijke beschreven taken, bevoegd-heden en verantwoordelijkheden.
- ≥ 1 FTE inzet op het onderwerp informatiebeveiliging



Afronden

- Conclusies
- Adviezen

Conclusies

- Informatieveiligheid = risicomanagement
- Bestuurder is eindverantwoordelijk voor beoordelen van risico's en voorstellen van beheersmaatregelen.
- Onderzoek benadrukt belang van informatiebeveiligingsbeleid en verantwoordelijkheden.
- Goed scorende instellingen op onderwerp informatieveiligheid kennen actieve betrokkenheid van de bestuurder.
- Verschillen in inzicht tussen bestuurder en IBP-functionaris over
  - Rollen van de bestuurder
  - Positionering en verantwoordelijkheden van IBP-functionaris.
  - Besluitvormingsproces.
- 63 procent van de instellingen legt de operationele verantwoordelijkheid voor risicomanagement in de lijn. (3-lines)

Advies

mbo digitaal

1. Hanteer een risicogerichte aanpak voor informatiebeveiliging.
2. Zorg voor duidelijke beschreven taken, bevoegdheden en verantwoordelijkheden en versterk risico-eigenaarschap in de organisatie.
3. Hanteer het 3-Lines model voor risicomanagement.
4. Verhelder de rol van de bestuurder en vergroot diens betrokkenheid.
5. Verbeter de afstemming tussen bestuurders en IBP-functionarissen en zorg voor een gedeeld referentiekader.
6. Een directe lijn naar de bestuurder is aan te raden voor grote informatieveiligheidsrisico’s. Wees open als je escaleert als IBP-functionaris.
7. Evalueer de rol en positie van de IBP-functionaris.
8. Zet de GRC-applicatie in om risicomanagement onder controle te krijgen.