# NIS2: wat kunnen we leren van DORA implementatie?

Information risk management en cybersecurity

Erik Zoetmulder – Danny Bos

Versie maart 2026

eraneos

Public

# Even voorstellen


**Danny Bos**

Regulatory implementation

Danny.Bos@eraneos.com
+31623992525

**Erik Zoetmulder**

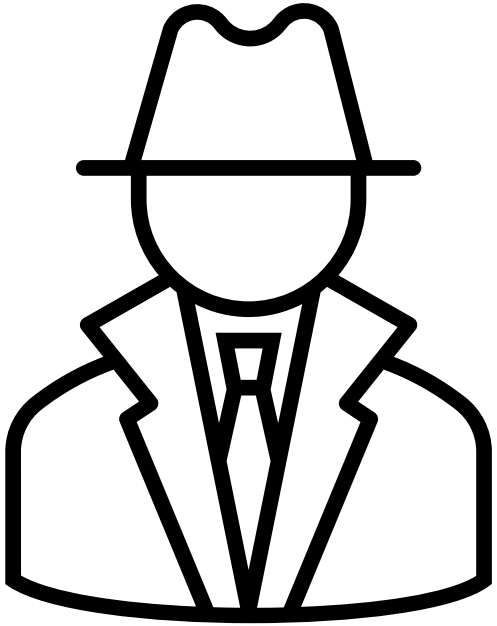
Regulatory implementation

Erik.zoetmulder@eraneos.com
+31622574613

# Vooraf

Twee vragen:

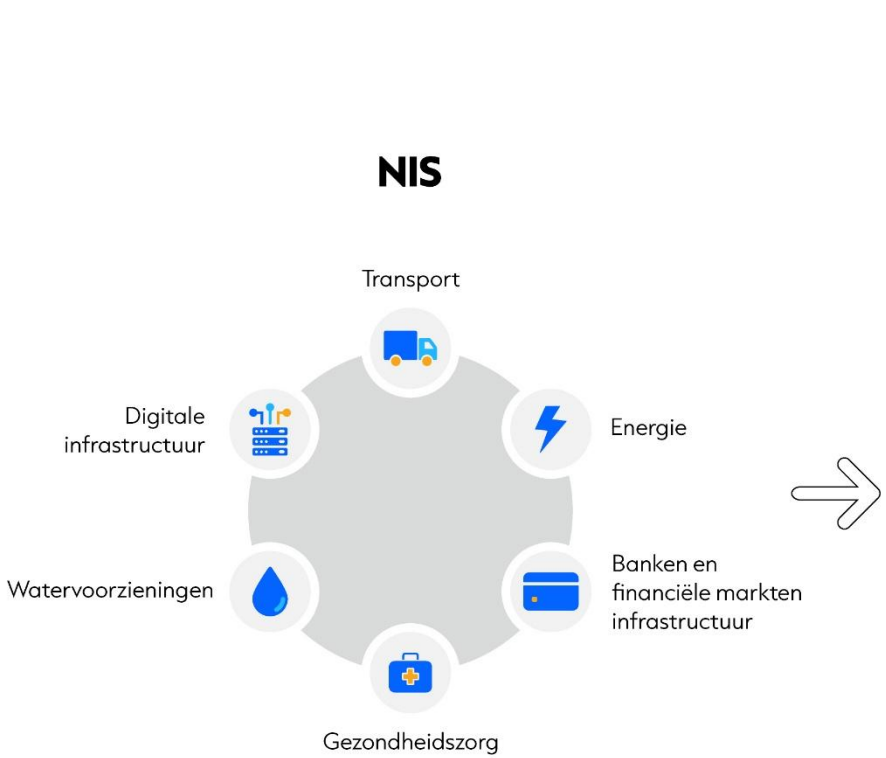
1. Welke vragen zou je idealiter in deze presentatie behandeld willen zien?
2. Is compliant zijn met NIS2 de reden dat je hier luistert?



# NIS versus NIS2: Uitbreiding sectoren

## Kritieke sectoren en relaties in de supply chain

Meer sectoren en industrieën zijn gereguleerd





Het directe bereik van NIS2 is vergroot en de indirecte effecten via de toeleveringsketen zijn nog veel groter

eraneos



Public

# Bevoegde autoriteiten per sector

## Sectorale toezicht en toezichthouder

Rijksinspectie Digitale Infrastructuur
*Ministerie van Economische Zaken en Klimaat*

**Ministerie van Economische Zaken en Klimaat**

- Digitale Dienstverleners
- Digitale Infrastructuur
- Ruimtevaart
- Postdiensten
- Productie
- Energie
- Onderzoek

**Ministerie van Financiën**

- Banken en financiële markten
- Onderzoek

**Ministerie van Infrastructuur en Waterstaat**

- Transport
- Water-voorzieningen
- Chemische sector
- Afvalbeheer
- Onderzoek

**Ministerie van Volksgezondheid, Welzijn en Sport**

- Gezondheidszorg
- Onderzoek

**Ministerie van Binnenlandse Zaken en Koninkrijksrelaties**

- Overheids-diensten
- Onderzoek

**Ministerie van Landbouw, Natuur en Voedselkwaliteit**

- Voedings-middelen
- Onderzoek

**Ministerie van Onderwijs, Cultuur en Wetenschap**

- Onderwijs
- Onderzoek

eraneos



Public

# DORA Is lex specialis van NIS2 voor de financiele sector

## En is onderdeel van het ”Europe fit for a Digital Age”-pakket

**Overlappende thema’s** creëren die naadloos kunnen worden aangepakt vanuit een **holistische** benadering.


Network and Information Security directive (NIS2)

Cyber Security Act

Artificial Intelligence Act

European Banking Authority (EBA) Guidelines

General Data Protection Regulation (GDPR)

Banking Recovery & Resolution Directive (BRRD)

Payment Service Directive 2 (PSD2)

# NIS2 is Richtlijn, DORA een verordening

Korte toelichting EU-terminologie

Een **verordening** is een bindende rechtshandeling. Deze zijn van algemene toepassing, in al hun onderdelen verbindend en rechtstreeks toepasselijk in EU-lidstaten..

DORA en GDPR zijn voorbeelden van verordeningen.

**vs**

Een **richtlijn** is een juridisch instrument van de EU om nationale wetgeving binnen de EU op elkaar af te stemmen. Elke lidstaat is bevoegd om hiervoor intern de toepasselijke methode te kiezen.

NIS2 is een richtlijn.

**DORA als “lex specialis” krijgt voorrang boven “lex generalis” NIS2.**
**DORA is dus in alle landen hetzelfde geïmplementeerd.**

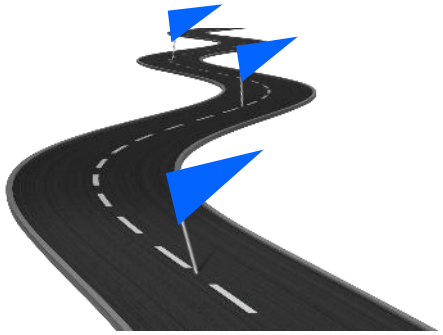
**NIS2 implementatie kan dus verschillen per land**


**Wat als je zowel onder DORA valt als NIS2?**

# DORA concretiseert bestaande vereisten en introduceert nieuwe onderdelen

DORA kent 5 onderdelen vanuit de wetsartikelen (level 1) met aanvullende eisen (level 2)

De weg naar compliance hangt af van de voorgaande implementatie van regulering en volwassenheid hiervan.



Chapter II

ICT Risk Management

Governance, ICT risk management framework, informatie risk- en -security management, BCM requirements.

Chapter III

Incident Management

Aanpak, classificatie en rapportage van ICT-gerelateerde incidenten(en cyber dreiging).

Chapter IV

Resilience Testing

Testspecificatie voor ICT-tools en -systemen, inclusief op bedreiging gebaseerde penetratietesten.

Chapter V

3rd Party Risk Management

Risicobeheer voor het gebruik van ICT-diensten bij externe ICT-aanbieders langs de gehele outsourcing- en leverancierskete en Europees het monitoringskader voor kritische externe ICT-dienstverleners

Chapter VI

Information Sharing

Vertrouwelijke uitwisseling van informatie en inzichten over cyberdreigingen tussen financiële instellingen en externe ICT-aanbieders

# DORA legt heel specifieke nieuw en gedetailleerd eisen neer

Met name de level 2 (RTS) teksten bevatten nieuwe en specifieke eisen*

- NIS2 is meer principle based dan DORA, DORA kent heel veel rules

Aantal level 1 eisen per pilaar

Aantal level 2 eisen per pilaar

**ICT Risk Management** *(Chapter II)*

Level 1: 92

Level 2: 339

**Incident Management** *(Chapter III)*

Level 1: 23

Level 2: 140

**Resilience Testing** *(Chapter IV)*

Level 1: 23

Level 2: 124

**3rd Party Risk Management** *(Chapter V)*

Level 1: 44

Level 2: 153

**Information Sharing** *(Chapter V)*

Level 1: 5

Totaal: 943

*Indicatief aantal uit Eraneos gap-analyse aanpak



Public

# Kritieke of belangrijke functies vormen de top van de DORA-piramide

Met daaronder de kritieke en belangrijke processen, leveranciers, data en systemen

- NIS2 kent geen CoIF maar je kan Risico's
- alleen effectief beheren als je weet wat je
- belangrijkste processen zijn

## Kernvragen voor CoIF's

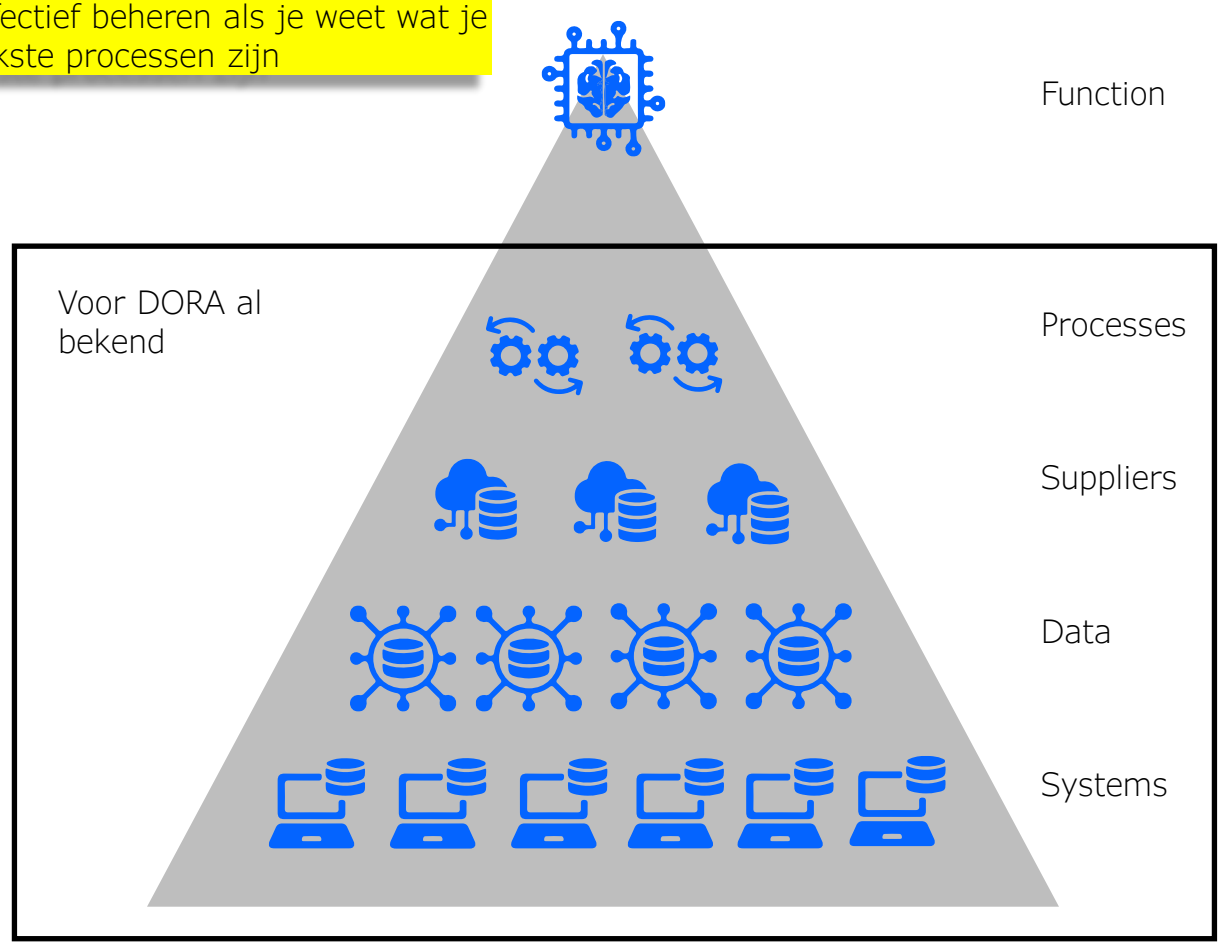
Extern perspectief:
Leidt een verstoring tot:

- Verstoring van diensten die essentieel zijn voor de economie?
- Verstoring van de financiële stabiliteit door (internationale) omvang of marktaandeel?

  En: Kunnen de activiteiten of diensten gemakkelijk worden vervangen (substitution)?

Intern perspectief:
Beïnvloedt een verstoring op drastische wijze:

- De financiële prestaties?
- De continuïteit van de dienstverlening?
- De naleving van verplichtingen onder de financiële wetgeving (vergunning om te opereren)?



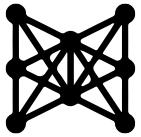

**Veel bedrijven gebruiken de BCM (BIA's) als basis**


Public

# Hoe interpreteert jullie organisatie CoIF?
Praktische voorbeelden ter bespreking

Het niet functioneren van een dienst die aan klanten wordt aangeboden:

- Impact heeft op de Nederlandse economie
- De beschikbaarheid of juistheid van de dienstverlening in gevaar is



Voorbeelden:

- Betalingsverkeer
- Verzekeren

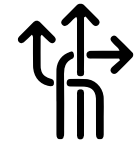
Het niet functioneren van een dienst die niet aan klanten wordt aangeboden:

- De financiële performance direct raakt
- De vergunning in gevaar brengt
- Een inbreuk veroorzaakt op financial services regelgeving

Voorbeelden:

- Treasury
- Client due dilligence
- Rapportage-verplichting

Als je aan de verplichting kunt blijven voldoen, op een andere manier, is er geen sprake van “niet functioneren”



Voorbeelden:

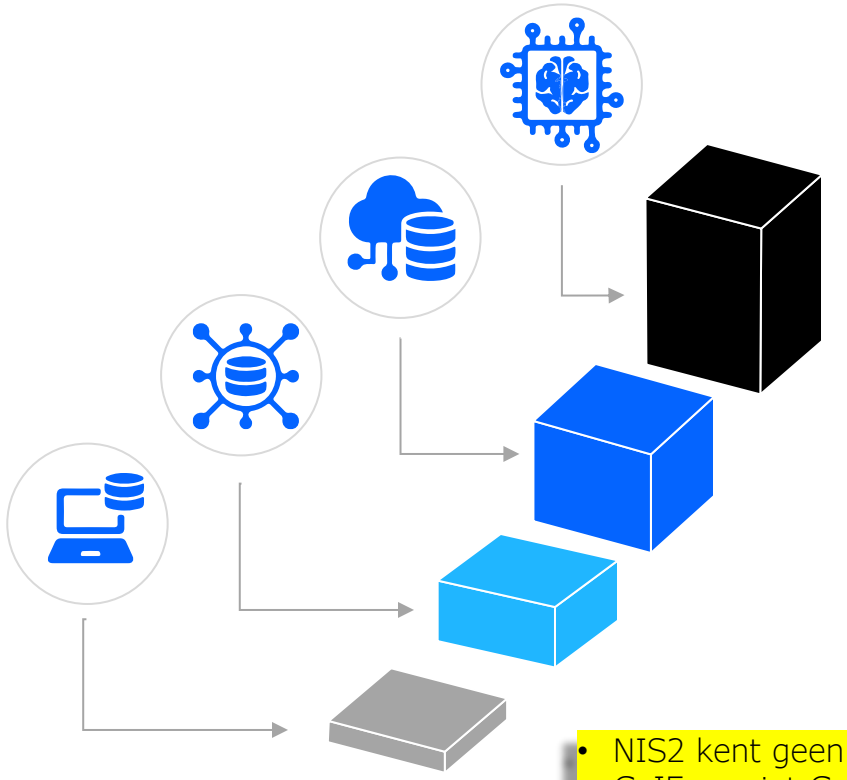
- Handmatig vs electronisch
- Geen sprake van tijdskritisch of datakritisch

**Echter DORA limiteert zich niet alleen tot CoIFs!**

**Welke scope zien we in de praktijk?**

# 3rd Party Risk Management

## Uitgangspunt ICT met toenemende eisen bij belangrijke en kritieke functies



- NIS2 kent geen verschil tussen
- CoIF en niet CoIF leveranciers maar
- verreist Risico gebaseerde aanpak:
- De CoIF-benadering kan je hierbij hanteren
- (extra contractuele eisen opnemen
- Als een leverancier essentieel is voor
- Een CoIF.

### Kritieke 3e partijen

Grote partijen waar de sector sterk afhankelijk van is vallen onder directe toezicht van de ESAs.

### 3e partijen onder CoIF functies

Organisaties dienen verscherpte eigen monitoring toe te passen. Risico's sourcing-mix, exit strategie.

### Overige ICT 3e partijen

Due dilligence en aanvullende eisen, tenminste rond business continuity en testing.

### Algemeen

Toepassing inkoopbeleid en reguliere inkoopvereisten, inclusief cybersecurity en risk management aspecten – concentration risk - en register of information.

Bepaald door Toezichthouder of op verzoek

Contractueel af te spreken



Public

# Bewegen van leveranciers management naar ketenregie

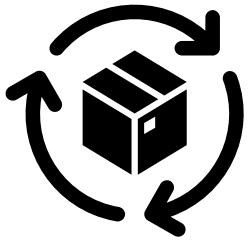
## De RTS Subcontracting is gericht op beheersing van de keten

Voor kritische of belangrijke functies:
([xkcd])

- NIS 2 beperkt zich tot  de directe leveranciers dus geen n-de partijen!
- Geen harde verplichte contractuele bepalingen
- Geen verplicht register van leverancierscontracten

**Risico inventarisatie**
Evalueer of de eigen organisatie en de ICT-subcontractor in staat zijn om de uitbestede dienst effectief te beheren, evenals de risico's die aan deze uitbesteding verbonden zijn.

**Ketenbeheersing**
Beschrijf contractuele verplichtingen voor het actueel houden van de keten en zie hierop toe.



**Voorwaarden in de keten**
Stel vast onder welke contractuele voorwaarden verdere uitbesteding is toegestaan.

**Ketenmonitoring**
Maak afspraken over materiële wijzigingen van subcontractors door de ICT-leverancier en ontbindingsrechten.

eraneos



Public

# Register of Information en incident meldingen
Onderschat de rapportageverplichtingen niet!

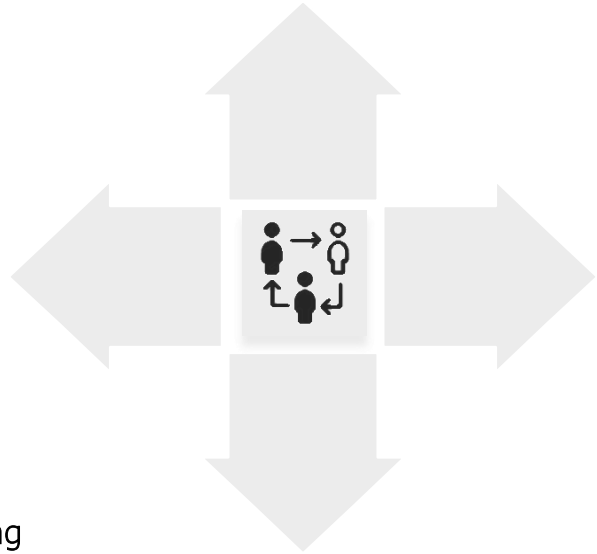
- NIS2 kent geen register of information
- NIS2 kent wel verplichte incidentmeldingen
- en tijdslijnennet als DORA.
- Maar format kan verschillen per land.

**Aanlevering**
Insturen via MyDNB via xBRL-CSV format: ook  dit jaar gestandaardiseerd excel van DNB beschikbaar.

Meest voorkomende fouten te vinden op DNB site:Update on DORA RoI reporting.pdf

**Doel toezicht korte termijn**
Bevat ALLE contracten met ICT leveranciers, ondersteunde processen, subcontractors, risico's.

Met dit inzicht wordt bepaald wie van de grootste leveranciers onder direct toezicht komen te staan. Dat zijn er tot nu toe 17



**Korte termijn vervolg**
terugkoppeling door EBA en kan DNB vragen om een nieuwe – dan gecorrigeerde – aanlevering

**Ontwikkeling**
Let op artikel 3 van de ITS on registration: Data Quality Principles. Datamodel met bepaalde kwaliteit is verplicht. Data Model for DORA RoI.pdf

RTS on subcontracting: onduidelijk hoeveel niveaus van subcontractors moeten worden bijgehouden. Wij verwachten 5 niveaus.

eraneos



Public

# Samenwerken in de supply chain voor DORA
## Acties om te nemen met 3e partijen

- Mogelijke leerpunten voor hoe u kunt omgaan met kritische 3e partijen

Gebruik een risico-gebaseerde aanpak om te bepalen welke onderwerpen meer aandacht verdienen bij verschillende soorten 3e partijen

Sluit 3e partijen expliciet aan op incident meldprocessen

Oefen en test business continuity en disaster recovery met 3e partijen

Onderwerp 3e partijen aan cybersecurity testen

Zorg voor afstemming van beleid tussen de organisatie en 3e partijen

Neem cyberweerbaarheid en cybersecurity mee als governance onderwerpen tijdens het contractperiode en zorg voor exit plannen

Monitor via rapportage hoge-risico onderwerpen naast reguliere beoordeling audit rapporten

Vraag 3e partijen hoe zij omgaan met training en awareness



Public

## Compliancy gericht

- Voldoen = klaar
- "Staat het in artikel 9? Dan doen we het."
- Controles ingesteld → audit-klaar!
- Afvinklijstjes & beleidsdocumenten – “We hebben gedocumenteerde policies”
- We hebben de trainingen afgevinkt (Click Through theatre)
- We hebben logs
- Risico's buiten de scope? Niet ons problem
- Evidence gericht (documentatie)

## Risico management

- Aandacht voor impact, niet alleen vorm
- "Wat zijn onze echte risico's?"
- Risk owner = betrokken & verantwoordelijk
- “We volgen onze policies gedisciplineerd”

- We leren en evalueren echt (PCDA)
- Proportionaliteit & context centraal
- We analyseren logs en nemen actie
- Continue verbetering van weerbaarheid
- Resultaatgericht

**NIS2 en DORA vereisen dit allebei**

**Toezichthouder ziet graag een risk based aanpak!**

# Praktijk: Drie Scenario's

## 🔥 Major Incident

**Compliance-bril**

*Log het incident in het systeem binnen 4u, stuur rapport naar DNB*

**Risk-bril**

*Waarom is het incident ontstaan? Welk risico zat er al langer onder de radar?*

💡 DORA Art. 17: Niet alleen rapporteren — ook root cause & lessons learned

## 🏭 Third Party Risk

**Compliance-bril**

*Zorg dat het contract de juiste clausules heeft (exit, audit, SLA)*

**Risk-bril**

*Wat als deze leverancier morgen wegvalt? Hebben we een scenario doorgerekend?*

💡 DORA Art. 28: Kritieke ICT-leveranciers vereisen concentration risk-analyse

## 🧪 TLPT / Pentesting

**Compliance-bril**

*Pentesten gedaan ✅ Rapport in de map ✅*

**Risk-bril**

*Wat testen we écht? Zijn de meest kritieke processen gedekt? Acteerden we op de bevindingen?*

💡 DORA Art. 26: TLPT voor significant instellingen — threat-led, niet checkbox-led

# ICT Risk Management

Raad van Bestuur heeft de volledige verantwoordelijkheid voor ICT Risk*

Organisatie
- €10 miljoen
- 2% totale jaarlijkse wereldwijde omzet

Bestuurders (persoonlijk)
- €1 miljoen


Zorg voor voldoende kennis, vaardigheden en continu leren om ICT-(cyber)risico's en de impact ervan te begrijpen

Opzet en periodiek herziening van ICT-gerelateerde rollen, governance, beleid, audit (plannen) en budget

Opzetten en goedkeuren van de Digital Operational Resilience Strategy (cyberweerbaarheis-strategie), inclusief het bepalen van het juiste ICT-risicotolerantieniveau

Inrichting incident meldproces inclusief ICT 3rd parties en materiële wijzigingen. ICT-gerelateerde grote incidenten zijn meldplichtig.

Toezichthouders kunnen maatregelen (o.a. boetes) nemen om ervoor te zorgen dat een organisatie blijft voldoen aan de wettelijke eisen
Deze maatregelen kunnen ook worden toegepast op leden van de Raad van Bestuur en andere personen

**Oversight** Doorlopend toezicht door de Raad van Commissarissen

eraneos

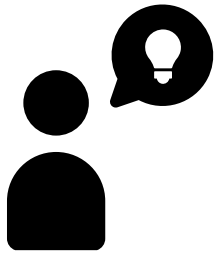
*DORA Articles 5 and 50



Public

# Rol invulling voor senior management

Drie gedragingen en 1 Digitale Operational Resilience Strategy om met vertrouwen verantwoordelijkheid te dragen



### 1. Actief inzetten op (cyber) weerbaarheid

Proactief

- Visie op de ontwikkeling van (cyber)weerbaarheid
- Begrip van de delta tussen visie en praktijk
- Kennis van de implementatie status

### 2. Bijsturen op basis van risico's

Risico-gebaseerd

- (Cyber)weerbaaarheids-strategie (DORS)
- Op risico gebaseerde jaarplan
- Rapportage over implementatie én de bereikte risico-verlaging

### 3. Voorbereiden op verantwoording

Uitlegbaar

- Duidelijke en verklaarbare keuzes
- Uitlegbare prioriteiten op basis van risico's
- Aantoonbare bijsturing

# DORA en NIS2 zijn “here to stay” en onderwerpen blijven zich ontwikkelen

Organisaties moeten dat ook; liefst op basis van eigen doelen en risico’s

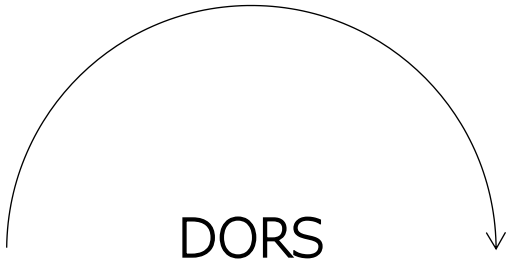
## Nog niet volledig?

Zorg voor planmatig opvolging van resterende gaps.

**Plan en stuur bij**
Maak een plan hoe de organisatie de resterende punten zal implementeren

Wees er op voorbereid dit plan te delen met de toezichtshouder

Stuur – als bestuur - op implementatie van dit plan



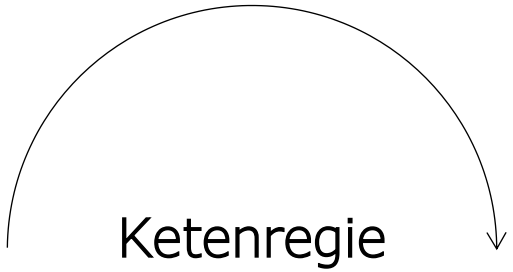
## DORS

Alles draait om resilience. DORS geeft dit invulling.

**Resilience als hoeksteen**
Compliancy alleen is hier onvoldoende.

Het gaat er om een lerende organisatie zijn of worden

In enkel landen buiten Europa is al aandacht voor brede resilience (dus niet alleen ICT)



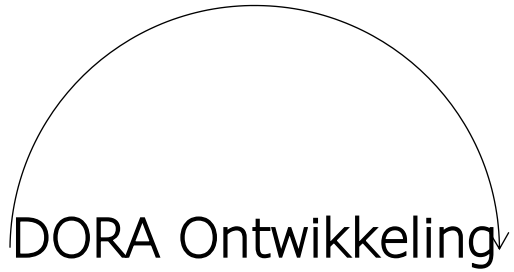
## Ketenregie

Kennen van afhankelijkheden ondersteunt resilience.

**Kritieke afhankelijkheden inzichtelijk**
Inzicht in de keten van leveranciers van leveranciers van leveranciers (5 niveaus) neemt meer tijd in beslag.

Samenwerking met de ICT leveranciers op gebied van cyberweerbaarheid is noodzakelijk.

.



## DORA Ontwikkeling

Nieuwe onderwerpen en verdiepingen vanuit de RTS’en.

**Onderwerpen in ontwikkeling**
Cloud soevereiniteit: nieuwe (oude) risico in huidige geopolitieke context is breed onder de aandacht.



Public

# Morgen mee beginnen
## Acties voor de hele korte termijn

### 1. Agendeer cyberweerbaarheid

Hoewel er meestal sprake is van reguliere rapportage over cybersecurity, is weerbaarheid niet overal onderdeel van de rapportagestroom. Zorg dat dit ook een eigen plek krijgt met monitoring op actuele dreigingen (ook geopolitiek).

### 2. Implementeer meldproces

Meldprocessen voor incidenten inrichten én testen voordat er zich een incident voordoet. Ook met leveranciers.

4 uur is een zeer kort tijdsbestek.

### 3. Train management

Zorg dat senior management getraind is. Hiermee help je eigenaarschap creëren, wat van belang is bij implementatie trajecten. Hiernaast is het een verplichting waar direct aan voldaan is.

### 4. Focus op kritieke functies

Ken je kritieke en belangrijke functies en zet hierop in met risico-gebaseerde keuzes. Zorg dat je weet welke (cloud) leveranciers hier zitten en zorg voor exit plannen.

Deze kritieke en belangrijke functies zijn de basis van een weerbare maatschappij.

**Permanente Educatie van de Management Body is key!**

(NOREA | DORA - Boardroom training guideline)

eraneos



Public

# Blijven doen voor de lange termijn

In 5 stappen bouwen aan vertrouwen door **proactief**, **risico-gebaseerd** en **uitlegbaar** te werken

Met je management team en je CISO ga je van acties naar resultaten voor verhoging van je cyberweerbaarheid.

**Actief inzetten op (cyber) weerbaarheid**

1. Ontwikkel een visie op weerbaarheid (DORS)

2. Stel een (cyber)weerbaarheids-strategie op

Duidelijke en verklaarbare keuzes

**Bijsturen op basis van risico's**

2. Analyseer de delta tussen visie en praktijk

3. Maak een risico-gebaseerde jaarplan voor relevante delta's

Uitlegbare prioriteiten op basis van risico's

**Voorbereiden op verantwoording**

4. Ontvang regelmatig rapportage over de implementatie

5. Stuur bij, waar nodig

Aantoonbare bijsturing



Public

# Hoe kijkt de toezichthouder naar DORA?

## Register of Information

## SBA Informatiebeveiliging

- Sector Brede Analyse over de financiële sector
- Gebaseerd op de Good Practice Informatiebeveiliging (2019/2023)
- Uitvraag algemene informatie over de organisatie
- Uitvraag  van de scores op alle 58 controls in de GP → Pensioenen / Verzekeren
- Banken hebben een uitgebreidere questionaire
- Toelichting optioneel
- Beantwoording kan onderdeel vormen van verder toezicht

## SBA Cyberweerbaarheid

- Sector Brede Analyse over de financiële sector
- Gebaseerd op DORA
- Uitvraag algemene informatie over de organisatie
- Uitvraag  van de scores op 46 door DNB gedefinieerde vragen → Pensioenen / Verzekeren
- Banken hebben een uitgebreidere questionaire
- Toelichting optioneel
- Beantwoording kan onderdeel vormen van verder toezicht

**Tip: Check NOREA InControl Framework**

# Links naar handige beschikbare guidance

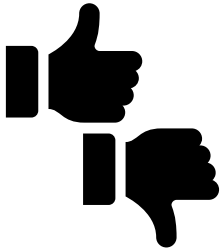
1. NOREA DORA InControl Framework
   - Microsoft Word - DORA in Control - A Practical Guide to Achieving Digital Resilience_V5.2
   - dora-in-control-framework-v32.xlsx
2. Auditdienst Rijk CBW (NIS2) Control Framework
   - Cbw (NIS2) Control Framework | Auditdienst Rijk
3. NOREA Boardroom Boardroom Training guideline
   - NOREA | DORA - Boardroom training guideline
4. NOREA Incident Classification Tool
   - NOREA | DORA Incident Classification Tool
5. NOREA Exit Plan Template
   - NOREA | DORA Template Exit Plan

**Disclaimer DNB:**
"DNB and AFM took note of the framework prepared by NOREA to provide guidance to the industry on practical implementation of DORA. DNB and AFM did not contribute to its development. Nor has the framework been assessed by DNB and AFM in terms of content. However, the development of such frameworks is in line with previous calls from DNB and AFM to work together within the sector to increase the overall cyber resilience of the sector and, if desired, to mutually develop and update standards that can contribute to this. DNB and AFM stress that complying with applicable laws and regulations is at all times a responsibility of the institution. No confidence can be derived from the use of such a framework that parties thereby act in line with laws and regulations."

- Tools en frameworks zijn geen garantie tot succes
- Zelf na blijven denken
- Kijken vanuit perspectief vanuit eigen organisatie
- Het verhaal is net zo belangrijk als de resultaten

# Dag afsluiting

1. Leerdoelen gehaald?



2. Feedback voor ons?



Public


Danny Bos
Regulatory Implementation

Danny.Bos@eraneos.com
+31623992525

Erik Zoetmulder
Regulatory Implementation

Erik.zoetmulder@eraneos.com
+31682012275


eraneos