Aandachtsgebieden IT-risicobeheersing per 17 januari 2025

Verzekeringsmiddag 12 november 2024

Marcel Verhoeven en Ingrid Talsma

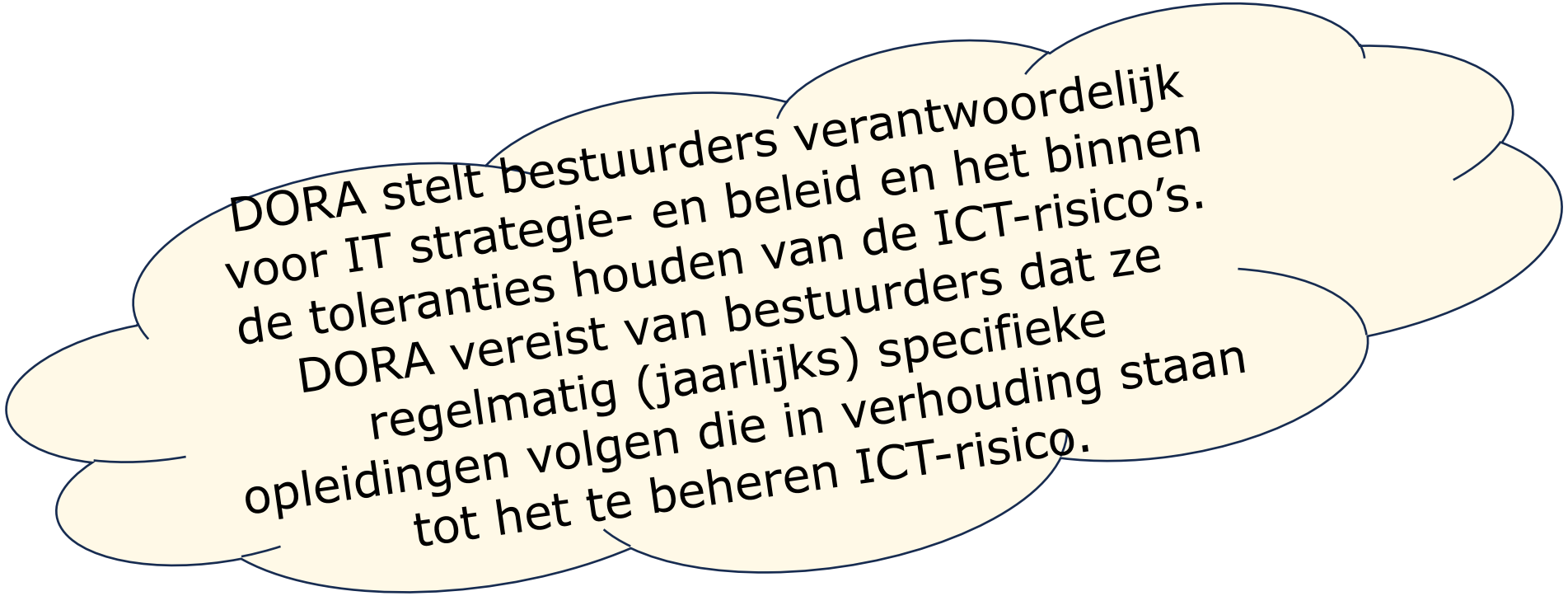
DeNederlandscheBank

EUROSYSTEEM

Aandachtsgebieden DORA

- DORA vervangt de DNB Good Practice Informatiebeveiliging
- Formele rol voor bestuur
- Majeure IT-incidenten melden
- Jaarlijks informatieregister IT uitbestedingen delen
- DORA bepalingen in contracten

Bestuurlijke verantwoordelijkheid vraagt actuele kennis ICT



Governance & Organisation art. 5.4 DORA
De leden van het leidinggevend orgaan van de financiële entiteit onderhouden actief voldoende kennis en vaardigheden om ICT-risico en de gevolgen daarvan voor de verrichtingen van de financiële entiteit te begrijpen en te beoordelen.

Learning & Evolving art.13
Awareness programma's
Trainingen geschikt voor alle medewerkers en senior management

Relatie met de Good Practice informatiebeveiliging

DeNederlandscheBank

EUROSYSTEEM

DNB Good Practice informatiebeveiliging & DORA

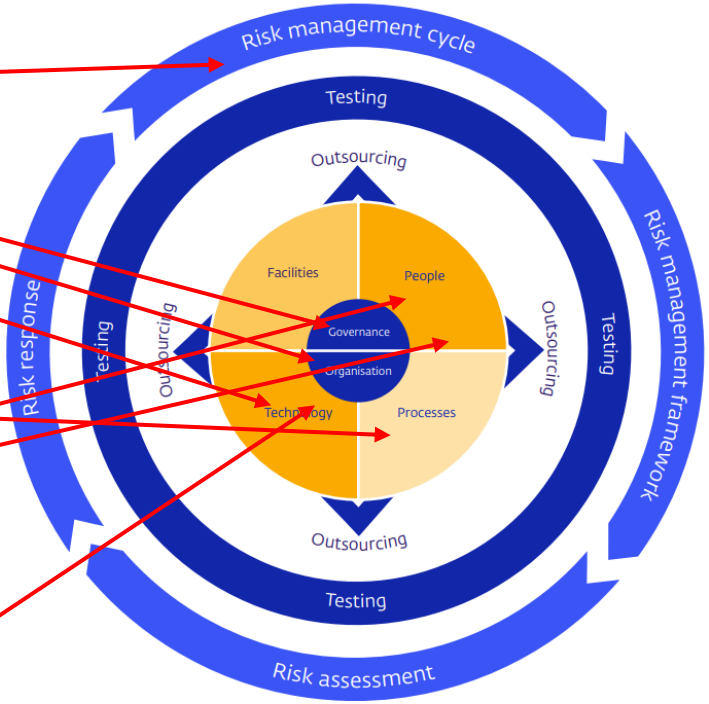
- Voor de sector-brede analyse informatiebeveiliging (SBA-IB) hanteert DNB nog eenmalig de huidige questionnaire en systematiek gebaseerd op de DNB Good Practice informatiebeveiliging.

- DNB zal DORA als wettelijk kader hanteren bij toekomstige uitvragen en onderzoeken.

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

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

DeNederlandscheBank
EUROSYSTEEM

Rapportage van ernstige ICT-gerelateerde incidenten

DeNederlandscheBank

EUROSYSTEEM

Melding van ernstige ICT-gerelateerde incidenten

- Methode: in het eerste half jaar 2025 upload Excel in Mijn DNB, besluit definitieve oplossing onderhanden.
- Ad hoc meldingen wanneer classificatie van het incident uitkomt op ‘major’:
  - **Initiële melding** binnen 4 uur na 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).

Digital operational resilience testing

DeNederlandscheBank

EUROSYSTEEM

Testen van de digitale operationele weerbaarheid

1. **Artikel 24/25**: vaststellen, handhaven en evalueren van een degelijk en alomvattend programma voor het testen van de digitale operationele weerbaarheid

2. **Artikel 26/27**: dreigingsgestuurde penetratietest o.b.v. TLPT

Alle DORA-normadressanten

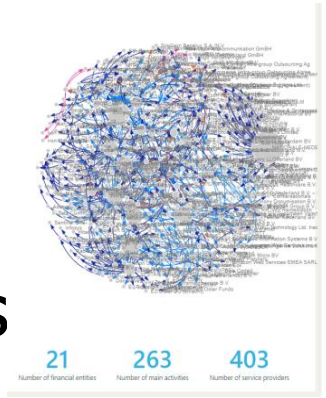
Geselecteerde groep

Uitbesteding en ICT diensten

DeNederlandscheBank

EUROSYSTEEM

Toezicht uitbestedingsrisico’s na 17 januari 2025



- Uitvragen van alle **ICT diensten** via EIOPA template incl subcontractors die kritieke of belangrijke functies ondersteunen: concentraties door de keten

- **SBA-NFR**

- **Onderzoeken naar uitbestedingsrisico**

- **Good Practice & Guidance Uitbesteding:** nog van toepassing bij niet Dora plichtige verzekeraars

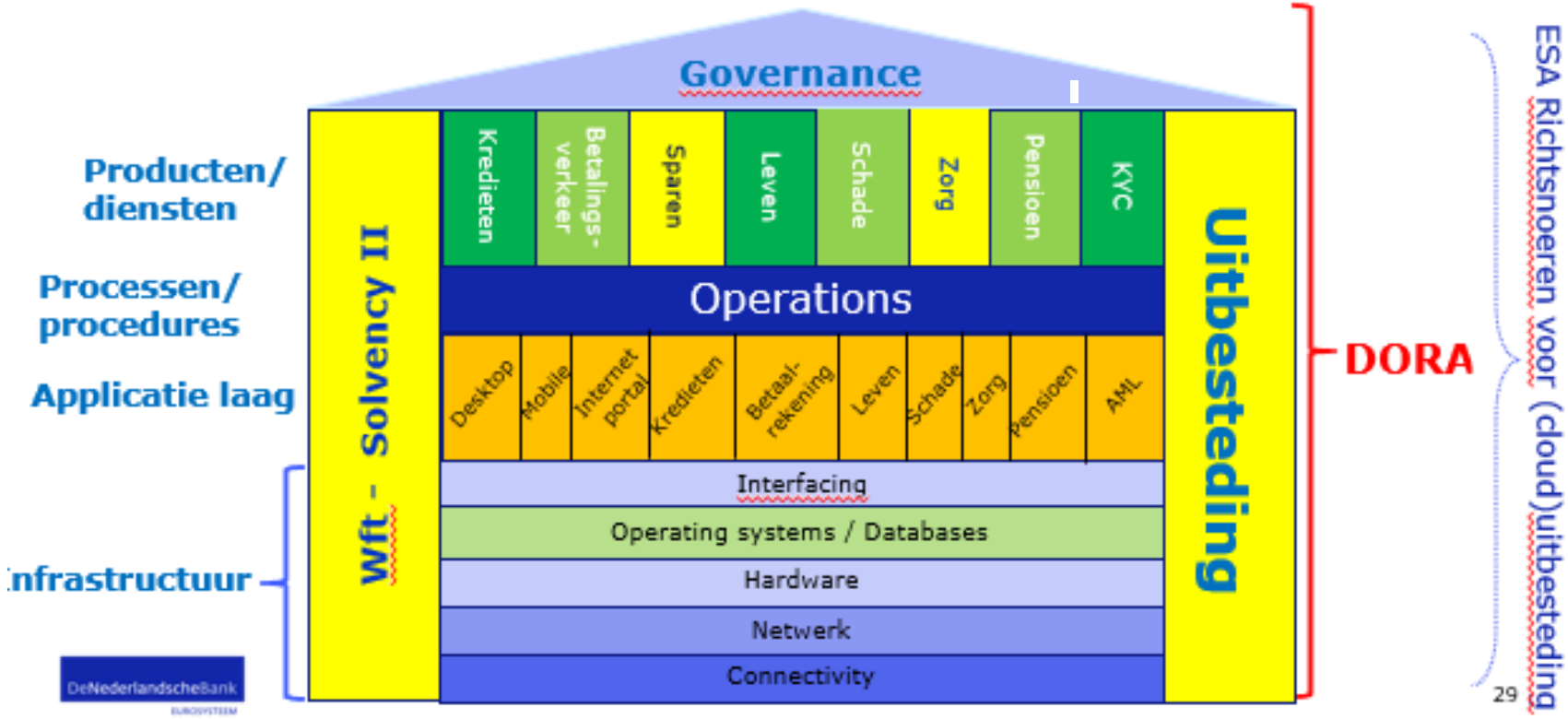
DeNederlandscheBank
EUROSYSTEEM

Hoe bent u betrokken bij uitvragen en onderzoeken?

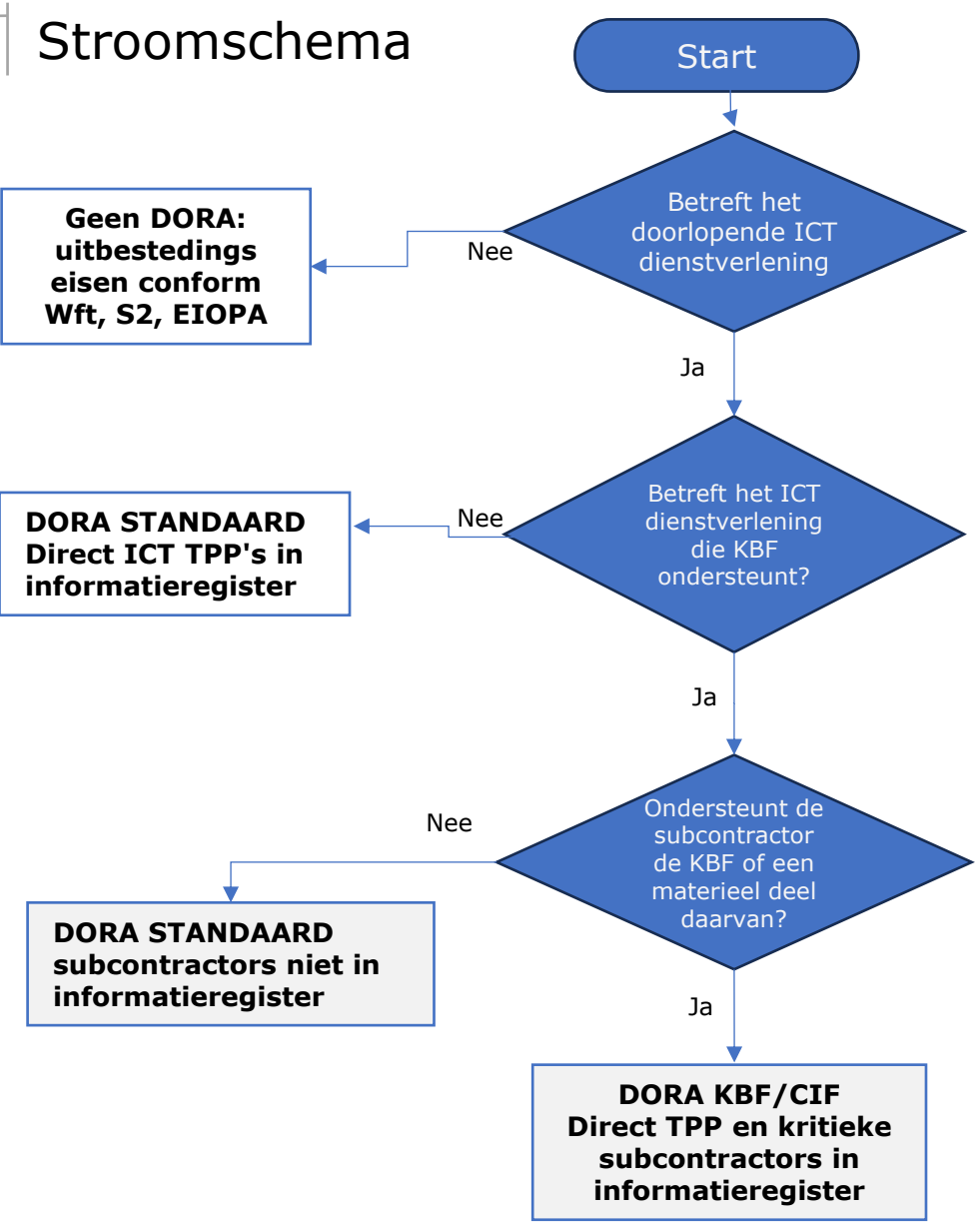
Uitbesteding en ICT diensten na 17 januari 2025

Geen DORA? Wel beheerste uitbesteding!

Aanvullend op DORA



Stroomschema



DeNederlandscheBank
EUROSYSTEEM

Wanneer in scope van DORA?

ICT dienstverlening
Digitale en gegevensdiensten die doorlopend (niet eenmalig) via ICT-systemen aan een of meer interne of externe gebruikers worden verleend

Ondersteunend aan Kritieke of Belangrijke Functie (KBF)
Aanvullende vereisten voor contracten en informatieregister

The Register of Information

DeNederlandscheBank

EUROSYSTEEM

Informatieregister en rapportages van ICT-diensten

- **Jaarlijkse rapportage** van de volledige informatieregisters.
- Eerste aanlevering verwacht **Q2 2025**, daarna jaarlijks eind maart.
- **Methode**: xBRL-CSV met een tabelgeoriënteerde lay-out voor de data
- 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)

- Direct oversight door de ESA's met bijdrage van nationale toezichthouders
- Selectiecriteria als marktaandeel, impact, vervangbaar
- Niet-bindende aanbevelingen door het oversight team
- U blijft verantwoordelijk!

Voor meer informatie

www.dnb.nl/dora

DeNederlandscheBank

EUROSYSTEEM

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.

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

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

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

Eindverantwoordelijkheid voor alle aandachtsgebieden

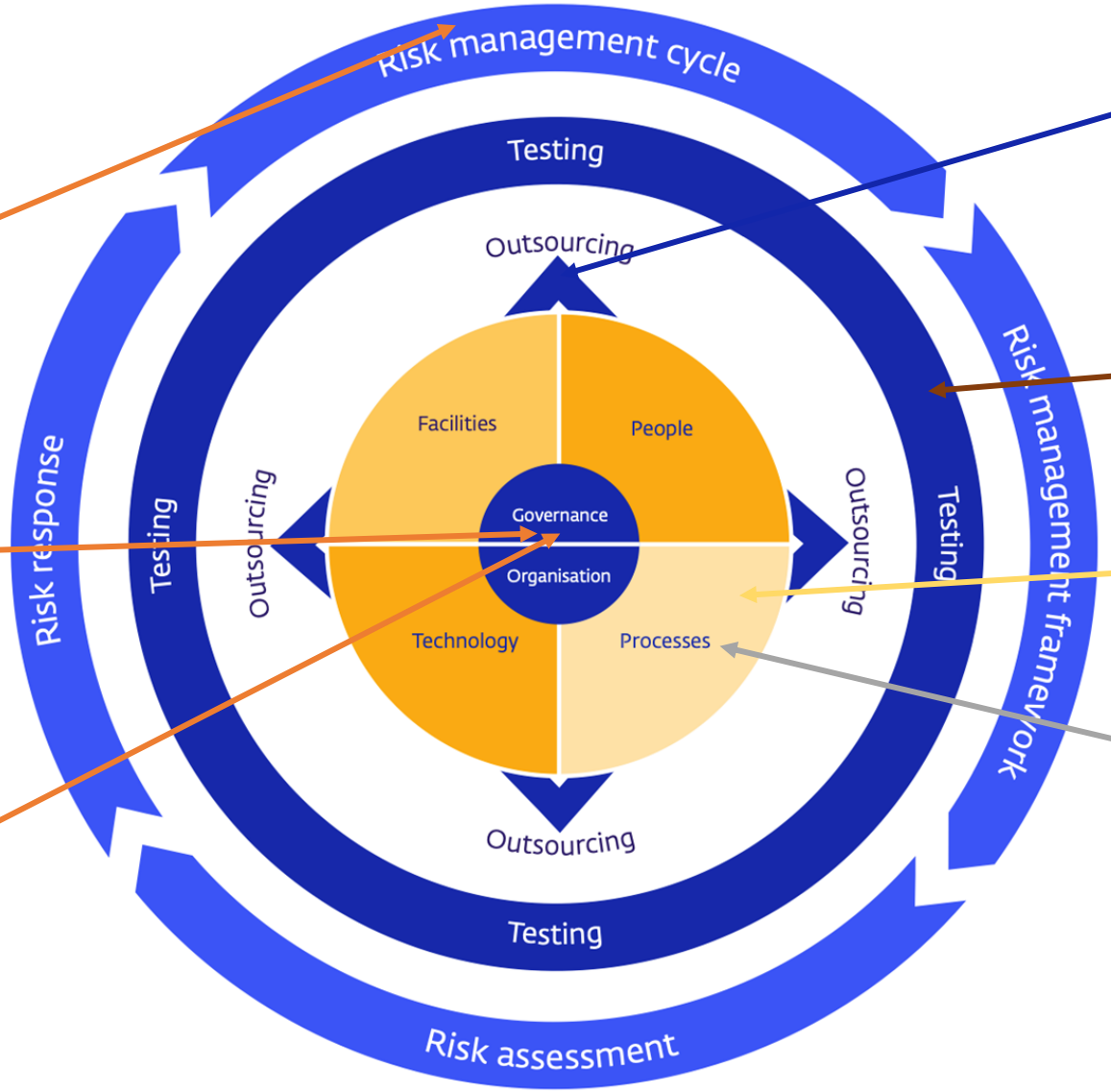
Digitale operationele weerbaarheid strategy raakt alle aandachtsgebieden GPIB & DORA

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

art 2(d)

Governance & Organisation
5.2. responsibilty management body

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



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

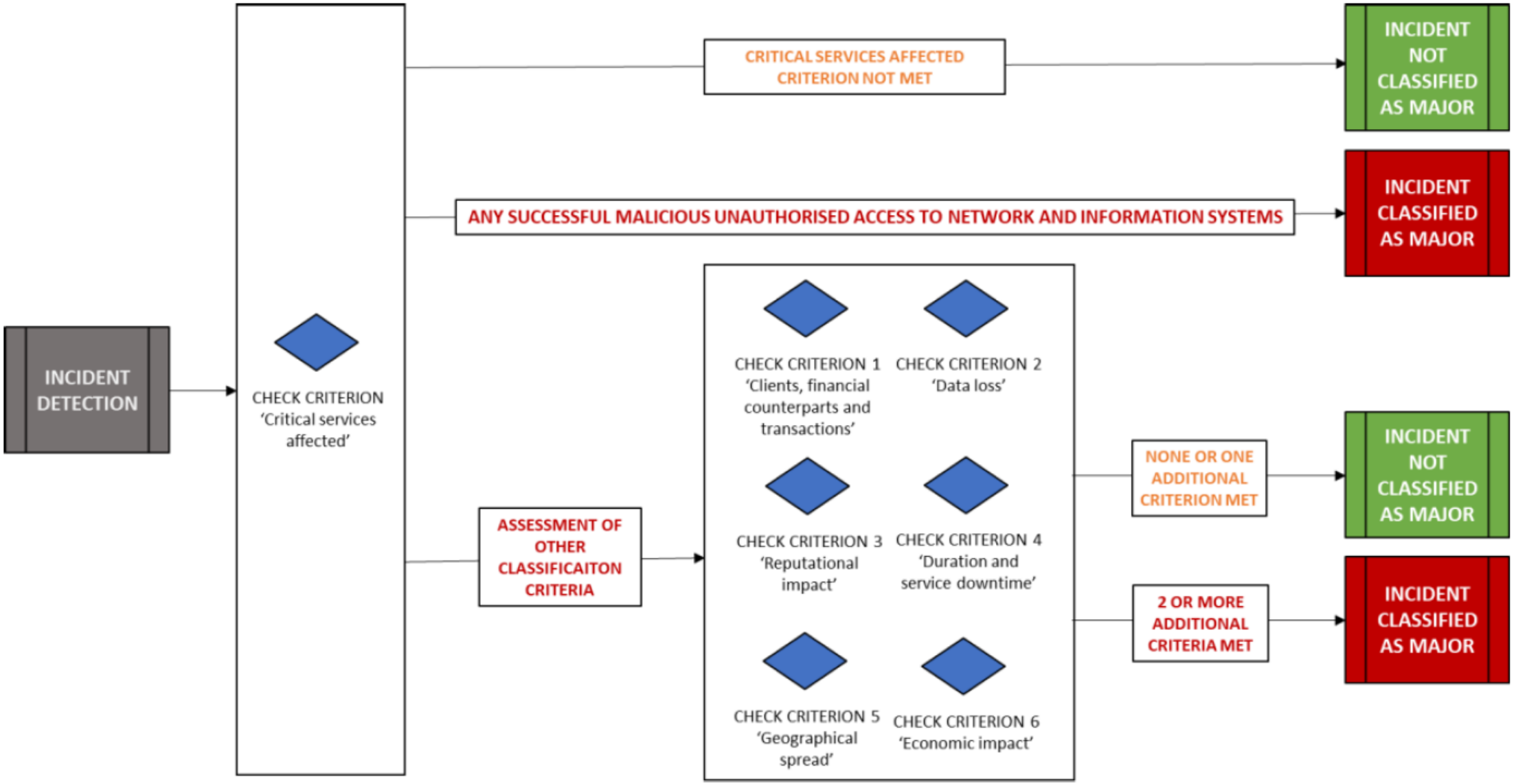
Incident management art. 17-23
6.8(f) Evidencing current Digital operational strategy on base of number major incidents

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

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

DeNederlandscheBank
EUROSYSTEEM

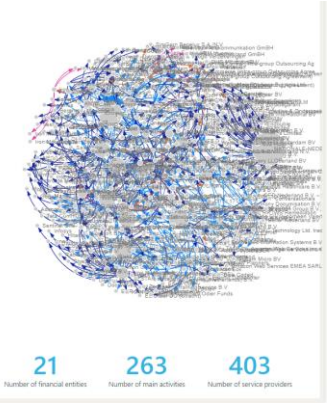
Classificatie van ICT-gerelateerde incidenten



Informatieregister m.b.t. ICT-contracten

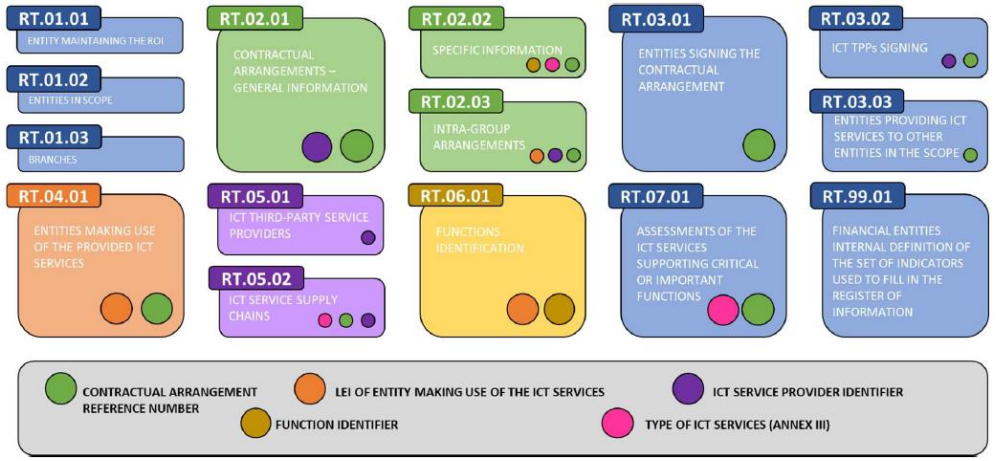
De drie doelstellingen van het informatieregister

- 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



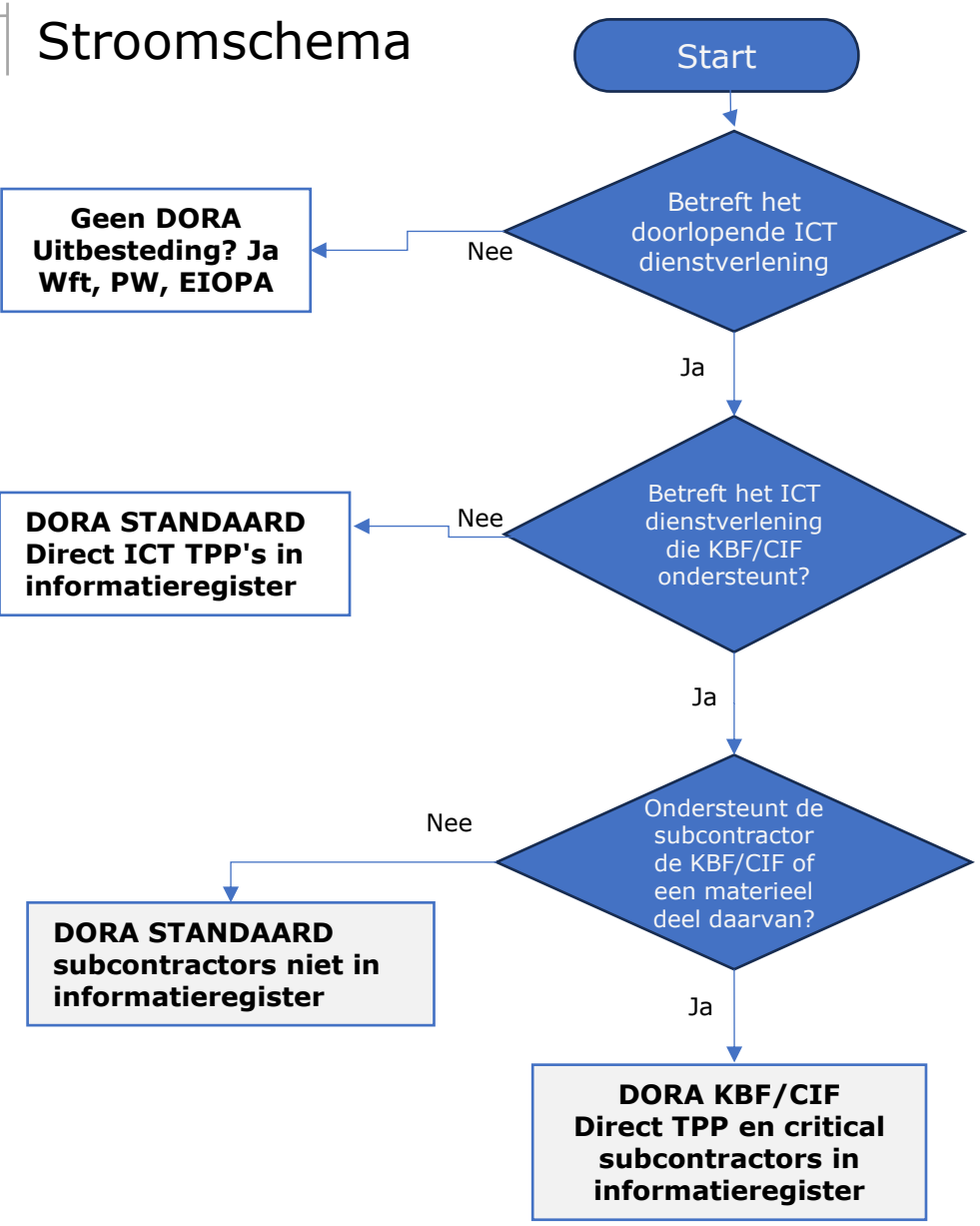
Concentratierisico's door de keten

- Belang van subcontractors die kritieke of belangrijke functies ondersteunen



DeNederlandscheBank
EUROSYSTEEM

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

Uitkomsten DNB onderzoeken en uitvragen 2024

- Risicomanagement rondom informatiebeveiliging en uitbesteding behoeft verbetering -> Belangrijke pijler in DORA!
- Nog te vaak maken instellingen gebruik van kritieke systemen die niet meer worden voorzien van beveiligingsupdates
- Uitbestedingscontracten nog onvoldoende compliant
- Beschikbaarheid immutable back-ups (alleen lezen) en de organisatie en plannen om bij langdurige uitval van IT de bedrijfsvoering te kunnen herstarten volgens SLA’s & contracten
- Meer aandacht nodig voor kennis/awareness programma’s

Wanneer ICT contractenbeleid van toepassing?

"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"

- Contracten met aanbieders van ICT-diensten die kritieke of belangrijke functies (KBF's) ondersteunen
- Als onderdeel van ICT-risicostrategie en beleid bij uitbesteding
- Niet alleen 'externe' IT-leveranciers, maar ook in geval van intragroep uitbesteding
- Ook onderaannemers die KBF's ondersteunen verderop in de keten
- Volgt de lifecycle uit DNB Good Practices; niet nieuw
- Evaluatie beleid (minimaal 1x per jaar)

RTS onderuitbesteding: wanneer van toepassing?

"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 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
- U blijft volledig verantwoordelijk voor het managen van de risico's, ook in geval van serviceproviders onder oversight