DORA-wetgeving: Hoe staat het ervoor?

VIP CONGRES

1 juli 2025

Introductie

Arno Kroese

Director IT Assurance & Advisory

KPMG Nederland

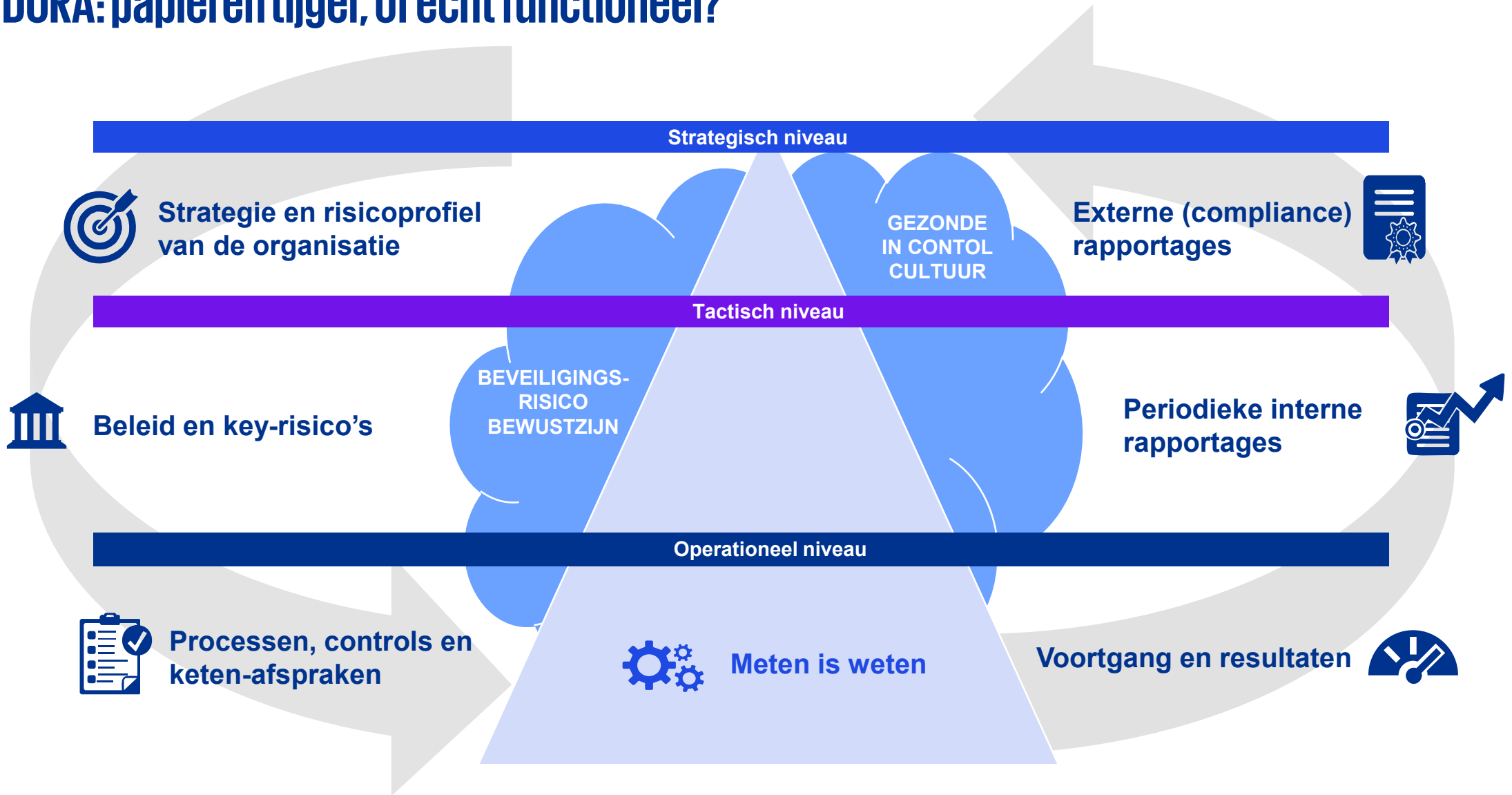
DORA: om uw geheugen op te frissen

Verbeteren digitale operationele weerbaarheid

Financiële sector + ICT-leveranciers

Aantoonbaar compliant vanaf 17 januari 2025

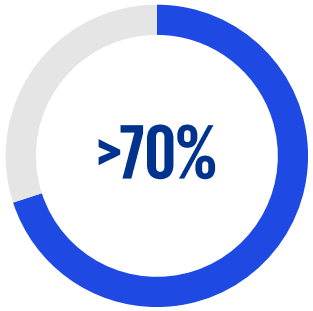
DORA: papieren tijger, of écht functioneel?



De belangrijkste uitdaging is om de balans te bewaren tussen aantoonbare naleving van de DORA-vereisten en focus op daadwerkelijke weerbaarheid!

Tot eind 2025 nodig om DORA-implementatie te voltooien!

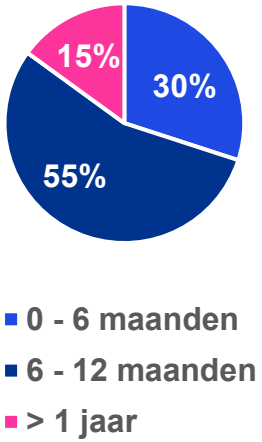
DeNederlandscheBank
EUROSYSTEEM



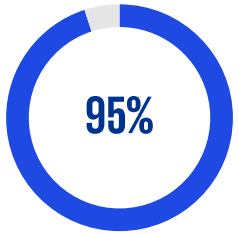
Meer dan 70% van de inspanningen voor implementatie gerealiseerd

Veel instellingen hanteren een risicogebaseerde aanpak voor de implementatie

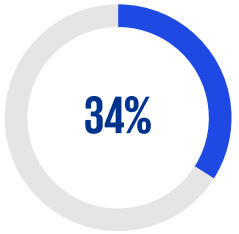
Hoeveel tijd nog nodig?



ICT Third Party Risk Management



Uitbestedingsbeleid geactualiseerd



ICT-contracten in lijn met DORA, gerelateerd aan kritieke of belangrijke functies

Restrisico niet formeel geaccepteerd door het bestuur

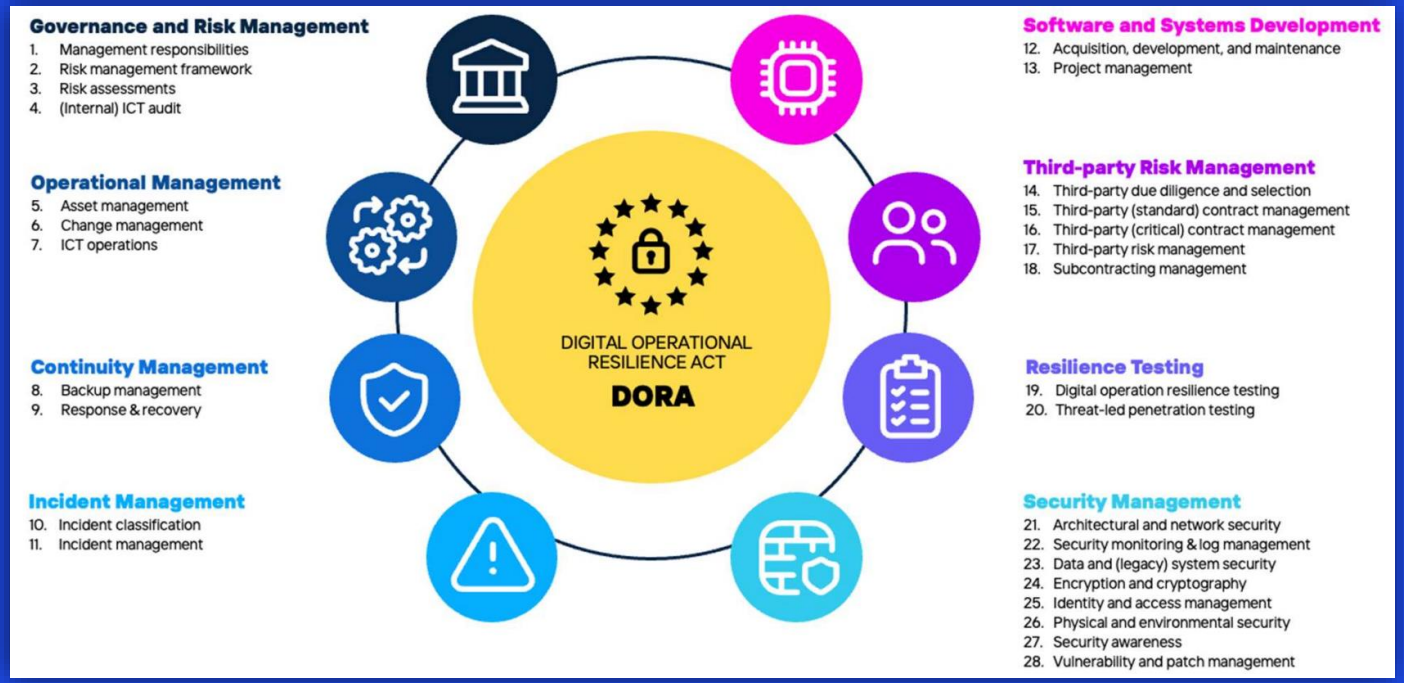
Bron: Resultaten sectorbrede (verzekerings- en pensioensector) uitvraag naar DORA-implementatie van DNB (gepubliceerd: 28 mei 2025)

ICT Risk Management

Observaties en uitdagingen

- **Lastig om verantwoordelijkheid (accountability) in de organisatie eenduidig te beleggen.**
- **Welk beheersingsraamwerk te hanteren?**
- **Hoe integreert dit met andere beheersingsraamwerken?**
- **Een pragmatische en effectieve implementatie?**

Voorbeeld: DORA control framework (NOREA DORA Taskforce)



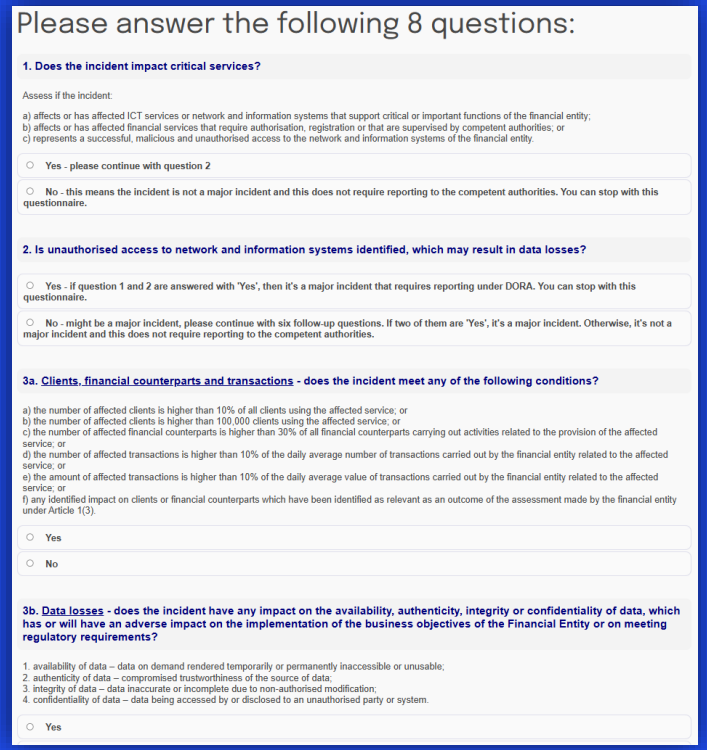
Inclusief mapping met DORA vereisten en DNB Good Practice IB (58 controls)!

Incident reporting

Observaties en uitdagingen

- **Wanneer is een ICT-incident ernstig en moet deze gerapporteerd worden?**
- **Uitdagende tijdslijnen voor de meldingen en veel datapunten benodigd.**
- **Nog geen meldingen van ernstige ICT-incidenten publiekelijk beschikbaar.**

Voorbeeld: DORA Incident Classification tool (NOREA DORA Taskforce)

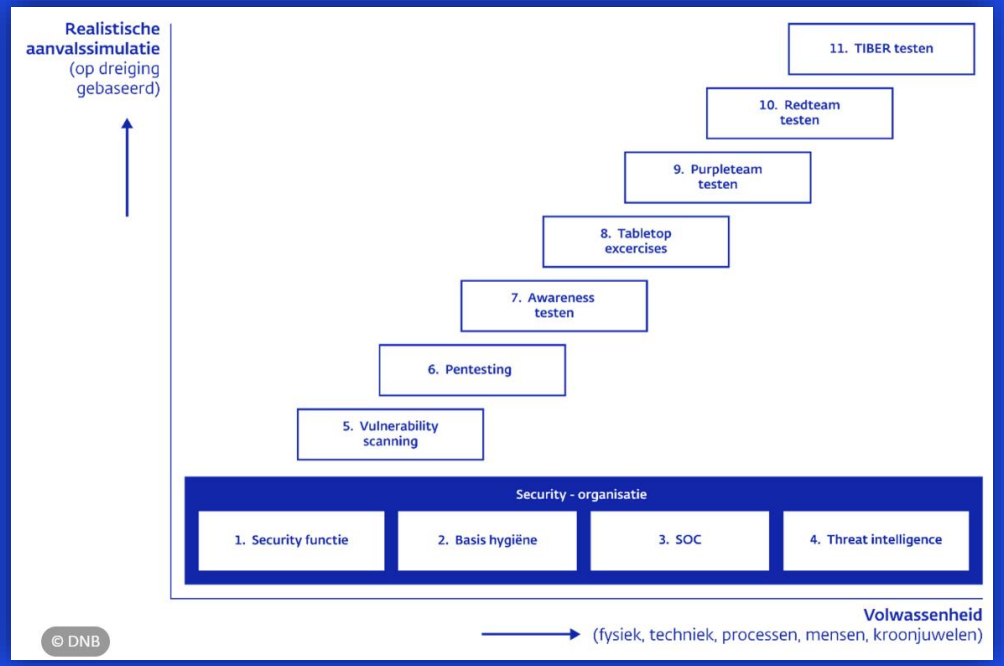


Operational resilience testing

Observaties en uitdagingen

- **Ontbrekende strategische visie op DOR-testen.**
- **Verschillende testen (bijv. vulnerability tests, pentests, business continuity tests) staan nog veelal los van elkaar.**
- **Samenwerking in de keten bij het uitvoeren van testen lastig.**

Pas het model van DNB toe om tot een securitytest-roadmap te komen!



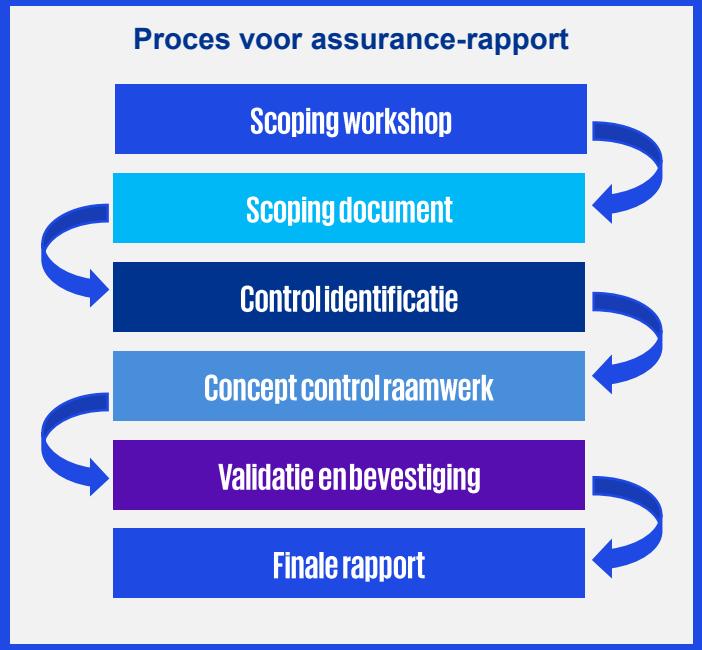
Bron: www.dnb.nl/nieuws-voor-de-sector/toezicht-2023/bereid-je-voor-op-een-cyberaanval/

Third Party Risk Management

Observaties en uitdagingen

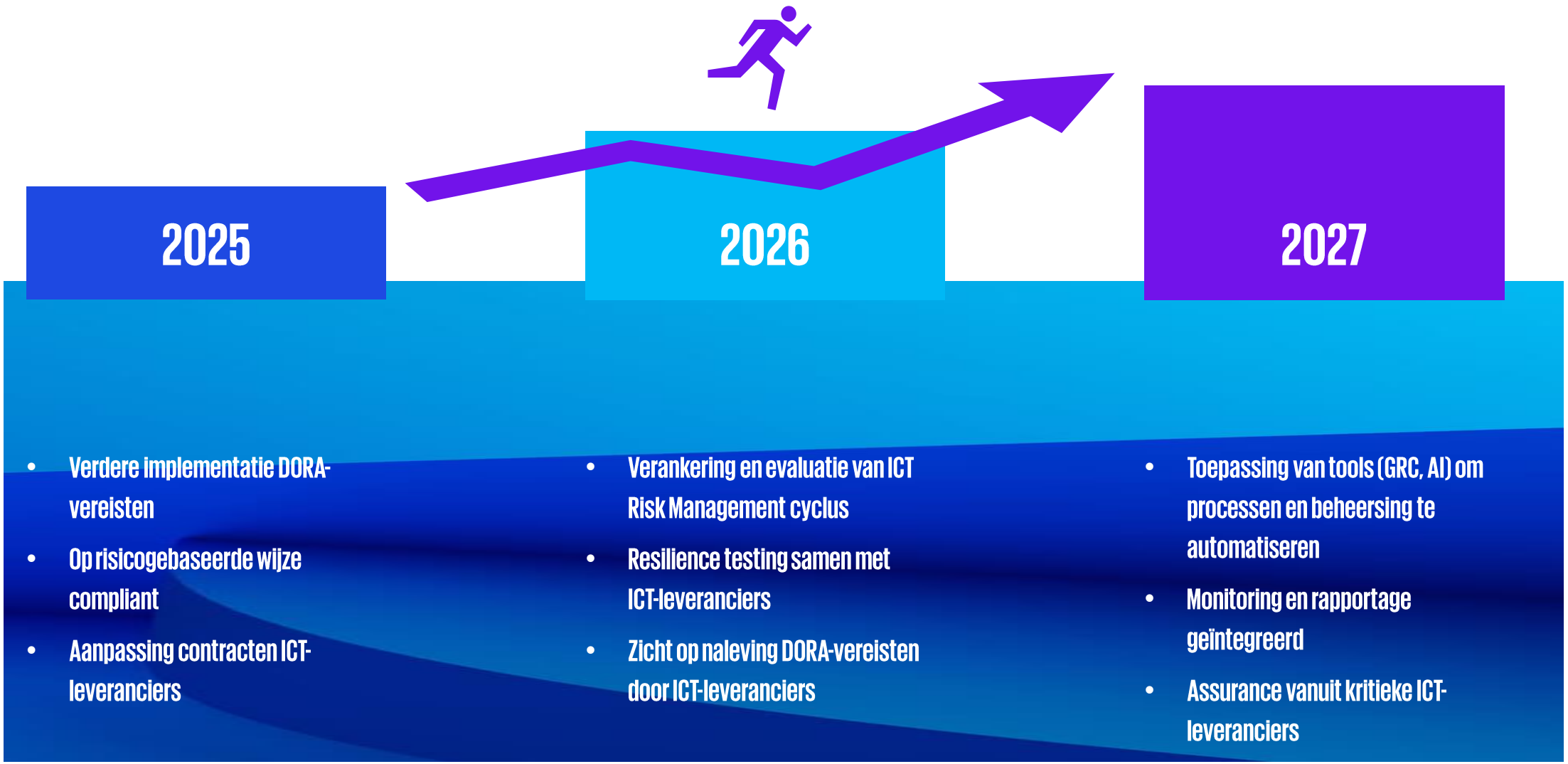
- **Informatieregisters tijdig aangeleverd, ondanks verschillen in validaties. Nog geen sectorbrede terugkoppeling.**
- **Inzicht krijgen in onderuit-bestedingen in de keten lastig.**
- **Aanpassing ICT-contracten nog lopend. Addendum* roept bij leveranciers nog veel vragen op.**
- **Wel / geen assurance van (kritieke) ICT-leveranciers?**

Kritieke ICT-leveranciers:
Voorkom vragen door zelf een DORA assurance rapport op te leveren!



* *DORA-clausules voor aanpassing van contracten, opgesteld door DUFAS, VV&A, Pensioenfederatie en Verbond van Verzekeraars.*

DORA outlook 2025 - 2027



Vragen?

Arno Kroese

Director IT Assurance & Advisory

KPMG Nederland

Artikel (juni 2025):

De proef op de DORA-som: De weg naar duurzame compliance

https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/sectoren/dora-duurzame-compliance-verzekeringen.pdf