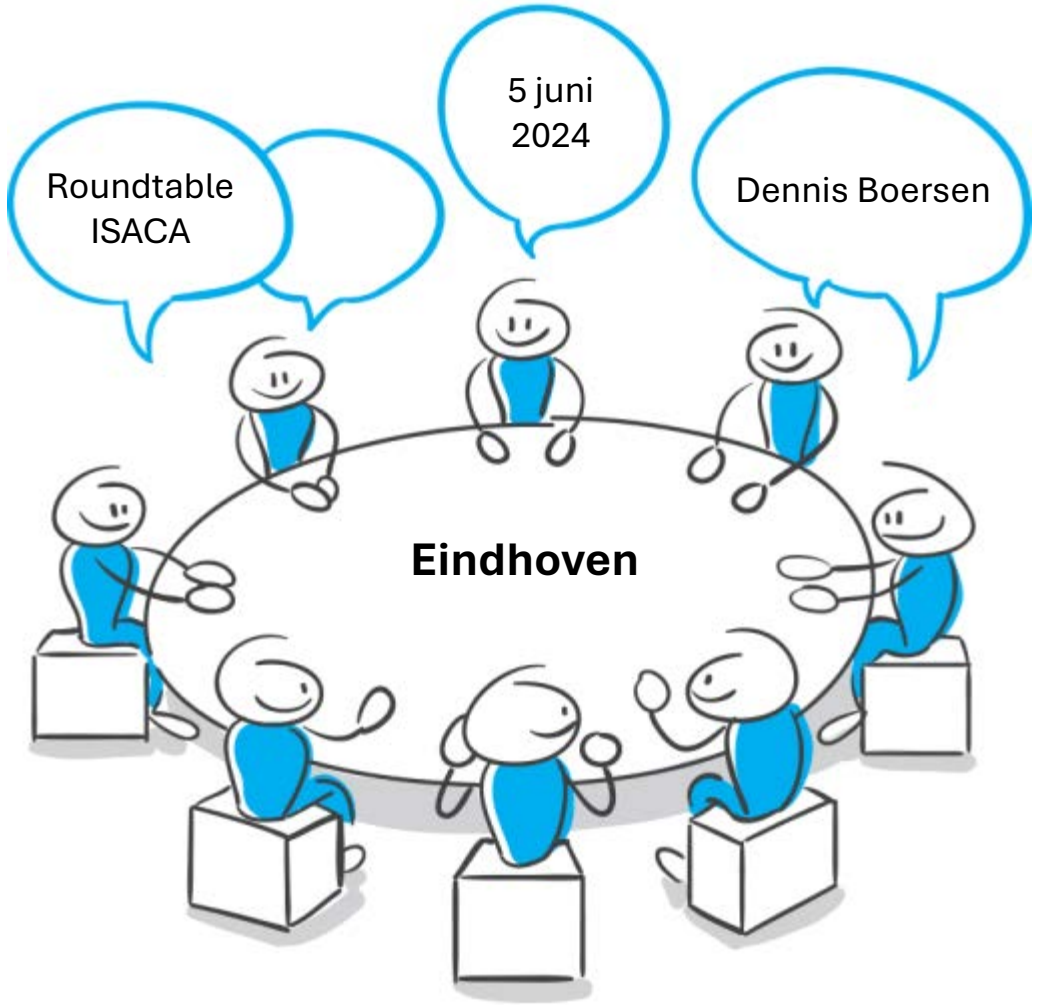
DORA, Swiper no swiping

ISACA

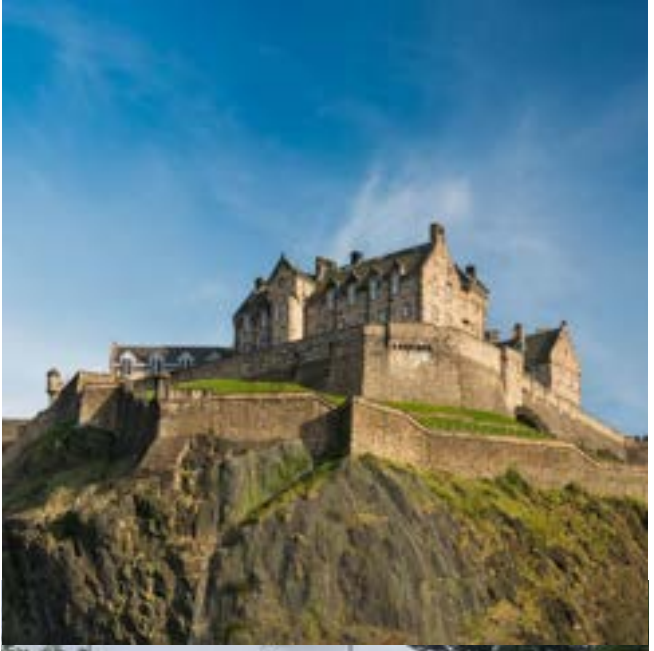
argis consultants

DORA, hacker niet stelen

1. Digital Operational Resilience Act (DORA)
2. Vereisten op 5 pijlers
    a. Pijler 1: ICT-risicobeheer
    b. Pijler 2: Rapportage van ICT-incidenten
    c. Pijler 3: Digitale operationele veerkrachttesten
    d. Pijler 4: ICT-risicobeheer van derden
    e. Pijler 5: Informatie en inlichtingen delen.
3. DORA vs. DNB GP Informatiebeveiliging
4. Manieren van toezicht op ICT-derden
5. DORA samengevat in kernpunten
6. Te zetten stappen, what's next
7. Discussie



Dennis Boersen RE



MORET ERNST & YOUNG

achmea

argis
consultants

1. Digital Operational Resilience Act

De digitale dreiging voor Nederland is onverminderd groot.

Bijzondere kenmerken van digitale risico's vragen een bredere manier van beheersing dan andere risico's. Zo maken digitale risico's onderdeel uit van een breder, dynamisch én complex risicopalet en is de digitale ruimte een uiterst complex systeem dat zich lastig laat doorgronden.

1. Digital Operational Resilience Act

Een **verordening van de Europese Commissie** (EC) om de digitale weerbaarheid te vergroten in de **financiële sector.**

(Verordening (EU) 2022/2554)

- Bescherming van netwerken en informatiesystemen (toenemende afhankelijkheid van complexe digitale infrastructuren en technologieën);
- Weerbaarheid tegen cyberdreigingen financiële sector (toenemende kwetsbaarheid van de financiële dienstverlening);
- Consumentenbescherming en financiële stabiliteit.

Hoofddoelen & Vereisten

Met DORA heeft de Europese Commissie drie hoofddoelen voor ogen:

1. De versnipperde regels t.a.v. digitale weerbaarheid in de EU harmoniseren, één uniform wetgevend kader.
2. Een basiskader scheppen voor financiële organisaties waarvoor nog geen regelgeving is.
3. Het beter mitigeren van risico's van uitbesteding door de financiële sector aan kritieke digitale derde dienstverleners.

Concreet vereist DORA dat financiële organisaties:

1. ICT-risicomanagement implementeren, inclusief het beheer van ICT-incidenten;
2. Periodiek de digitale weerbaarheid testen;
3. Risico's beheersen bij het uitbesteden aan derden, rekening houdend met factoren zoals grootte, risicoprofiel en systeembelang (evenredigheidsbeginsel).

Is dit nieuw?

STELLING 1

NIS2, BIO, DNB GP, DORA kan DNB ook DORA adopteren ?

Met andere worden zijn we niet murw van alles waar we aan moeten voldoen……..

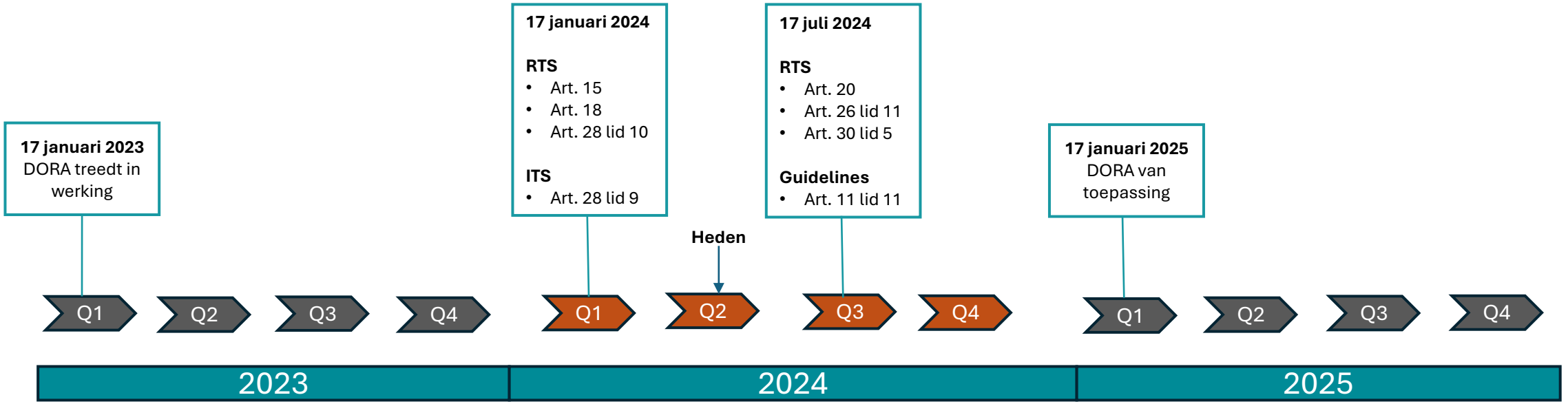
Op wie van toepassing

- Kredietinstellingen
- Betalingsinstellingen
- Aanbieders van rekeninginformatiediensten
- Instellingen voor elektronisch geld
- Beleggingsondernemingen
- Aanbieders van cryptoactiviteiten net vergunning
- Centrale effecten bewaarinstellingen
- Centrale tegenpartijen
- Handelsplatformen
- Transactieregisters
- Beheerders van alternatieve beleggingsinstellingen

- Beheermaatschappijen
- Aanbieders van datarapporteringsdiensten
- Verzekerings- en herverzekeringsondernemingen
- Verzekeringstussenpersonen, herverzekeringspersonen en neven verzekeringtussenpersonen
- Instellingen voor bedrijfspensioenvoorziening
- Ratingbureaus
- Beheerders van kritieke benchmarks
- Aanbieders van crowdfundingdiensten
- Securisatieregister
- Derde aanbieders van ICT-diensten

Al deze partijen krijgen met DORA te maken. De mate waarin DORA op hun van toepassing is, is afhankelijk van de omvang. Ook daarvan zijn criteria gedefinieerd.

Tijdslijnen



Regulatory Technical Standards, 1e pakket (batch) 17 januari 2024

- RTS on ICT risk management framework and on simplified ICT risk management framework;
- RTS classification of ICT-related incidents;
- RTS on ICT third-party service providers (TPPs);
- ITS register of information.

Regulatory Technical Standards, 2e pakket (batch) 17 juli 2024

- RTS and ITS on content, timelines and templates on incident reporting;
- GL on aggregated costs and losses from major incidents;
- RTS on subcontracting of critical or important functions;
- RTS on threat-led penetration testing (TLPT).

Regelgeving

Regelgeving van DORA bestaat uit:

- De verordening zelf (level 1);
- 2 pakketten (batches) van Regulatory Technical Standards en Implementing Technical Standard (level 2), dit is een gedetailleerde invulling van vereisten t.b.v. level 1.

Regulatory Technical Standards

Een Regulatory Technical Standard (RTS) is een gedetailleerde regel die door Europese toezichthouders wordt opgesteld om Europese wetten, zoals DORA, duidelijker en specifieker te maken. RTS'en worden goedgekeurd door de Europese Commissie en zijn verplicht voor iedereen die onder de wet valt. RTS'en helpen organisaties om precies te weten wat ze moeten doen om aan de wet te voldoen en zorgen ervoor dat dit op een uniforme manier in heel Europa gebeurt.

Implementing Technical Standard

Een Implementing Technical Standard (ITS) is een richtlijn opgesteld door Europese toezichthouders om de praktische uitvoering van Europese wetten te verduidelijken. ITS'en zorgen ervoor dat regels consistent worden toegepast in alle EU-lidstaten en geven gedetailleerde instructies voor de uitvoering en rapportage van verplichtingen. ITS'en maken duidelijk wat er praktisch van organisaties wordt verwacht om aan de wet te voldoen.

DORA geeft ook guidelines. Guidelines helpen organisaties door praktische en toepasbare adviezen te geven om aan de wettelijke eisen te voldoen, waarbij ze een beter inzicht geven in wat toezichthouders verwachten.

Regelgeving level 1

De verordening van DORA is opgedeeld in hoofdstukken en kent de volgende hoofdstukkenindeling die van toepassing is op financiële entiteiten die onder DORA vallen:

- Hoofdstuk I (art. 1 – 4): Algemene bepalingen
- Hoofdstuk II (art. 5 – 16): **ICT Risicomanagement**
  - Doel: ervoor zorgen dat financiële ondernemingen adequaat ICT-risicomanagement hebben ingericht.
- Hoofdstuk III (art 17 – 23): **Beheer, classificatie en rapportage van ICT-gerelateerde incidenten**
  - Doel: het borgen van een adequaat proces/ procedure voor het rapporteren, adresseren en beheren van alle ICT-gerelateerde incidenten.
- Hoofdstuk IV (art. 24 – 27): **Testen van digitale operationele weerbaarheid**
  - Doel: financiële ondernemingen worden verantwoordelijk voor het continue testen en beoordelen van de adequaatheid van maatregelen en de veerkracht van ICT-systemen, zodat mogelijke kwetsbaarheden aan het licht komen.
- Hoofdstuk V (art. 28 – 44): **Beheer van ICT-risico van derde aanbieders**
  - Doel: ervoor zorgen dat financiële ondernemingen een gedegen monitoring inrichten van het ICT-risico van derden aanbieders/ ICT-dienstverleners/ cloud server providers.
- Hoofdstuk VI (art. 45): **Regeling voor informatie-uitwisseling**
  - Doel: de verordening maakt het mogelijk dat bedrijven informatie over cyberdreigingen delen.
- Hoofdstuk VII (art. 46 – 56): Bevoegde autoriteiten.
- Hoofdstuk VIII (art. 57): Gedelegeerde handelingen.
- Hoofdstuk VIIII (art. 58 – 64): Overgangs- en slotbepalingen.

Regelgeving level 2

De wet wordt verder ingevuld door middel van technische reguleringsnormen (level 2), beter bekend als Regulatory Technical Standards (RTS) en Implementing Technical Standards (ITS). Deze verdere invulling geeft invulling en details op bepaalde punten van de wet en schrijven het gebruik van bepaalde standaarden en formats voor.

- Enkele ITS en RTS'en zijn gepubliceerd op 17 januari 2024:
  - Art. 15 Verdere harmonisatie van ICT-risicobeheersinstrumenten, -methoden, processen en beleidslijnen (RTS);
  - Art. 16 Specificatie van ICT-risicobeheer elementen voor het vereenvoudigd kader voor ICT-risicobeheer (RTS);
  - Art. 18 Specificatie voor de inrichting van classificatie van ICT-gerelateerde incidenten en cyberdreigingen (RTS);
  - Art. 28 lid 9 (lid 3) Algemene beginselen – informatieregister derde aanbieders (ITS);
  - Art. 28 lid 10 (lid2) Algemene beginselen – beleid contractuele overeenkomsten met derde ICT-dienstverleners (RTS).
- De volgende RTS'en zijn naar verwachting gereed op 17 juli 2024:
  - Art. 20 Harmonisatie van inhoud en modellen van rapportage (RTS);
  - Art. 26 lid 11 Nadere specificatie/ vereisten m.b.t. geavanceerde tests van ICT-instrumenten, - systemen en -processen op basis van TLPT (Threat Led Penetration Testing, testen hoe huidige bedreigingen kritieke bedrijfsfuncties kunnen beïnvloeden) (RTS);
  - Art. 30 lid 5 (lid 2 punt a) Opstellen van technische reguleringsnormen ter bepaling van uitbesteding van ICT-diensten die kritieke of belangrijke functies ondersteunen (RTS)
- Tevens volgt er rond 17 juli nog een guideline op artikel 11, lid 11:
  - "Overeenkomstig artikel 16 van de Verordeningen (EU) nr. 1093/2010, (EU) nr. 1094/2010 en (EU) nr. 1095/2010 Die, via de Gemengd Comité, uiterlijk op 17 juli 2024 gemeenschappelijke richtsnoeren opstellen voor de raming van de in lid 10 bedoelde geaggregeerde jaarlijkse kosten en verliezen."

STELLING 2

DORA is niet meer dan oude wijn in nieuwe zakken

2. Vereisten DORA op 5 pijlers

Information and intelligence sharing	/ Guidelines on information sharing arrangements for cyber threats and vulnerabilities
ICT incident reporting	/ Standardised incident classification / Compulsory and standardised reporting of major incidents / Anonymised EU-wide reports
Digital Operational Resilience testing	/ Comprehensive testing programme, with a focus on technical testing / Large-scale threat-led live tests performed by independent testers every 3 years
ICT third-party risk management	/ Strategy, policy and standardised register of information / Guidelines for pre-contract assessment, contract contents, termination, stressed exit / Setup of an oversight framework for critical providers across the EU with clear requirements and penalties
Information and intelligence sharing	/ Guidelines on information sharing arrangements for cyber threats and vulnerabilities

2.1 Pijler 1 – ICT-risicobeheer

Waarom?
Ervoor zorgen dat er specifieke maatregelen en controles zijn om de verstoring van de markt en de consumenten door incidenten te beperken, en ervoor zorgen dat het beheersorgaan verantwoording aflegt over het ICT-risicobeheer.

Belangrijkste vereisten:

- Governancebeginselen inzake ICT-risico's volgen, met nadruk op de verantwoordingsplicht van het bestuursorgaan.
- Risicotolerantie voor ICT-risico's bepalen o.b.v. de risicobereidheid van de organisatie en de impacttolerantie voor ICT-verstoringen.
- Beschikken over een kader voor risicobeheer met een inventarisatie van kritieke en belangrijke functies, de daaraan verbonden risico's en het in kaart brengen van de ICT-middelen die deze functies ondersteunen, alsmede specifieke beschermings-, preventie-, detectie-, reactie- en herstelplannen en -capaciteiten, processen voor continue verbetering en meetmethoden.
- Beschikken over een strategie voor crisiscommunicatie met duidelijke rollen en verantwoordelijkheden.
- Verplichte DORA-opleiding als onderdeel van de continue verbeteringsprocessen over digitale operationele weerbaarheid voor het leidinggevend orgaan, maar ook voor het voltallige personeel, als onderdeel van hun algemene opleidingspakket.

Grootste uitdaging:
Als onderdeel van de continue verbeteringsprocessen introduceert DORA een verplichte opleiding over digitale operationele weerbaarheid voor het leidinggevend orgaan, maar ook voor het voltallige personeel, als onderdeel van hun algemene opleidingspakket.

STELLING 3

met name onze leveranciers gaan moeite hebben met het toezicht regime en zal leiden tot een shake-out

2.1 Pijler 2 – Rapportage van ICT-incidenten

Waarom?
De melding van incidenten moet worden geharmoniseerd en gecentraliseerd, zodat de regelgever snel kan reageren om te voorkomen dat de gevolgen zich verspreiden, en om collectieve verbeteringen en de kennis van bedrijven over actuele bedreigingen voor de markt te bevorderen.

Belangrijkste vereisten:
DORA voert een standaardindelingsmethode voor incidenten met reeks specifieke criteria inrichten en incidentenclassificatiemethode aanpassen aan de eisen (drempels nog niet bekend):

1. Ernstig ingedeelde incidenten moeten binnen dezelfde werkdag aan de regelgever worden gemeld, volgens een bepaald model. Juiste processen en kanalen opzetten om de toezichthouder snel op de hoogte te kunnen brengen van een ernstig incident.
2. Na een week en na een maand moet een follow-uprapport worden ingediend.
3. Al deze rapporten zullen worden geanonimiseerd, gebundeld en regelmatig voor de hele gemeenschap toegankelijk worden gemaakt.

(Verwachte methodologie: ENISA-referentie taxonomie voor incidentclassificatie (European Union Agency for Cybersecurity).)

Grootste uitdaging:
Bedrijven zullen hun incidentenclassificatiemethode moeten aanpassen aan de eisen. Zij zullen ook de juiste processen en kanalen moeten opzetten om de toezichthouder snel op de hoogte te kunnen als zich een ernstig incident voordoet. Op basis van wat als "ernstig" wordt geclassificeerd, kan dit vaak gebeuren. Om organisaties te helpen zich voor te bereiden, verwachten wij dat de methodologie voor incidentclassificatie zal worden afgestemd op de ENISA-referentie taxonomie voor incidentclassificatie.

STELLING 4

Rapporteren over kosten van beveiligingsincidenten dat zie ik nog niet zo snel gebeuren

Digital Operational Resilience testing	/ Comprehensive testing programme, with a focus on technical testing / Large-scale threat-led live tests performed by independent testers every 3 years

2.3 Pijler 3 – Testen van digitale operationele veerkracht

Waarom?
Ervoor zorgen dat financiële entiteiten de efficiëntie testen van het risicobeheerkader en de maatregelen om te reageren op en te herstellen van een breed scala aan scenario's voor ICT-incidenten, met minimale verstoring van kritieke en belangrijke functies, op een manier die evenredig is met hun omvang en critici voor de markt.

Belangrijkste vereisten:

- Een uitgebreid testprogramma opzetten, met inbegrip van een reeks beoordelingen, tests, methodologieën, praktijken en instrumenten, met nadruk op technische tests.

- De meest kritieke ondernemingen: om de drie jaar een grootschalige dreigingsgestuurde live penetratietest organiseren (soort red-team oefening), uitgevoerd door onafhankelijke testers, die betrekking hebben op kritieke functies en diensten en waarbij in de EU gevestigde ICT-derden worden betrokken. Het scenario moet vooraf door de toezichthouder worden goedgekeurd en ondernemingen ontvangen na afloop van de test een conformiteitscertificaat.

Grootste uitdaging:
Waarschijnlijk moeten kritieke bedrijven deze dreigingsgestuurde penetratietest tegen eind 2024 organiseren en dit soort tests vergt veel voorbereiding. Het feit dat er kritieke ICT-derden bij moeten worden betrokken, betekent ook dat zij bij de voorbereiding moeten worden betrokken. Bedrijven die denken dat zij binnen het toepassingsgebied zullen vallen (dit kunnen bedrijven zijn die al onder de regelgeving inzake netwerk- en informatiebeveiliging vallen), moeten zo snel mogelijk beginnen na te denken over het scenario, zodat zij ten minste twee jaar vóór de deadline met de regelgever kunnen valideren.

STELLING 5

We beginnen in Q4 wel, in januari zal DNB nog niet op de stoep staan

2.4 Pijler 4 – ICT-risicobeheer voor derden

Waarom?
Ervoor zorgen dat financiële organisaties een passend niveau van controles en toezicht op hun ICT-derden hebben, met name degenen die kritieke functies ondersteunen; en een specifiek toezicht instellen op providers die kritisch zijn voor de markt als geheel.

Belangrijkste vereisten:
- Beschikken over een welomschreven strategie en beleid inzake de risico's van ICT-derden met meerdere leveranciers, die worden beheerd door een lid van het leidinggevend orgaan.
- Standaardinformatieregister samenstellen met een volledig overzicht van alle externe ICT-leveranciers (niet alleen meest kritische), de diensten die zij verlenen en de functies die zij ondersteunen. Eenmaal per jaar aan de toezichthouder verslag uitbrengen over de wijzigingen in dit register.
- Alvorens een contract af te sluiten, ICT-dienstverleners aan de hand van bepaalde criteria beoordelen.
- Exitstrategie plannen voor het geval een dienstverlener failliet gaat.
- De DORA-richtsnoeren voor de inhoud van contracten en de redenen van contractbeëindiging koppelen aan een risico of bewijs van niet-naleving op het niveau van de dienstverlener.
- Kritieke providers worden jaarlijks getoetst aan de veerkrachtvereisten door de toezichthouder.

Grootste uitdaging:
Het verzamelen van informatie over alle ICT-leveranciers (niet alleen de meest kritische), met de geleverde diensten en functies die zij ondersteunen voor het informatieregister zal een zeer grote taak zijn voor grote financiële organisaties die typisch afhankelijk zijn van duizenden grote en kleine leveranciers en legacy contract management systemen die het moeilijk maken om gegevens uit te mijnen.

STELLING 6

mijn leverancier is ISO27001 gecertificeerd, heeft een PDCA/management cyclus, dat is toch prima

2.5 Pijler 5 – Delen van informatie en inlichtingen

Waarom?
Bevorderen van het delen van informatie en inlichtingen over cyberdreigingen tussen financiële organisaties, zodat zij beter voorbereid zijn.

Belangrijkste vereisten:
Implementeren DORA-richtsnoeren voor het opzetten van regelingen voor het delen van informatie tussen ondernemingen over cyberdreigingen.

Grootste uitdaging:
Wij zien voor veel financiële instellingen geen bijzondere uitdaging op dit gebied, aangezien veel organisaties al over dergelijke afspraken beschikken. Denk bijvoorbeeld aan de P-ISAC, Digitaal Trust Community, NCSC. Het zal een kans zijn om lokale initiatieven, netwerken of verenigingen zichtbaar te maken en meer bedrijven aan te moedigen om er deel van uit te maken.

STELLING 7

Dit doen wij al voor datalekken, toch

3. DORA versus DNB GP Informatiebeveiliging

Synergie tussen DORA en Good Practice Informatiebeveiliging

De DORA wetgeving en DNB's Good Practice Informatiebeveiliging vullen elkaar aan en dragen bij aan een veiliger financieel ecosysteem. DORA bevat basisvereisten waaraan financiële instellingen moeten voldoen, terwijl de Good Practice gedetailleerde richtlijnen geeft om deze vereisten te implementeren. Door de implementatie van Good Practice Informatiebeveiliging 2023 van DNB voldoen financiële instellingen in grote lijnen al aan de eisen van DORA. Belangrijke focus onderwerpen van DNB zijn altijd Cyber en uitbesteding (de keten) geweest.

Ben je als organisatie reeds bekend met de volwassenheidsniveau van DNB Good Practice Informatiebeveiliging dan helpt dat bij de verdere implementatie van DORA. Minder volwassen of nog onbekend met de DNB Good Practice Informatiebeveiliging dan snel aan de slag. DORA kan immers leiden tot boetes.

DNB GP Informatiebeveiliging

- Level 3
- 58 controls binnen 9 gebieden
- Ontstaan vanuit Cobit perspectief
- Jaarlijks (verplicht) self assessment op volwassnheidsniveau

- Level 3
- 58 controls binnen 9 gebieden
- Ge-update en aangevuld met vereisten ten opzichte van de digitale weerbaarheid.
- Van kracht H2 2024

Grote overlap;

- Diverse elementen uit DORA toegevoegd
- Het is meer geworden, ook al blijft het aantal controls (58)
- Controls zijn meer richting risico's geschreven ("voldoende robuust" of "passend binnen risicoprofiel");
- DNB heeft nog niet concreet de plannen voor 2025 gecommuniceerd

Good Practice Informatiebeveiliging 2023 DeNederlandscheBank EUROSYSTEEM	
Nationaal	EU-Regulation
Level 3	Level 1
Rule based	Rule based, maar gaat een stap verder!
58 controls	200+ vereisten
Mitigerende maatregelen	Focus op risico’s
Jaarlijkse verplichte self assessment	???
Geen doorlopende toezichthouders-verplichtingen	Diverse verplichte meldingen + diverse op te vragen documenten

Voorbeeld IT risk management framework

DNB GP IB 2019-2020	DNB GP IB 2023 DORA	DORA
De instelling heeft een proces ingericht dat onder meer het volgende waarborgt: A. De instelling ontwikkelt en onderhoudt een IT risk management framework. B. Het IT-risk management framework sluit aan op het risk management raamwerk van de instelling. C. De instelling adresseert risico's op het gebied van informatiebeveiliging en cybersecurity in het IT-risk management raamwerk. D. De risicotoleranties ten aanzien van informatiebeveiliging en cybersecurity zijn bepaald en vastgelegd.	A Het bestuur laat zich informeren. B De instelling adresseert risico's en beheersmaatregelen op het gebied van informatiebeveiliging en cybersecurity in het ICT Risk Management raamwerk in lijn met de eigen digitale operationele weerbaarheid strategie. C Het ICT-Risk Management Framework is onderdeel van het overall Risk Management raamwerk van de instelling. D De risicotoleranties ten aanzien van informatiebeveiliging en cybersecurity zijn bepaald en vastgelegd. E Het bestuur stelt voldoende middelen beschikbaar om effectieve beheersmaatregelen te treffen op grond van het risicoprofiel van de instelling en de risicobereidheid van het bestuur. F Het bestuur evalueert jaarlijks risicogebaseerd het gewenste/ benodigde niveau van volwassenheid van de 58 beheersmaatregelen. G Het bestuur evalueert jaarlijks, en bij grote ICT-gerelateerde incidenten, via een schriftelijk verslag over het resultaat van het ICT-Risk Management raamwerk.. H Het ICT-Risk Management raamwerk wordt regelmatig onderworpen aan (interne) audits.	Het raamwerk zal strategieën, beleid, procedures en protocols bevatten die nodig zijn om adequate bescherming te bieden ten opzichte van informatie en ICT assets. Verantwoordelijkheid voor het managen en 'overseeing' van ICT risico's is bij een tweedelijns functie belegd (of een passend niveau van onafhankelijkheid geborgd); Het raamwerk bevat een Digitale weerbaarheidsstrategie

3. DORA versus DNB GP Informatiebeveiliging

Conclusies

- DNB GP 2019 haalt de lat niet meer
- DNB GP beschrijft mitigerende maatregelen, DORA koppelt de maatregelen ook aan de risico's
- DNB GP meer focus op generiek ICT Beheerprocessen
- DNB GP 2023 bevat erg veel DORA vereisten, maar is nog niet volledig
- De vijf pijlers van DORA zijn veel gedetailleerder en meer voorschrijvend dan in DNB GP
- Risk versus Compliance!

STELLING 8

Wij voldoen aan de DNB GP IB, wij maken ons niet druk

STELLING 9

Aha, Compliance is aan zet…..

4. Manieren van toezicht op ICT-derden

Het bestuur van een financiële instelling dient regie te voeren over haar business partners met betrekking tot de naleving van DORA. Dit kan op verschillende manieren:

- Contractuele afspraken: Zorg voor duidelijke contractuele afspraken met de leveranciers waarin de vereisten en verantwoordelijkheden met betrekking tot DORA worden vastgelegd. Dit kan onder meer betrekking hebben op beveiligingsmaatregelen, incidentrapportageprocedures en compliance-monitoring.
- Periodieke rapportage: Vereis regelmatige rapportage van je IT dienstverleners over hun naleving van DORA-voorschriften, o.a. via ISAE3402, DNB self assessment en Service Level Rapportages. Dit kan onder meer betrekking hebben op incidenten, uitgevoerde beveiligingsmaatregelen, getroffen maatregelen voor operationele veerkracht en eventuele wijzigingen in de digitale infrastructuur.
- Audits en controles: Voer regelmatig audits en controles uit op de processen, systemen en beveiligingsmaatregelen van de IT dienstverleners om te controleren of deze voldoen aan de vereisten van DORA. Dit kan worden gedaan door interne auditors of externe specialisten op het gebied van IT-beveiliging.
- Risicomanagement: Zorg voor een gestructureerd risicomanagementproces waarin de risico's met betrekking tot de dienstverlening van de IT dienstverlener worden geïdentificeerd, geanalyseerd en beoordeeld. Dit stelt het bestuur in staat om proactief risico's te beheren en passende maatregelen te nemen om deze te verminderen of te beheersen.
- Samenwerking en communicatie: Onderhoud open communicatielijnen met de IT dienstverleners en werk samen aan het verbeteren van de naleving van DORA. Dit kan onder meer inhouden dat er regelmatig overleg is met vertegenwoordigers van de organisatie, deelneemt aan gezamenlijke workshops of trainingen, uitvoeren van penetratietesten en informatie deelt over best practices op het gebied van ICT-beveiliging en operationele veerkracht.

STELLING 10

Wij werken al 20 jaar met dezelfde IT partner, we vertrouwen elkaar volledig

5.  samengevat in kernpunten

De belangrijkste boodschap aan besturen van financiële instellingen over DORA is het belang van proactief handelen en het nemen van verantwoordelijkheid voor de digitale operationele veerkracht van hun organisatie.

Hier zijn de kernpunten:

- Naleving van regelgeving: Het is essentieel dat financiële instellingen voldoen aan de vereisten van DORA om de digitale operationele veerkracht te verbeteren en de integriteit van gegevens en systemen te waarborgen.
- Verantwoordelijkheid van de leiding: de leiding draagt de uiteindelijke verantwoordelijkheid voor de naleving van DORA en moet actief toezicht houden op de naleving van de regelgeving door de organisatie.
- Samenwerking met dienstverleners: Financiële instellingen moeten nauw samenwerken met dienstverleners, om ervoor te zorgen dat zij ook voldoen aan de vereisten van DORA.
- Risicomanagement en veerkracht: Het implementeren van effectief risicomanagement en het verbeteren van de operationele veerkracht van de organisatie zijn cruciaal voor het beschermen tegen cyberaanvallen, technische storingen en andere digitale bedreigingen.
- Continu leren en verbeteren: Financiële instellingen moeten zich voortdurend blijven ontwikkelen en verbeteren op het gebied van digitale operationele veerkracht door middel van training, educatie en evaluatie van best practices.

Al met al is het begrijpen en naleven van DORA van vitaal belang voor de financiële sector om de veiligheid, betrouwbaarheid en continuïteit van hun activiteiten te waarborgen in een steeds digitaler wordende wereld.

STELLING 11

We hebben momenteel de WTP te draaien, DORA moet even wachten

6. Te zetten stappen….

- Voer een gap-analyse uit op de DORA-vereisten mogelijk in relatie tot de huidige frameworks
  - Op basis van gestructureerde interviews
  - Kijk naar je ketepartners
  - Review van bestaande policies en procedures.
- Stel op basis van de uitkomsten van de gap analyse een roadmap op met onderwerpen zoals
  - ICT risicomanagement
  - ICT Incident management
  - Resilience testing
  - ICT third party risk management
- (Her)Overweeg ISO 27001 certificering als basis
  - Groeipad richting assurance verklaring

7. Discussie….

Bedankt voor uw aanwezigheid en aandacht, succes met uw DORA project

Dennis Boersen
+31 (0)6 3072 4840

argis consultants

Informatiebeveiliging • IT Auditing • Privacy

KVK 71841229 • BTW NL858870514B01
Katerveerdijk 17 • 8019 BL ZWOLLE • www.argis.nl