De impact van DORA op toezicht

- DORA brengt harmonisering van regels ten aanzien van digitale weerbaarheid, schept (waar nodig) een basiskader dat direct regulerend is en richt zich op beheersing van uitbestedingsrisico's.
  - DORA voorziet in het proportionaliteitsbeginsel.
  - DNB zal DORA opnemen in haar huidige Good Practices.

- Het uitgangspunt is dat de vergunningverlenende toezichthouder ook DORA-toezicht zal uitvoeren.

- De impact van DORA kan vooral voor ketenpartners aanzienlijk zijn.
  - DNB vraagt instellingen en hun uitvoeringsorganisaties de ontwikkelingen rondom DORA adequaat te vertalen naar impact op haar eigen organisatie en die van haar uitbestedingspartners en zich tijdig op DORA voor te bereiden.

Wat gaat er “veranderen”?

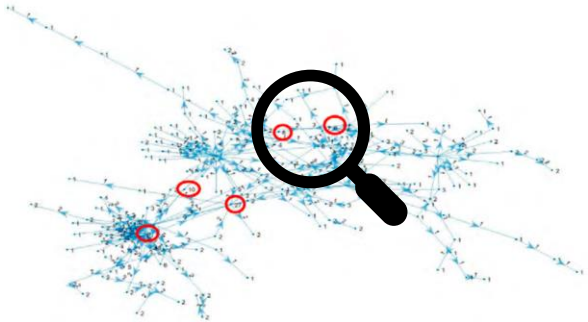
- Van “beheerste en integere bedrijfsvoering” naar wettelijke normeringen.
  - DORA bevat stringentere normen dan de huidige Guidelines en Good Practices.
  - Noodzaak tot (geavanceerde, dreiging gestuurde) testen (waarbij TIBER als raamwerk wordt onderschreven).

- Inzicht in de gehele uitbestedingsketen (en de beheersing daarover) wordt nog belangrijker en is een verplichting.

- Formalisatie van de Meldplicht ICT-incidenten bij de toezichthouder(s)

DeNederlandscheBank
EUROSYSTEEM

Oversight op kritieke dienstverleners/CTPPs



- Oversight op kritieke dienstverleners/CTPPs komt bij de ESAs te liggen (waaronder EIOPA).
  - EIOPA kan hierdoor rechtstreeks onderzoek doen bij CTPPs.
  - CTPPs krijgen daarnaast ook te maken met de Network and Information Security (NIS) directive.
  - Instellingen kunnen vragenlijsten en aanvullende verzoeken vanuit de ESA verwachten om het ‘kritieke derde partijen landschap’ in kaart te brengen (veelal via de NCA uitgezet).