Implementing DORA

Achieving enhanced digital operational resilience

21 oktober 2024

DeNederlandscheBank

EUROSYSTEEM

Opbouw van DORA

ICT risk management

- **Responsibility** continues to reside with the management body of the financial entity
- **ICT risk management and governance**
- **Technical requirements** (identify, protect, detect, response, recover)

ICT incident reporting

- Determination of **processes** for identifying, managing and reporting ICT-related incidents
- **Classification** of ICT-related incidents and cyber threats
- **Reporting of major ICT-related incidents** (and voluntary notification of cyber threats)

Testing of digital operational resilience

- **Basic testing**
- Entire financial sector
- Vulnerability scans, source code tests, performance tests, etc.

TLPT

- **Advanced testing**
- TLPT: threat led penetration tests
- Only ‘systemic and ICT-mature’ financial entities, TIBER-EU as ‘blueprint’

ICT third-party risk management

- **General principles** (incl. register of information covering ICT third-party contractual relationships, notices to the supervisory authorities and minimum contractual elements)

EU oversight framework

- Oversight of **critical ICT third-party service providers**

Information sharing and EU cyber exercises

- Voluntary **exchange of information and findings** between financial entities to raise awareness
- EU-wide cross-sector cyber-related **crisis management and contingency exercises** enabling an effective coordinated response at EU level

Beleidsmandaten

ICT risk management

- **RTS on ICT Risk Management framework (Art.15)**
- **RTS on simplified risk management framework (Art.16.3)**
- Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (Art. 11.1)

ICT incident reporting

- **RTS on criteria for the classification of ICT related incidents (Art. 18.3)**
- RTS to specify the reporting of major ICT-related incidents (Art. 20.a)
- ITS to establish the reporting details for major ICT related incidents (Art. 20.b)
- Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21)

Testing of digital operational resilience

- RTS to specify threat led penetration testing (Art. 26.1)

ICT third-party risk management

- **ITS to establish the templates of register of information (Art.28.9)**
- **RTS to specify the policy on ICT services performed by third-party (Art.28.10)**
- RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art.30.5)

EU oversight framework

- **Call for advice on criticality criteria (Art. 31.6) and fees (Art. 43.2)**
- Guidelines on “CAs-ESAs cooperation” regarding DORA oversight (Art. 32.7)
- RTS on “oversight conduct” (Art. 41)

ICT Risk Management & ATM

DeNederlandscheBank

EUROSYSTEEM

DNB Good Practice informatiebeveiliging & DORA

- Vanaf 17 januari 2025 is DORA het wettelijke kader voor operationele weerbaarheid en vervangt daarmee de huidige Good Practice Informatiebeveiliging 2023 voor de instellingen die onder de reikwijdte van DORA vallen.

- DNB zal DORA als wettelijk kader hanteren bij toekomstige uitvragen en onderzoeken (*uitzondering op volgende sheet).

- DNB zet zich in voor effectief en efficiënt toezicht op de financiële sector en hanteert hierbij een risicogebaseerde en proportionele benadering.

- Onder DORA zullen de bestaande toezichtmethoden niet drastisch veranderen. We continueren ons bestaande toezicht waarbij DORA nieuwe accenten introduceert.

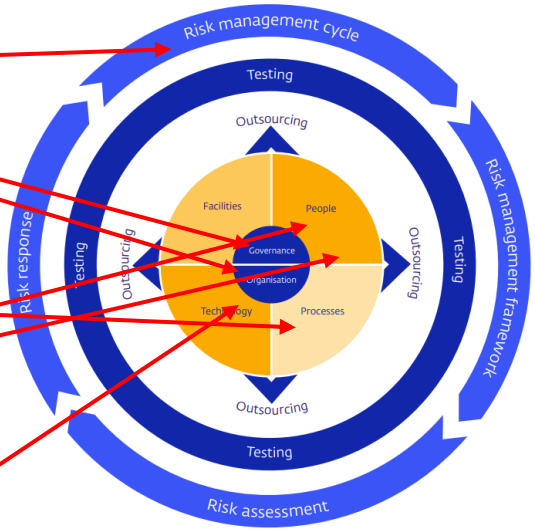
Sector-brede analyse informatiebeveiliging & DORA

- Voor de sector-brede analyse informatiebeveiliging (SBA-IB) hanteert DNB nog eenmalig de huidige questionnaire en systematiek gebaseerd op de DNB Good Practice informatiebeveiliging (peiljaar 2024).
    - In deze SBA-IB wordt wel een separate DORA vragenlijst opgenomen.

- Vanaf 2026 stuurt DNB een geactualiseerde vragenlijst uit, gebaseerd op DORA, die meer geharmoniseerd en gestandaardiseerd wordt over de verschillende toezichtdivisies heen.

DORA & Good Practice informatiebeveiliging

Art.	Onderwerp
5	Governance en organisatie
6	Kader voor ICT-risicobeheer
7	ICT-systemen, -protocollen en -instrumenten
8	Identificatie
9	Bescherming en voorkoming
10	Detectie
11	Respons en herstel
12	Back-upbeleid en -procedures, terugzettings- en herstelprocedures en -methoden
13	Scholing en ontwikkeling
14	Communicatie
15	Verdere harmonisatie van ICT-risicobeheersinstrumenten, -methoden, -processen en –beleidslijnen (RTS 2024/1774)



* Illustratief, niet uitputtend

DORA & Risico-gebaseerd toezicht

- DNB houdt risicogebaseerd toezicht, ook op DORA.
  - Dit betekent dat de toezichtcapaciteit wordt ingezet daar waar de grootste risico's worden gesignaleerd.
  - Bij de uitvoering van onze toezichtstaken is proportionaliteit een belangrijk uitgangspunt. De inzet van de toezichtcapaciteit is hoger naarmate de omvang, maar ook de complexiteit en de risico's, die een instelling of de financiële sector als geheel loopt, groter zijn.

- Risico's bepalen in belangrijke mate de toezichtsprioriteiten voor de aankomende periode. Nieuwsuitingen, seminars, en toezichtkalenders geven een goede indicatie waar die prioriteiten liggen.

DeNederlandscheBank
EUROSYSTEEM

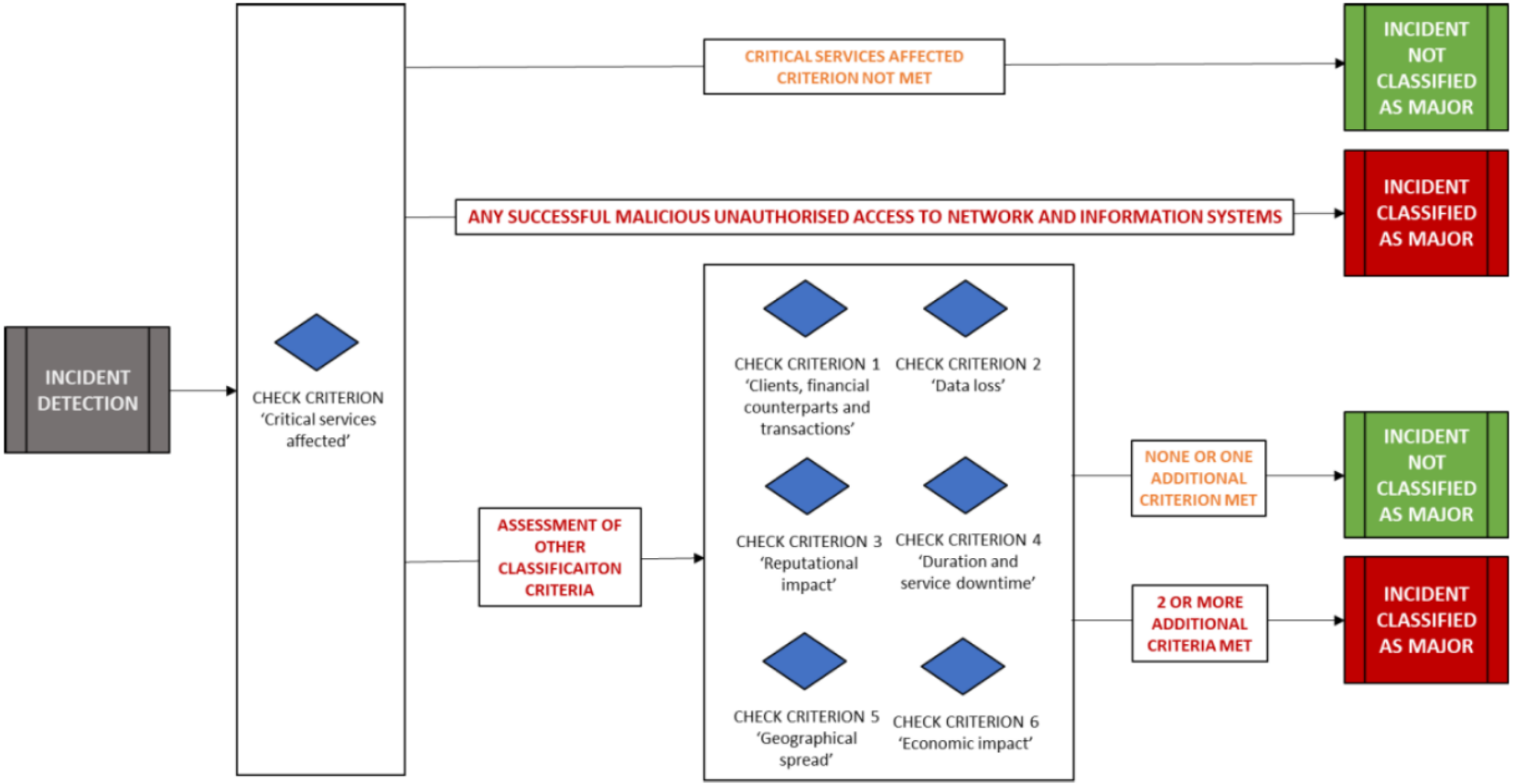
Voor meer informatie, zie de ATM brochure op dnb.nl
Brochure ATM | De Nederlandsche Bank (dnb.nl)

Major ICT-related incidents

DeNederlandscheBank

EUROSYSTEEM

Classificatie van ICT-gerelateerde incidenten



Melding van ernstige ICT-gerelateerde incidenten

- **Ad hoc melding** wanneer classificatie van het incident uitkomt op ‘major’
- Drie verschillende typen meldingen
  - **Initiële melding** binnen 4 uur naar classificatie als major
  - **Tussentijds verslag** binnen 72 uur na initiële melding, en bij significante wijzigingen
  - **Eindverslag** binnen 1 maand na het laatste tussentijdse verslag
- **10 velden** voor de initiële melding (e.g. datum, omschrijving, reden classificatie major)
- **Methode**: in het eerste half jaar 2025 upload Excel in Mijn DNB, besluit definitieve oplossing onderhanden.

Digital operational resilience testing

DeNederlandscheBank

EUROSYSTEEM

Testen van de digitale operationele weerbaarheid

1. **Artikel 24/25**: programma voor het testen van digitale operationele weerbaarheid
   Als deel van het ICT-risicobeheer

2. **Artikel 26/27**: TLPT

alle DORA-normadressanten

geselecteerde groep

DeNederlandscheBank
EUROSYSTEEM

Algemene vereisten

Een testprogramma **binnen** het kader van ICT-risicobeheer

Een reeks beoordelingen, tests, methodologieën, praktijken en instrumenten

Zie art 25

Met een risicogebaseerde benadering

Rekening houdend met proportionaliteit, het veranderende landschap van het ICT-risico, eventuele specifieke risico's waaraan de betrokken financiële entiteit wordt of kan worden blootgesteld, de kritieke aard van informatieactiva en verleende diensten, alsmede alle andere factoren die de financiële entiteit passend acht.

Algemene vereisten

Door interne of externe onafhankelijke partijen

Belangenconflicten moeten voorkomen worden

Opvolging door bevindingen te prioriteren, classificeren en verhelpen. Voortgang moet gevalideerd worden

Ten minste eenmaal per jaar op alle ICT-systemen en -toepassingen die kritieke of belangrijke functies ondersteunen

Type testen

- Eind-tot-eindtest
- Scenariogebaseerde test
- Penetratietest
- Beoordelingen van broncodes
- Kloofanalyse
- Prestatietest
- Compatibiliteitstest
- Opensourceanalyse
- Netwerkbeveiligingsbeoordelingen
- Beoordelingen van fysieke beveiliging
- Kwetsbaarheidsbeoordelingen en -scans
- Vragenlijsten en scanningsoftwareoplossingen

Uitzondering: micro-ondernemingen

Voor micro-ondernemingen geldt een op risico's gebaseerde aanpak waarbij enerzijds rekening wordt gehouden met de hoeveelheid middelen en tijd die nodig zijn voor het uitvoeren van de tests en anderzijds de urgenties, het soort risico, de kritieke aard van het ICT systeem en eventuele andere relevante factoren.

TLPT

Aanwijzing volgt op of na 17 januari 2025
Periodieke review door DNB

Planning houdt rekening met laatste TIBER-test

TIBER geeft extra guidance

Interne testers eens in 3 keer niet toegestaan

TLPT een van vele bronnen voor beoordeling toezicht
Geen automatische reactie, maar bevindingen worden niet genegeerd

Aan de slag

Het opstellen van een risicogebaseerd programma voor het testen

Reserveren van fondsen op begroting aankomend jaar

Hou rekening met inkooptijdslijnen

DeNederlandscheBank
EUROSYSTEEM

Uitbesteding en ICT diensten

DeNederlandscheBank

EUROSYSTEEM

Bestuurlijke verantwoordelijkheid

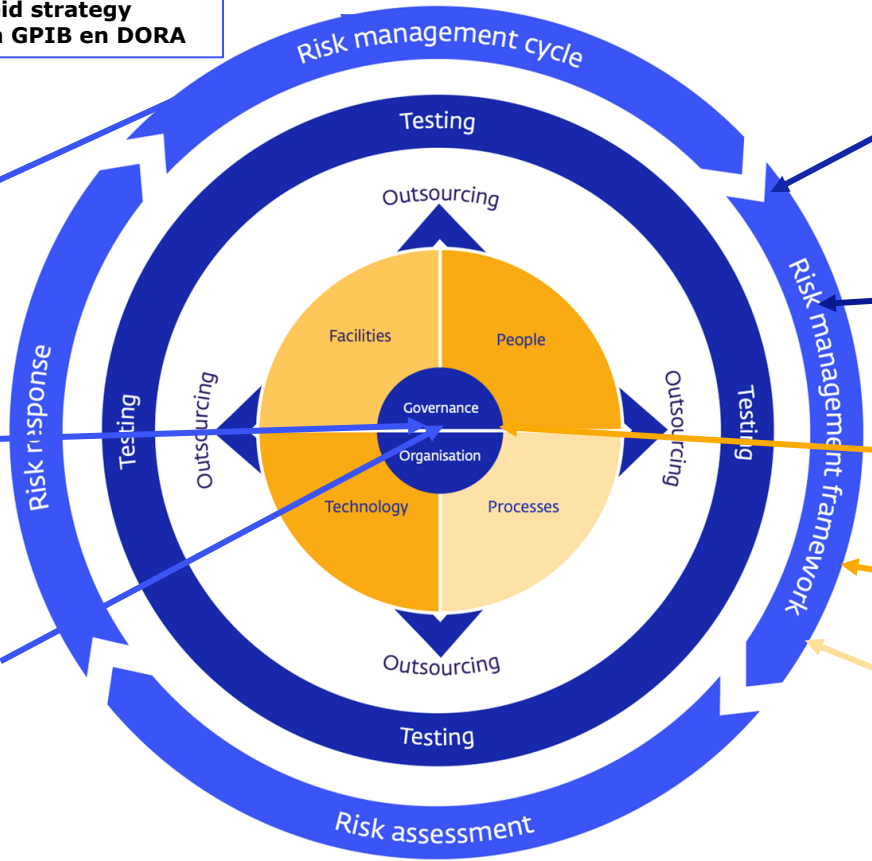
Digitale operationele weerbaarheid strategy raakt alle aandachtsgebieden van GPIB en DORA

ICT riskmanagement Framework art.6
6.8 Include a Digital Operational Resilience (DOR) strategy & approprioate risk tolerance levels of ICT risk

art 2(d)

Governance & Organisation art.5
5.2. responsibilty management body
5.4. actively keep up to date knowledge & skills

ICT Riskmanagement art.5-16 & RTS 15-16
Raakt G&O en alle vier kernelementen



Digital Operational Resiliency Testing art. 24-26
6.8(g) Attain DOR strategy & objectives implementing testing

Managing ICT Third Party Risk art 28-30
28.1 Manage TPP Risk as integral component of ICT risk within ICT RMF

Learning & Evolving art.13

Communication art.14
6.8 (h) Outlining communication strategy and policies for different levels

Incident management art. 17-23
6.8(f) Evidencing current DOR on base of number major incidents

DeNederlandscheBank
EUROSYSTEEM

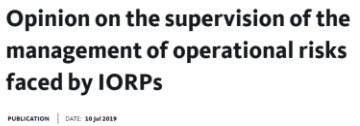
Huidige uitbesteding regelgeving

- Wet financieel toezicht artikel 3:18 – beheerste uitbesteding
- Besluit Prudentiële regels: artikelen 27 – 32 over uitbesteden van werkzaamheden

- Solvency II Richtlijn art. 49 (Wft) & Solvency II Verordening art. 274
- EIOPA governance richtsnoeren 60-64 in afdeling 11 over uitbesteding

- Pensioenwet (PW) art 34 en Wet Verplichte Beroepspensioenregeling (WVP) art.43
- Besluit uitvoering PW en WVP artikelen 12 – 14 over uitbestedingsrisico's en meldplicht
- Q&A melding uitbesteding van werkzaamheden bij DNB; beleidsregel die meldplicht beperkt tot alleen kritieke en belangrijke uitbestedingen

- ESA Guidelines on (cloud)outsourcing arrangements; EBA, EIOPA en ESMA
- Guidance Uitbesteding, Good Practice Uitbesteding & Informatiebeveiliging
- IORP opinie met verwijzing naar outsourcing (en cyberrisk)



DeNederlandscheBank
EUROSYSTEEM

Uitbesteding regelgeving na 17 januari 2025

- DORA: hoofdstuk V - artikelen 28 – 44

- ITS to establish the templates of register of information (Art.28.9)
- RTS to specify the policy on ICT services performed by CTPP's (Art.28.10)
- RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (CIF) (Art.30.5)

Verzekeraars niet S2 en Dora plichtig Premie onder drempelwaarde

- ❑ Wft artikel 3:18 – beheerste uitbesteding & BPR artikelen 27 – 32
- ❑ Solvency II Richtsnoer (Wft)
- ❑ Solvency II Verordening en Richtsnoeren H11

Verzekeraars

Pensioensector

- ❑ PW art 34 & WVP art 43 en besluit uitvoering PW & WVP

Intrekken of herschrijven of in stand houden

- ESA Guidelines on (cloud)outsourcing arrangements
- IORP opinie en Q&A meldplicht
- Good practices behouden tbv niet DORA plichtige instellingen

DeNederlandscheBank
EUROSYSTEEM

ICT contractenbeleid

"RTS to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers"

Wanneer van toepassing?

- Als onderdeel van ICT-risicostrategie en beleid bij uitbesteding
- Contracten met aanbieders van ICT-diensten die kritieke of belangrijke functies (KBF's) ondersteunen
- Niet alleen 'externe' IT-leveranciers, maar ook in geval van intragroep uitbesteding
- Ook onderaannemers verderop in de keten die Kritieke of belangrijke functie ondersteunen
- Volgt de lifecycle uit DNB guidance / good practices
- Niet: micro-ondernemingen of entiteiten die onder vereenvoudigd kader ICT-risicobeheer vallen: pensioenfondsen minder dan 100 deelnemers

Evaluatie beleid (minimaal 1x per jaar)

Onderuitbesteding kritieke functies

"RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by article 30.5 n.b. kunnen nog wijzigingen worden doorgevoerd op het Final Draft, nog niet goedgekeurd door EC

Wanneer van toepassing?

- Wanneer onderuitbesteding is toegestaan
- Contracten met aanbieders van ICT-diensten die kritieke of belangrijke functies ondersteunen
- Niet alleen 'externe' ICT-leveranciers, maar ook in geval van intragroep uitbesteding
- Vastleggen welke voorwaarden van toepassing zijn
- Afspraken over meldings- en rapportagekanalen

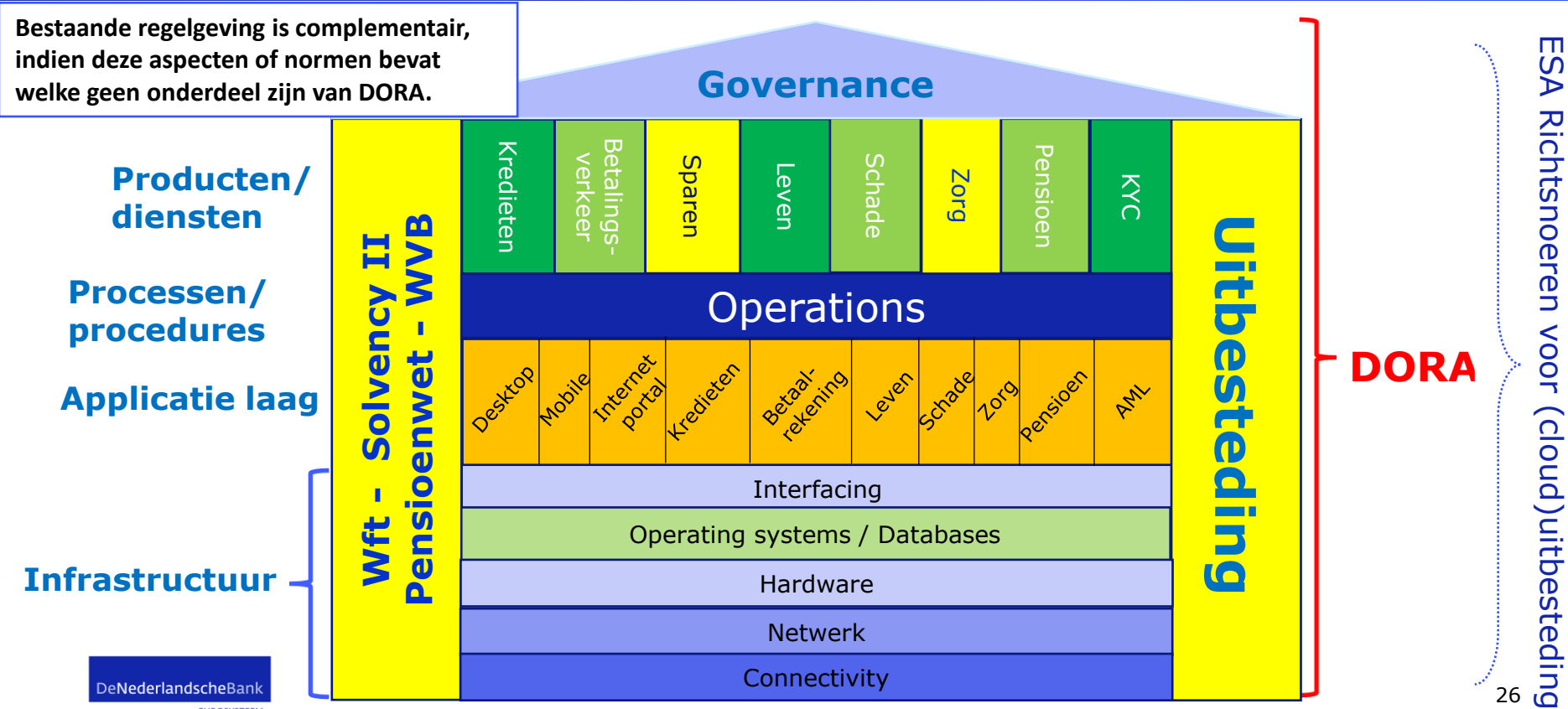
FE blijft volledig verantwoordelijk voor het managen van de risico's, ook in geval van serviceproviders onder oversight.

DeNederlandscheBank
EUROSYSTEEM

Pensioenfondsen hebben onvoldoende zicht op langer wordende uitbestedingsketens (dnb.nl)
Verzekeraars hebben onvoldoende zicht op langer wordende uitbestedingsketens (dnb.nl)

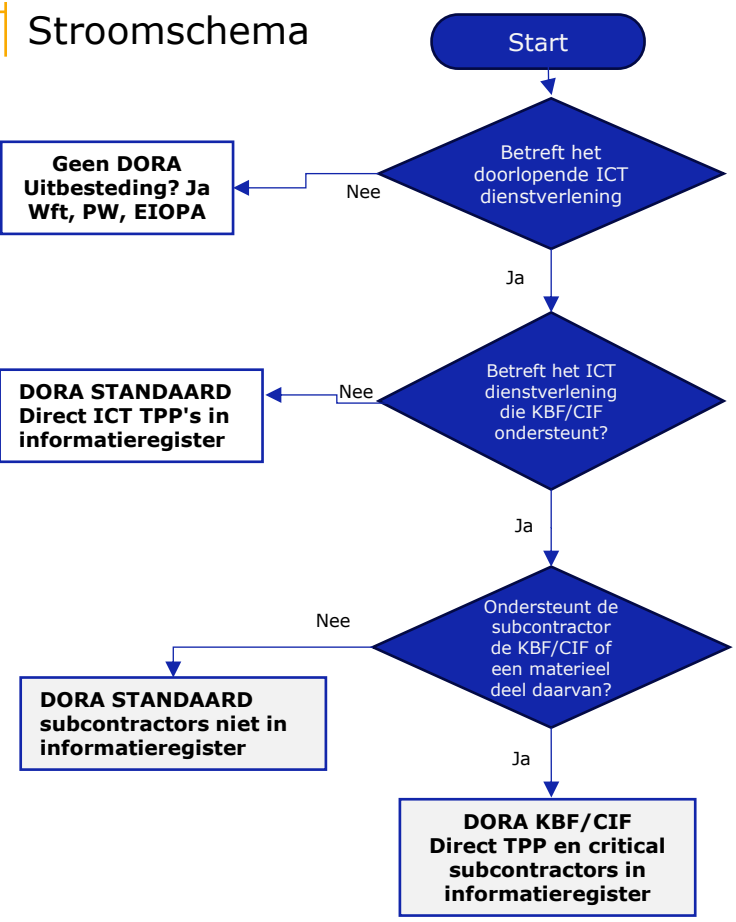
Schets na 17 januari 2025 – Uitbesteding & ICT

Bestaande regelgeving is complementair, indien deze aspecten of normen bevat welke geen onderdeel zijn van DORA.



DeNederlandscheBank
EUROSYSTEEM

Stroomschema



DeNederlandscheBank
EUROSYSTEEM

ICT dienstverlening: "digitale en gegevensdiensten die doorlopend (niet eenmalig) via ICT-systemen aan een of meer interne of externe gebruikers worden verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten".

Annex 3 van ITS on register of information kent een tabel met alle type ICT diensten die in het informatieregister opgenomen moeten worden.

Voorbeelden ICT dienstverlening wel DORA (niet uitputtend): **zie ook Annex 3 ITS en Q&A EIOPA**

- Varianten van netwerk, hardware en software 'as a service' (IaaS, PaaS, SaaS, ASP)
- Contracten waarin het verkrijgen van updates van firmware, besturingssystemen en (standaard) applicaties, die je als gebruiker verplicht moet gebruiken, onderdeel is van de dienstverlening.
- Data(-analyse) diensten waarbij data via ICT-systemen van derden 'als dienst' continu opgevraagd/ aangeleverd/geüpdatet/geschoond/aangevuld/gefilterd etc. wordt om vervolgens bv als input in de administratie opgenomen te worden, en/of gebruikt wordt als basis voor het nemen van beslissingen.
- Overeenkomsten met online platforms waarbij via de portal/website van de derde partij bewerkingen worden uitgevoerd en/of gegevens in de ICT-systemen van de instelling gemuteerd kunnen worden.
- Business Proces Outsourcing met ICT dienstverlening, ICT dienstverlening via een niet ICT TPP (MSP)

(Mogelijke) voorbeelden géén DORA: **zie ook Q&A EIOPA**

- Software licenties vallen in principe onder DORA. De uitzondering hierop is een licentieovereenkomst die uitsluitend voorziet in een eenmalige levering van software zonder bijkomende diensten, waarbij geen sprake is van een onderhoudsovereenkomst met de leverancier. Eenmalige koop kan alleen wanneer de instelling zelfstandig het onderhoud en support uitvoert (zoals gebreken verhelpen of beveiligingslekken dichten).
- Business Proces Outsourcing zonder ICT dienstverlening.
- Q&A ligt voor bij EC: Onder Toezicht Staande instelling is geen ICT dienstverlener als het gaat om een vergunde dienst. Valt wel onder Wft, S2, PW, Eiopa (ESMA, EBA). Wel opnemen in informatieregister (geen onderuitbestedingen) en monitoring uitvoeren.
- Q&A mbt contracten voor de inhuur van mensen waarbij alleen diensten worden verricht op de systemen van de instelling onder leiding en toezicht van de instelling. Geen ICT component in uitbesteding -> S2/EIOPA. Hoe verhoud dit zich tot Annex 3 van ITS: typeert ICT projectmanagement, ICT development en ICT consulting als ICT dienstverlening

Kritieke of Belangrijke functie (KBF) Critical Important Function (CIF)

Een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit; of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten. Voorbeelden (niet limitatief): als proces langer uitvalt dan de vastgestelde maximale uitvalstijd of als in het kritieke proces / ICT systeem wordt ingebroken, sprake is van manipulatie of als fouten ontstaan met wezenlijke impact

Toezicht op uitbestedingsrisico's: hoe doen we het nu?

- Uitvragen Kritieke uitbestedingsketens
- **SBA-NFR**; vragen over uitbestedingsrisico in ORM deel

- **Deep Dive uitbestedingsrisico; onderzoeksvragen**
  - Uitbestedingsbeleid borgt dat kan worden voldaan aan wettelijke eisen -> procedures en modelcontracten
  - Kritieke uitbestedingen in beeld (uitbestedingsregister) & conform beleid; analyse van de risico's / contracten / beveiligingsstandaarden / Business Continuiteit & Backup
  - Monitoring, evaluatie & bijsturing uitbestedingen
  - Informatievoorziening richting DNB, PF's cq RvB/RvC (& Intragroep)

- **Uitbestedingscontrols GPIB**
  - 14.1 Third party and supplier service management
  - 14.2 Third party and supplier risk management
  - 16.3 Internal control at third parties

Basis voor onze onderzoeken en uitvragen

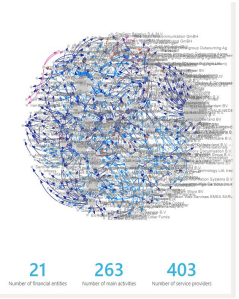
- Solvency II art.49 en 274 & EIOPA richtsnoeren
- PW artikel 34 en WvB artikel 43 & besluit uitvoering PW en WvB
- GPIB

DeNederlandscheBank
EUROSYSTEEM

Let op!
Risicogebaseerd, uitbesteding en het three lines model

Toezicht ICT risico’s TPP's onder DORA en non ICT uitbestedingsrisico's

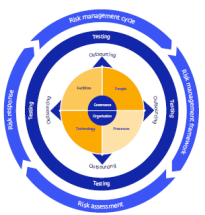
- **Uitvragen Kritieke uitbestedingsketens ->** aansluiten bij ITS - ESA informatieregister uitvragen -> Indien tooling beschikbaar start DNB met het omzetten en inlezen van de data in het PowerBI dashboard, zodat concentraties op FE en NL niveau inzichtelijk worden.



- **SBA-NFR ->** vragen over uitbestedingsrisico in ORM deel aansluiten bij Dora wet en regelgeving art. 28-30 en RTS's

- **Deep Dive en RIG's uitbestedingsrisico ->** hoofddoelstellingen en onderliggende subdoelstellingen aansluiten bij Dora wet en regelgeving

- **Uitbestedingscontrols GPIB en Guidance Uitbesteding ->** alleen nog van toepassing bij niet Dora plichtige verzekeraars in aanvulling op Wft.



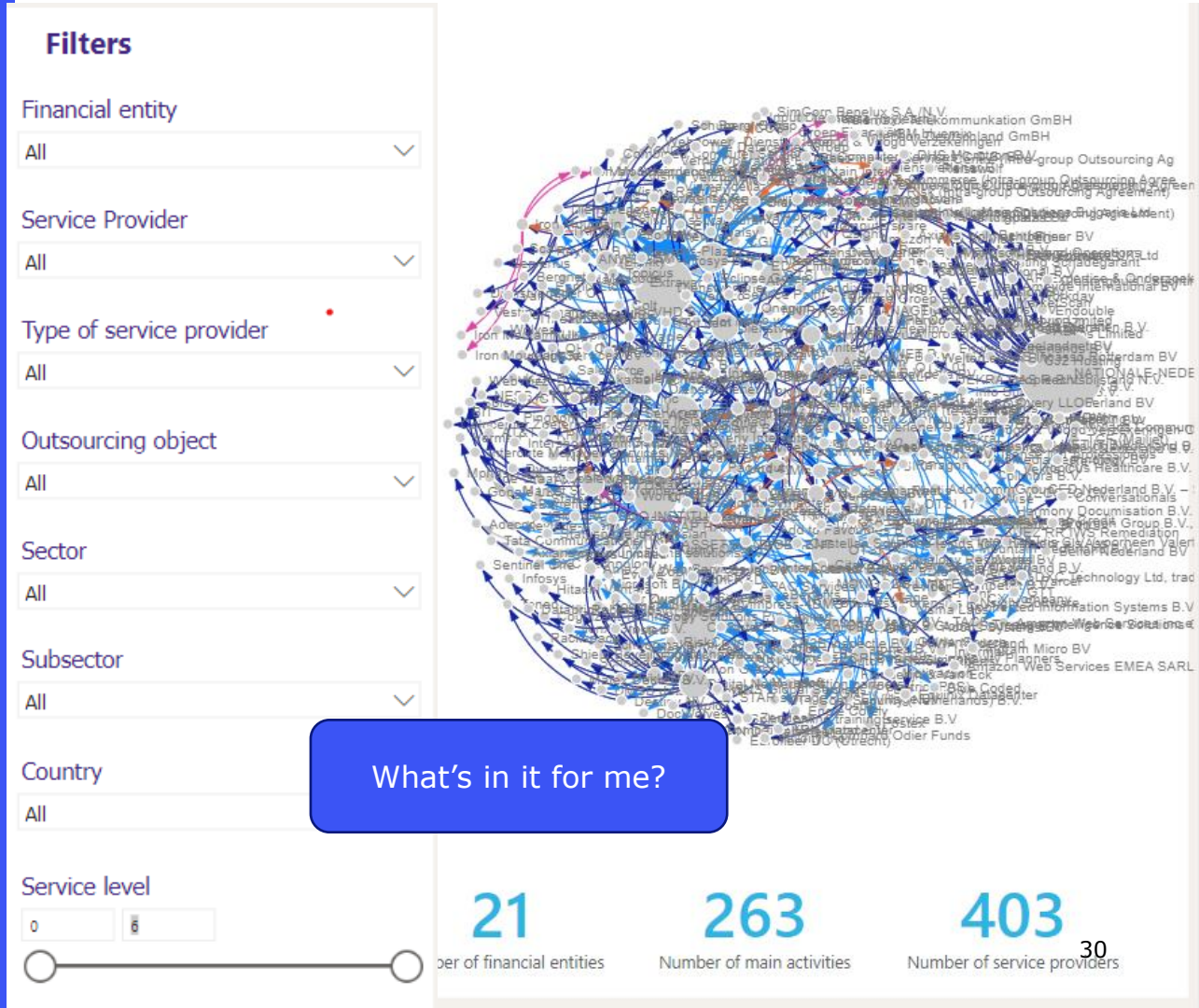
DeNederlandscheBank
EUROSYSTEEM

Dashboard

Inzicht in de instellingen die worden geraakt in geval van problemen bij een KOB dienstverlener

Marktonderzoekpartij met onderuitbesteding bij hostingpartij; niet kritiek geclassificeerd, dus niet in overzicht.

Zou deze hostingpartij onder DORA wel als kritieke onderaannemer worden meegenomen in register?



DeNederlandscheBank
EUROSYSTEEM

Addcom datalek

Wie heeft print en email dienstverlening als kritiek geclassificeerd?
Support aan kritieke functie?

[Steeds meer bedrijven melden datalek bij klantcommunicatiebureau AddComm (nos.nl)]

NOS Nieuws • Woensdag 29 mei, 19:42 • Aangepast woensdag 29 mei, 20:33

Steeds meer bedrijven melden datalek bij klantcommunicatiebureau AddComm

Het lek bij AddComm, een bedrijf dat voor bedrijven, instellingen en overheden brieven en mails naar klanten stuurt, wordt steeds zorgwekkender. Een week geleden meldde AddComm dat cybercriminelen in de systemen met klantgegevens waren gekomen.

Begin deze week informeerden we u dat AddComm, een van de partijen die betrokken is bij het innen van de pensioenpremies, is geraakt door een cyberaanval met gijzelsoftware. Inmiddels is duidelijk dat dit gaat om bedrijfsgegevens van twee bedrijven die bij PME zijn aangesloten.

[Belangrijke informatie over cyberaanval en gelekte bedrijfsgegevens | PME pensioenfonds]

Contractafspraken toereikend?
Support bij incidenten?
Deleten data?

DeNederlandscheBank
EUROSYSTEEM

Bericht inzake beveiligingsincident AddComm

Update september 2024 - AddComm heeft ons geïnformeerd dat de Autoriteit Persoonsgegevens (AP) haar onderzoek heeft afgerond. De AP heeft geconcludeerd dat eerdere bevindingen van AddComm en haar externe experts onvoldoende zekerheid bieden over de gevolgen van het beveiligingsincident. Wij hebben onze klanten hierover inmiddels geïnformeerd.

De AP is na onderzoek bij AddComm van oordeel dat niet met voldoende zekerheid kan worden vastgesteld dat data van de klanten van AddComm niet is weggenomen. Uit het onderzoek van de AP blijkt ook niet dat data van klanten (individuele zorgconsumenten) van Infomedics wel is weggenomen, maar enkel dat het risico niet kan worden uitgesloten. In die gevallen is het standpunt van de AP dat de betrokken zorgconsumenten moeten worden geïnformeerd.

The Register of Information

DeNederlandscheBank

EUROSYSTEEM

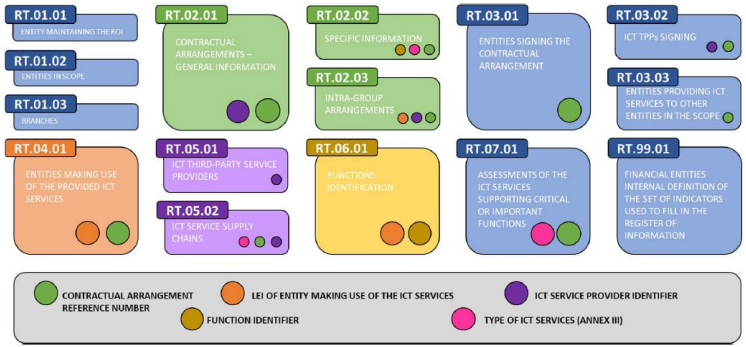
Informatieregister m.b.t. ICT-contracten

De drie doelstellingen van het informatieregister

- Ondersteuning bij het beheer en de monitoring van ICT third-party risico's
- Ondersteuning van het toezicht op ICT third-party risico's door DNB
- Ondersteuning van het Oversight Framework

Concentratierisico's door de keten

- Belang van subcontractors die kritieke of belangrijke functies ondersteunen



DeNederlandscheBank
EUROSYSTEEM

Informatieregister en rapportages van ICT-diensten

- **Jaarlijkse rapportage** van de volledige informatieregisters
- **Plain CSV**: xBRL-CSV met een tabelgeoriënteerde lay-out voor de data
- Eerste aanlevering verwacht **Q2 2025**, daarna jaarlijks eind maart.
- De jaarlijkse DORA-rapportage rondom het aantal nieuwe overeenkomsten, de categorieën van derde aanbieders, het soort contractuele overeenkomsten, en de ICT-diensten en -functies die worden geleverd wordt daarmee overbodig
- De tijdige in kennisstelling van *voorgenomen* uitbestedingen inzake ICT-diensten die **kritieke of belangrijke functies** ondersteunen naar verwachting conform bestaande opzet.

DeNederlandscheBank
EUROSYSTEEM

Informatie dry run exercitie ESA's

Oversight CTPP's

DeNederlandscheBank

EUROSYSTEEM

Oversight op Kritieke Derde aanbieders (CTPPs)

De grootste derde aanbieders van ICT diensten

- Beheersing van potentiële systeemrisico's door toegenomen uitbesteding en concentratie bij verschillende grote aanbieders
- Onderstaande tabel is *non exhaustive* in step 1 en 2

Criterium	Step 1: minimum relevance	Step 2: assessment
Systemic impact on the stability, continuity, or quality of the provision of financial services when large-scale operational failure	Provides services to >10% of the market	Impact of failure on financial entities
Systemic character or importance of the financial entities that rely on the ICT third-party service provider	Number of G-SIIs ≥1 Number of O-SIIs ≥3 Number of other systemic ≥3	Interdependence between G-SIIs or O-SIIs and other financial entities
Reliance w.r.t. critical or important functions of financial entities	Included in other step 1 indicators	Criticality of overall ICT services
Degree of substitutability	No alternative available to >10% of the market	Criticality per type of ICT service

Oversight op Kritieke Derde aanbieders (CTPPs)

- Direct oversight door de ESAs met bijdrage van nationale toezichthouders
- Niet-bindende aanbevelingen door het oversight team
- DNB stelt betreffende financiële instellingen op de hoogte van geconstateerde risico’s
- Financiële instellingen kunnen hierdoor rekening houden met de geconstateerde risico’s in het Third Party Risk Management

Voor meer informatie

www.dnb.nl/dora

DeNederlandscheBank

EUROSYSTEEM