



DORA-wetgeving: Hoe staat het ervoor?

VIP CONGRES

1 juli 2025

Introductie



Arno Kroese

Director IT Assurance & Advisory
KPMG Nederland

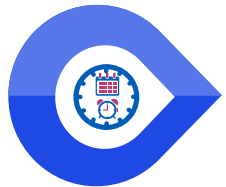
DORA: om uw geheugen op te frissen



Verbeteren digitale operationele weerbaarheid



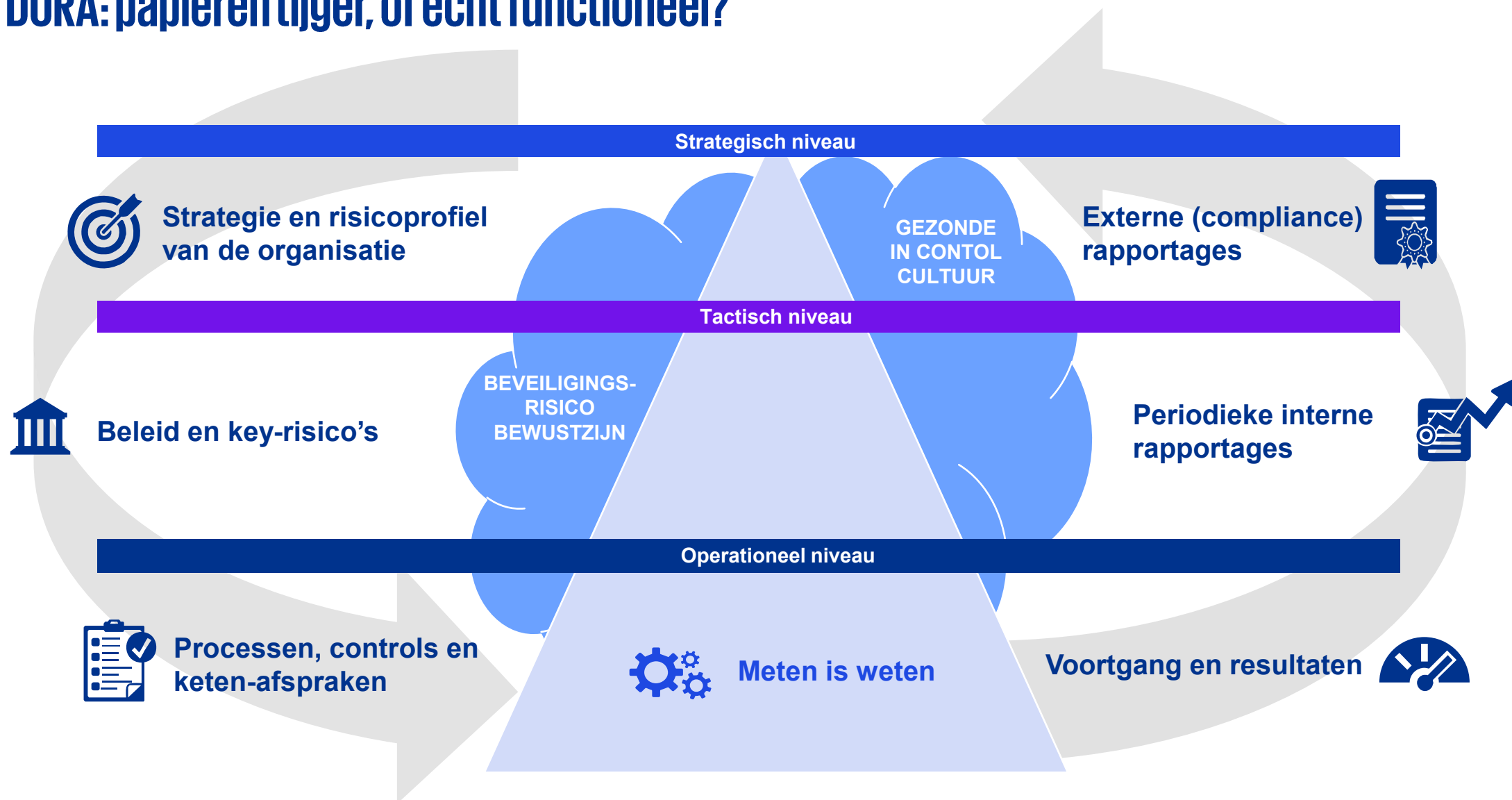
Financiële sector + ICT-leveranciers



Aantoonbaar compliant vanaf 17 januari 2025



DORA: papieren tijger, of écht functioneel?

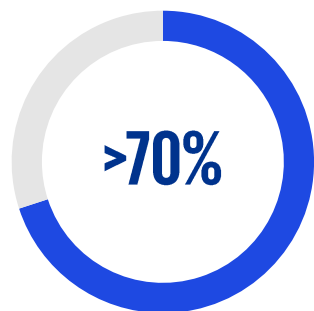


De belangrijkste uitdaging is om de balans te bewaren tussen aantoonbare naleving van de DORA-vereisten en focus op daadwerkelijke weerbaarheid!

Tot eind 2025 nodig om DORA-implementatie te voltooien!

DeNederlandscheBank

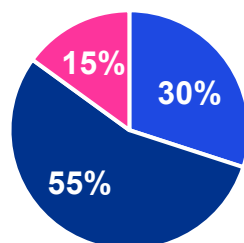
EUROSYSTEEM



Meer dan 70% van de inspanningen voor implementatie gerealiseerd

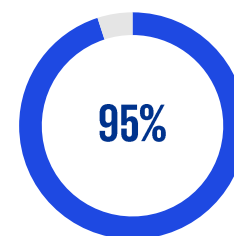
Veel instellingen hanteren een risicogebaseerde aanpak voor de implementatie

Hoeveel tijd nog nodig?

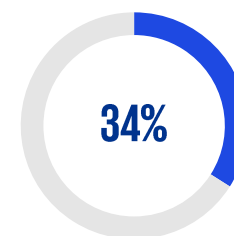


- 0 - 6 maanden
- 6 - 12 maanden
- > 1 jaar

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

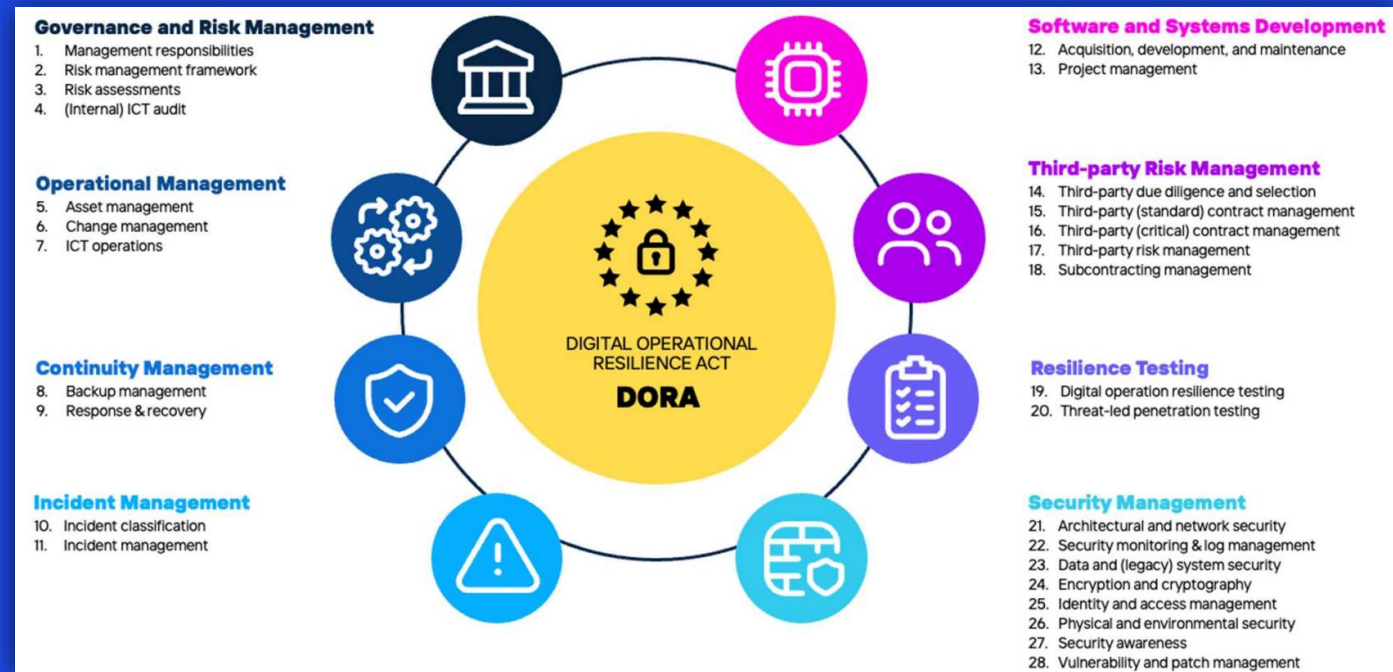
Bron: Resultaten sectorbrede (verzekerings- en pensioensector) uitvraag naar DORA-implementatie van DNB (gepubliceerd: 28 mei 2025)

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)



Please answer the following 8 questions:

1. Does the incident impact critical services?

Assess if the incident:

a) affects or has affected ICT services or network and information systems that support critical or important functions of the financial entity;
b) affects or has affected financial services that require authorisation, registration or that are supervised by competent authorities; or
c) represents a successful, malicious and unauthorised access to the network and information systems of the financial entity.

☐ Yes - please continue with question 2

☐ No - this means the incident is not a major incident and this does not require reporting to the competent authorities. You can stop with this questionnaire.

2. Is unauthorised access to network and information systems identified, which may result in data losses?

☐ Yes - If question 1 and 2 are answered with 'Yes', then it's a major incident that requires reporting under DORA. You can stop with this questionnaire.

☐ No - might be a major incident, please continue with six follow-up questions. If two of them are 'Yes', it's a major incident. Otherwise, it's not a major incident and this does not require reporting to the competent authorities.

3a. Clients, financial counterparts and transactions - does the incident meet any of the following conditions?

a) the number of affected clients is higher than 10% of all clients using the affected service; or
b) the number of affected clients is higher than 100,000 clients using the affected service; or
c) the number of affected financial counterparts is higher than 30% of all financial counterparts carrying out activities related to the provision of the affected service; or
d) the number of affected transactions is higher than 10% of the daily average number of transactions carried out by the financial entity related to the affected service; or
e) the amount of affected transactions is higher than 10% of the daily average value of transactions carried out by the financial entity related to the affected service; or
f) any identified impact on clients or financial counterparts which have been identified as relevant as an outcome of the assessment made by the financial entity under Article 1(3).

☐ Yes

☐ No

3b. Data losses - does the incident have any impact on the availability, authenticity, integrity or confidentiality of data, which has or will have an adverse impact on the implementation of the business objectives of the Financial Entity or on meeting regulatory requirements?

1. availability of data – data on demand rendered temporarily or permanently inaccessible or unusable;
2. authenticity of data – compromised trustworthiness of the source of data;
3. integrity of data – data inaccurate or incomplete due to non-authorised modification;
4. confidentiality of data – data being accessed by or disclosed to an unauthorised party or system.

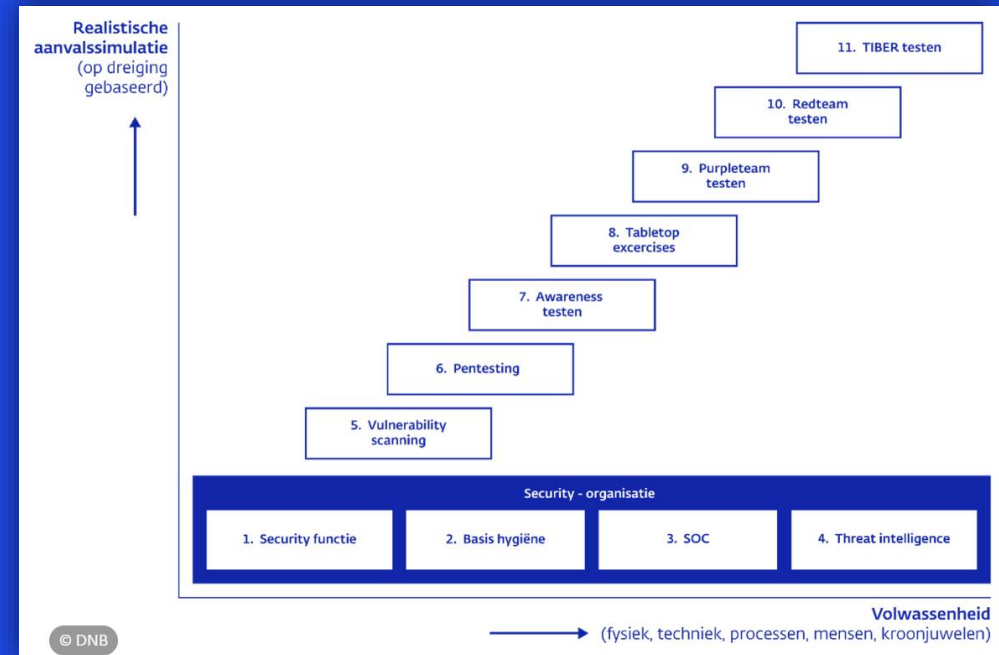
☐ Yes

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 onderuitbestedingen in de keten lastig.**
- **Aanpassing ICT-contracten nog lopend. Addendum* roept bij leveranciers nog veel vragen op.**
- **Wel / geen assurance van (kritieke) ICT-leveranciers?**

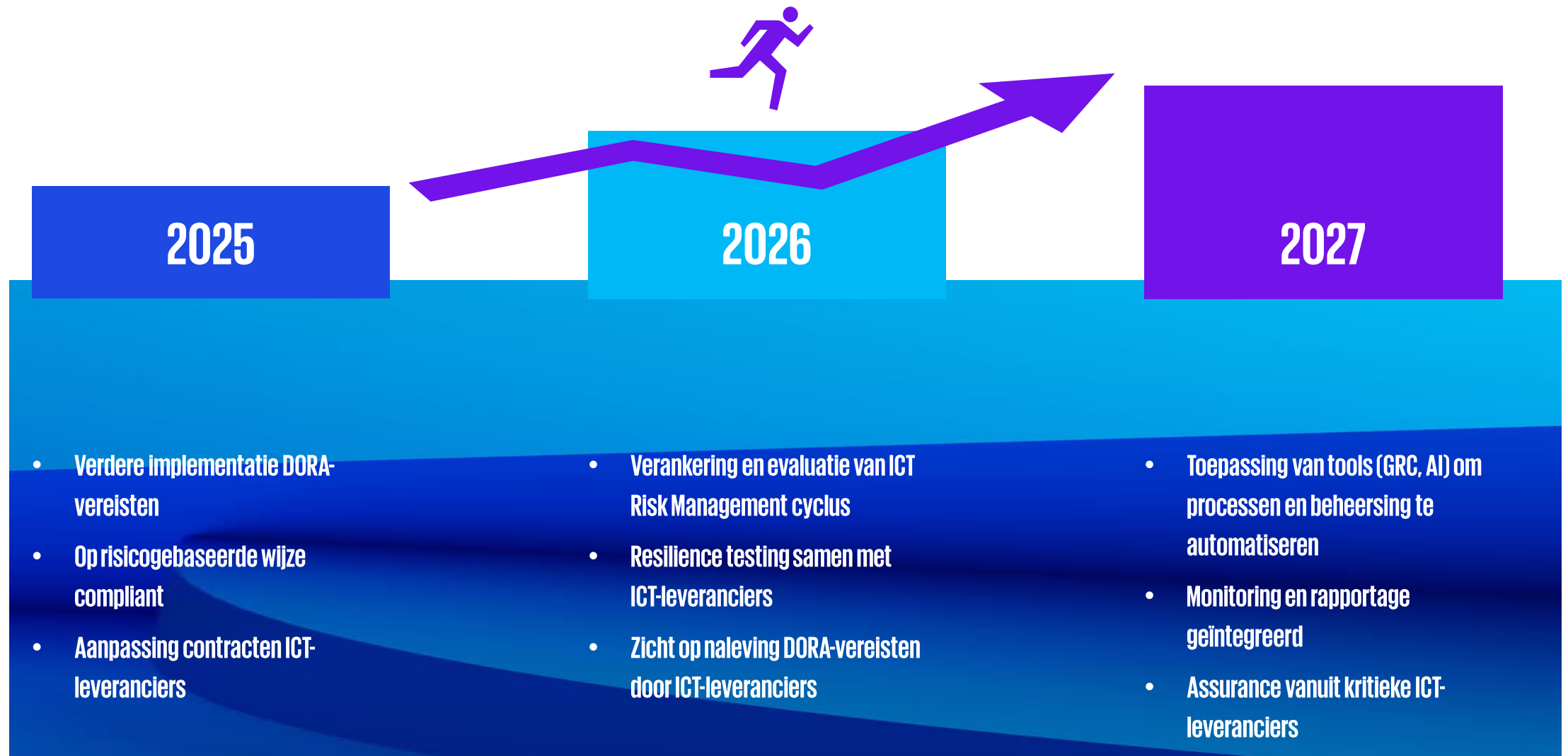
Kritieke ICT-leveranciers:

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>