# Nieuwe wetgeving op komst voor cybersecurity

## De Digital Operational Resilience Act (DORA)

## Wat gaan we doen?

- Digitalisering biedt kansen voor onze bedrijfstak.
- Cyber-risico’s ook in de scope van de regelgever en de AFM.
- Adfiz trekt daarbij samen op met de AFM en ondersteunt de leden
- Presentatie AFM vandaag:
- Wrap up en gelegenheid voor vragen

# Voorstellen AFM medewerkers

Yuri Mol

Erik Dorland

Aimo Pieterse

# Toename digitalisering in de sector

BRANCHE

## Hoekstra deelt DNB-zorgen over techreuzen

Demissionair minister van Financiën ook bezorgd over Big Tech en lock-in.

Wopke Hoekstra © Rijksoverheid

FINANCIËLE SECTOR

## DNB: Amerikaanse big tech vormt gevaar voor Europese financiële stabiliteit

Bestuurders worden steeds banger voor cyberrisico's

12 maart 2021 De Redactie

Het meeste budget (een derde) willen ze vrijmaken voor digitalisering

Nederlandse topbestuurders maken zich het meest zorgen over cyberaanvallen en overregulering door de overheid. Vooral cyberveiligheid een groeiende bron van onrust in de bestuurskamer. Het is inmiddels een even grote zorg als overregulatie door de overheid, die al jaren

# De volgende golf van ransomware


RECENT IN SECURITY

Atlassian Confluence suite getroffen door ernstige kwetsbaarheid
6 september 2 min SECURITY

'Bluetooth BrakTooth-bugs treffen mogelijk miljarden apparaten'
3 september 2 min SECURITY

'Persoonlijke informatie buitgemaakt na hackaanval op HAN Hogeschool'
3 september 1 min SECURITY

## Politie: ransomware-infecties bij mkb-bedrijven schering en inslag

maandag 30 augustus 2021, 11:28 door **Redactie**, 18 **reacties**

Ransomware-infecties bij mkb-bedrijven zijn schering en inslag. Toch doen veel slachtoffers geen aangifte bij de politie en dat is wel belangrijk. Dat laat Matthijs Jaspers van de Nationale Politie tegenover **RTL Nieuws** weten. "We weten, het is schering en inslag, een ongelofelijke dreiging, maar dat zie je niet perse terug in de aangiftes."

# Huidige thema's IT toezicht AFM

**Cyber-criminaliteit**

- Continuïteit bedrijfsvoering
- Beveiliging van voorwetenschap

**Uitbesteding**

- Continuïteit bedrijfsvoering
- Belangen-conflicten
- Governance

**Cloud**

- Beveiliging van data
- Concentratierisico
- Jurisdictie risico's

**Informatie-beveiliging**

- Toepassing principes voor informatiebevei-liging

**Algoritmes**

- Governance algoritmes
- Governance ML/AI

**Data kwaliteit**

- Data management
- Historisch (klant)beeld

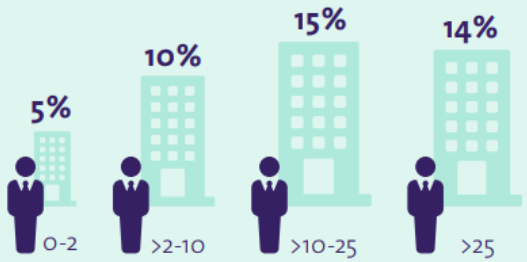
# Digitale weerbaarheid bij adviseurs en bemiddelaars

## Informatiebeveiliging van klantportalen 2018

**1428**
**adviseurs en bemiddelaars bieden een klantportaal aan**

### Functionaliteit klantportaal

**ICT kosten** als percentage van de omzet, gerelateerd aan omvang onderneming (o.b.v. fte)




Ondernemingen met een klantportaal geven gemiddeld **12%** van hun omzet uit aan **ICT**

**21%** van deze ondernemingen biedt klanten een vergelijkingsmodule aan op haar website, slechts 6% in combinatie met een klantportaal waarbinnen klanten zelf producten kunnen afsluiten


**Klanten kunnen binnen een vergelijkingsmodule de volgende producten vergelijken:**

**55%** schade particulier

**38%** zorg

**23%** schade zakelijk

**52%** van de ondernemingen gebruikt vergelijkingssoftware voor adviseurs

**26** ondernemingen gebruiken de vergelijkingsmodule als primaire bron bij de verwerving van nieuwe klanten

## Gebruik technologie en software

Veel ondernemingen communiceren nog op de **"traditionele"** manier met klanten:

**Gebruikte technologie**

**100%** klantportaal

**21%** vergelijkingstool

**9%** chatbot

**3%** geautomatiseerd advies

**Grote ondernemingen** lopen voorop in het gebruik van nieuwe communicatiemiddelen (**chatbots** en **geautomatiseerd advies** van website/ klantportaal)

**39**

**ondernemingen geven geautomatiseerd advies**

**De meest genoemde vormen van geautomatiseerd advies zijn:**

**40%** passende dekking schade

**32%** goedkoopste schade verzekering

**11** **ondernemingen gebruiken algoritmes om aanbod en/of pricing vast te stellen**

**9x** aanbod mede bepaald op basis van klantprofielen

**4x** prijs mede bepaald op basis van prijzen concurrenten

**6x** anders

(meerdere antwoorden mogelijk)

## Beveiligingsaspecten

**Klanten loggen in op het klantportaal via** → **Ter vergelijking:**

**Dual factor** authenticatie **5%**

**Single factor** authenticatie **94%**

**25%** van de ondernemingen vraagt dual factor authenticatie aan medewerkers bij het inloggen

**Overige veiligheidsmaatregelen mbt het klantportaal**

**18%** Klanten worden actief geattendeerd op beveiligingsaspecten en de maatregelen die klanten zelf kunnen treffen

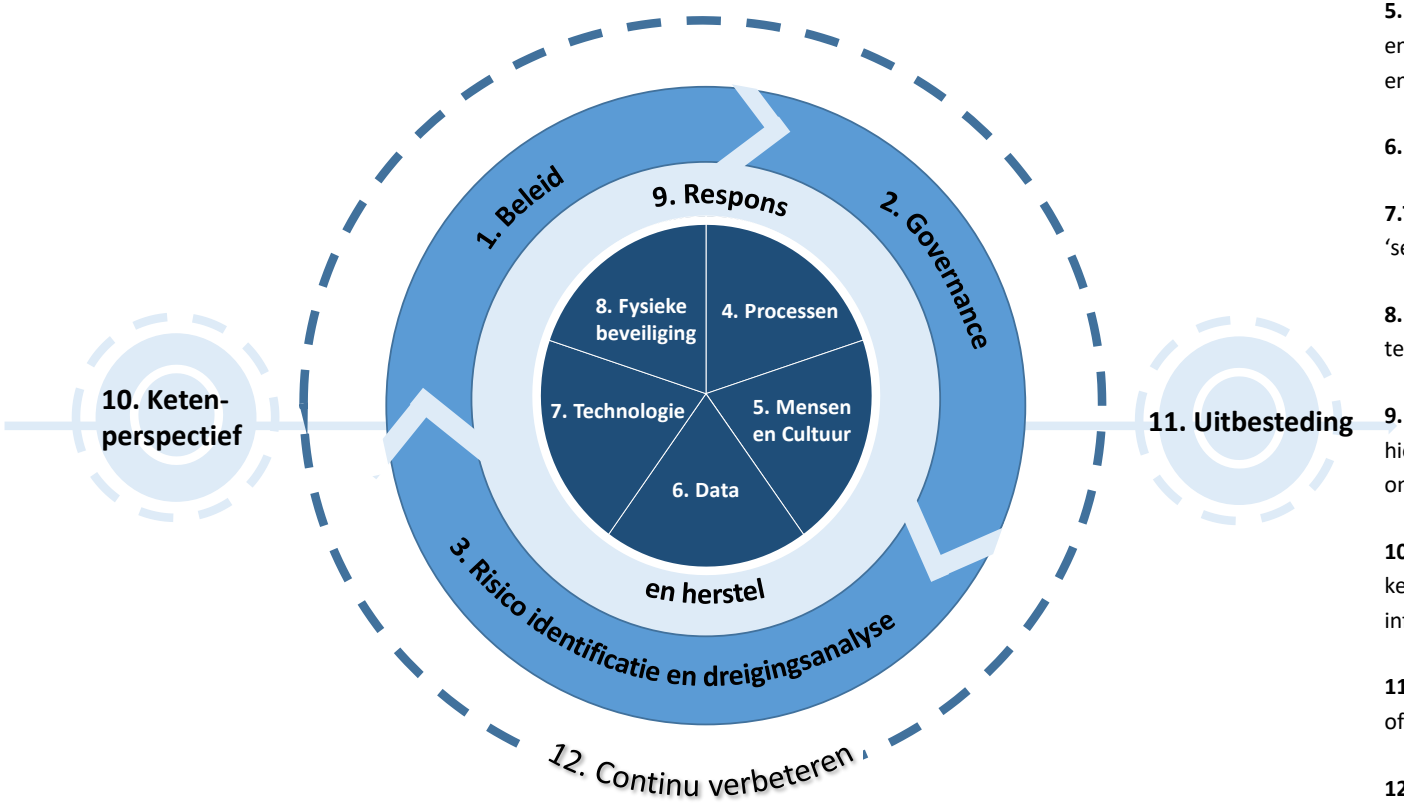
**40%** Wachtwoorden van klanten worden encrypted opgeslagen

**29%** van de communicatie tussen de portal en de back office vindt encrypted plaats

**47%** van de klanten wordt automatisch uitgelogd na een aantal minuten inactiviteit.

**Heeft de onderneming een beveiligingsbeleid gebaseerd op een risico-analyse van dreigingen? (afgezet naar omvang onderneming)**

# Uitgelicht: principes voor informatiebeveiliging




**1. Beleid:** De onderneming heeft een actueel informatiebeveiligingsbeleid waarin de wijze wordt beschreven waarop zij informatiebeveiliging waarborgt.

**2. Governance:** De onderneming heeft een governance structuur ingericht die effectieve informatiebeveiliging mogelijk maakt.

**3. Risico identificatie en dreigingsanalyse :** Informatiebeveiliging is ingericht op basis van een actueel inzicht in de interne en externe risico's en dreigingen, de potentiële impact van bestaande dreigingen en de risicobereidheid van de onderneming.

**4. Processen:** De inrichting van bedrijfsprocessen waarborgt de vertrouwelijkheid en integriteit van informatie en de beschikbaarheid van data en systemen.

**5. Mensen en Cultuur:** De onderneming onderkent het risico van menselijk handelen voor informatiebeveiliging en creëert een cultuur waarin medewerkers zich bewust zijn van het risico op informatiebeveiligingsincidenten en hierover open gecommuniceerd wordt.

**6. Data:** Beveiligingseisen zijn geïmplementeerd in lijn met de classificatie van informatie, data en va

**7.Technologie:** Bij de implementatie en het onderhoud van systemen wordt uitgegaan van het principe van 'secure by design'.

**8. Fysieke beveiliging:** De faciliteiten van de onderneming zijn ontworpen en ingericht om informatiebeveiliging te garanderen.

**9. Respons en herstel:** Ondernemingen zijn voorbereid op informatiebeveiligingsincidenten om de impact hiervan zo goed mogelijk te beperken. Wanneer zich een informatiebeveiligingsincident voordoet, treft de onderneming tijdig adequate respons- en herstelmaatregelingen.

**10. Ketenperspectief:** De onderneming past een integrale ketenbenadering toe waarbij de eigen plaats in de keten en de afhankelijkheden van andere ketenpartijen in acht wordt genomen bij het bepalen van informatiebeveiligingsrisico's en de benodigde beheersmaatregelen.

**11. Uitbesteding:** De onderneming is verantwoordelijk voor de informatiebeveiliging van uitbestede processen of systemen.

**12. Continu verbeteren:** De onderneming verbetert voortdurend haar informatiebeveiliging op basis van actuele inzichten in bestaande dreigingen en ontwikkelingen op het gebied van informatiebeveiliging.

n systemen.

# Uitgelicht: ketenrisico's in beeld

← Uitbestedingsuitvraag financieel dienstverleners

AFM

## Uitvraag uitbesteding financieel dienstverleners

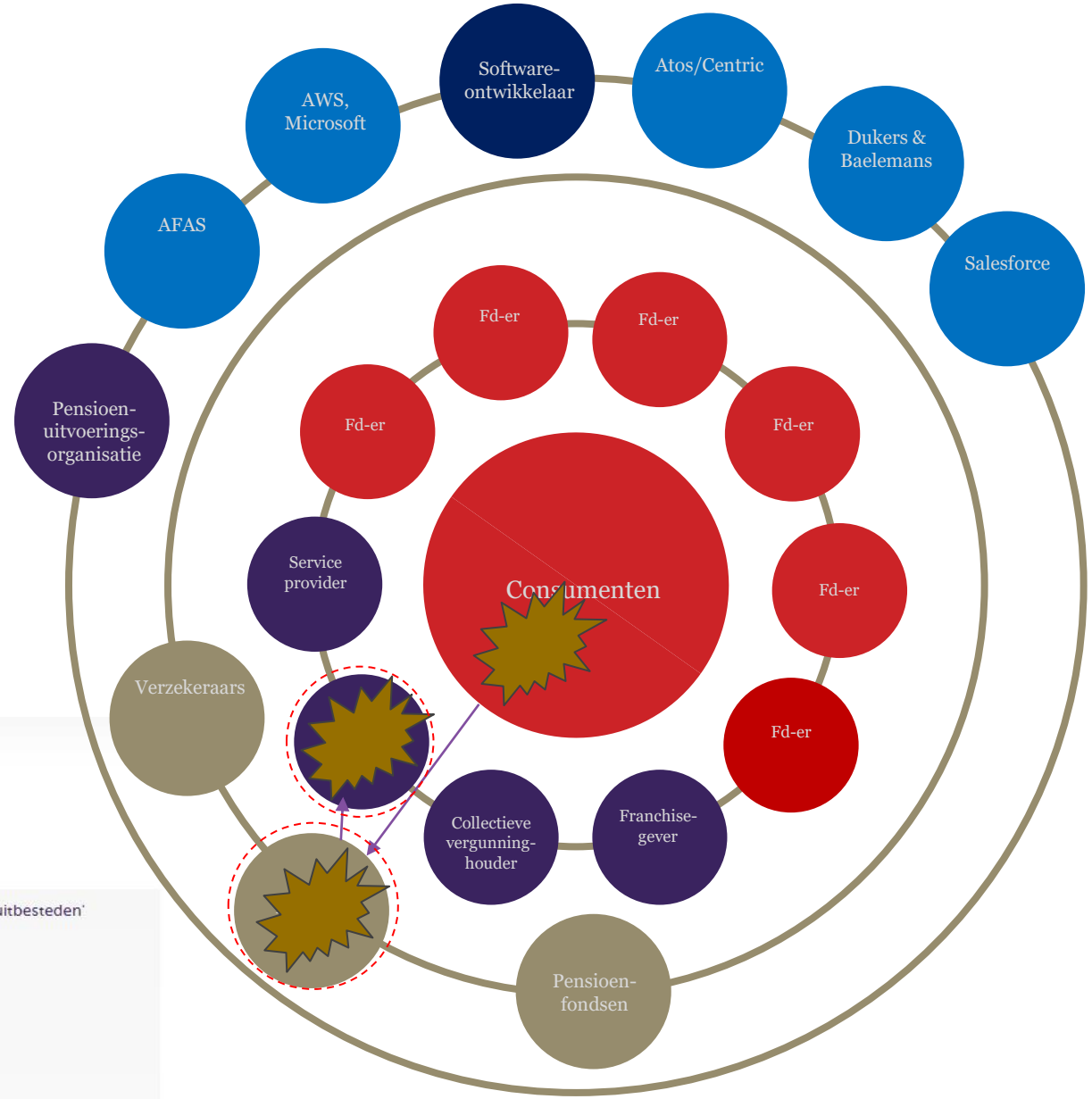
Financieel dienstverleners moeten jaarlijks aan de AFM doorgeven welke diensten en activiteiten de onderneming heeft uitbesteed. U ontvangt hiervoor een uitvraag van de AFM. De uitbestede diensten en activiteiten moeten worden aangeleverd in een vast format. Hieronder leest u meer over de uitvraag uitbesteding en de manier waarop u hieraan kunt voldoen.

## Uitbesteding diensten kent risico's voor dienstverleners en klanten

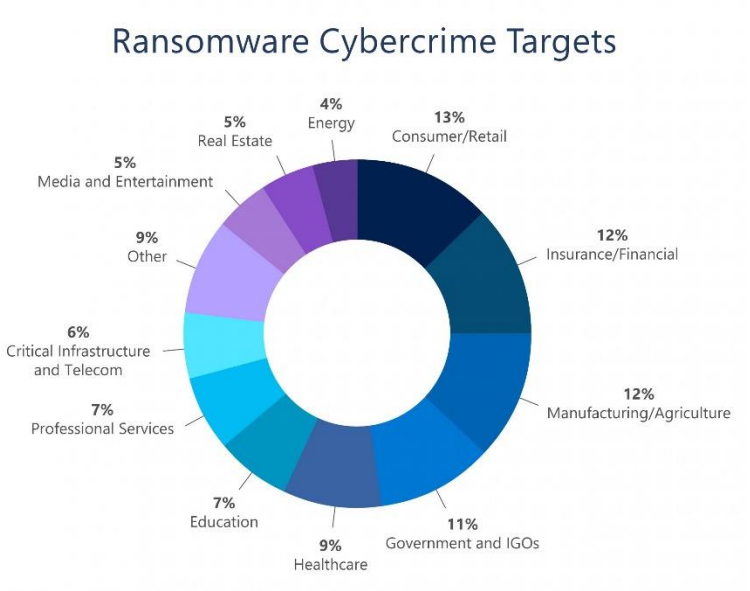
28 juni 2021 | **Nieuws**

Financieel dienstverleners moeten alert zijn op de risico's die komen kijken bij het uitbesteden van belangrijke en kritieke activiteiten. Mocht zich een incident voordoen, dan moeten zij dit in ieder geval melden bij de Autoriteit Financiële Markten (AFM). De AFM komt met aandachtspunten op basis van *good practices* hoe risico's te beheersen.

Verkenning 'Beheerst uitbesteden'



# DORA (Digital Operational Resilience Act)





## Achtergrond van het voorstel

- **Digitale technologieën of informatie- en communicatietechnologieën (ICT) brengen zowel kansen als risico's mee.** Die moeten goed worden begrepen en beheerd, vooral in tijden van stress. Beleidsmakers en toezichthouders hebben zich daarom steeds meer gericht op risico's die voortvloeien uit het gebruik van ICT.
- **ICT-risico's blijven echter een uitdaging** vormen voor de operationele veerkracht, de prestaties en de stabiliteit van het financiële stelsel van de EU.
- **Dit komt door een veelheid aan nationale regelgevingsinitiatieven** en toezichtbenaderingen.
- **Daarnaast hebben maatregelen op lidstaatniveau een beperkt effect** gezien het grensoverschrijdende karakter van ICT-risico's.
- **Bovendien hebben ongecoördineerde nationale initiatieven geleid tot overlappingen, inconsistenties**, dubbele vereisten, hoge administratieve en nalevingskosten – met name voor grensoverschrijdende financiële entiteiten – of ICT-risico's die niet worden ontdekt en dus niet worden aangepakt.
- **Deze situatie versnippert de Uniemarkt en brengt de bescherming van consumenten en beleggers in gevaar.**
- **Er is dus behoefte aan een gedetailleerd en geharmoniseerd kader.**

# DORA (Digital Operational Resilience Act)

## Een alomvattend en sectoroverstijgend kader inzake digitale operationele weerbaarheid in de EU, door:

- Geharmoniseerde regels voor het beheer van IT-risico's door financiële instellingen vast te stellen en te verdiepen;
- Het verplicht stellen van grondige tests van IT-systemen;
- IT-incidentrapportage te stroomlijnen;
- Toezichthouders meer bevoegdheden te geven om toezicht te houden op IT-uitbestedingen;
- Kritieke IT-dienstverleners (e.g., Microsoft, Amazon en Google) onder oversight te plaatsen van de ESA's.

### DORA kerninformatie:

- 40+ artikelen verdeeld over 5 onderdelen:
  - IT-risicomanagement;
  - IT-incidentrapportage;
  - IT tests, inclusief geavanceerde tests (i.e., TIBER) voor significante instellingen;
  - IT-uitbestedingsrisico's;
  - Informatie-uitwisseling;
- Scope: alle type marktpartijen onder toezicht van de AFM, m.u.v. accountantsorganisaties
- Proportionele toepassing met uitzonderingen voor micro- en kleine ondernemingen (<50 FTE en <10 mln EURO omzet op jaarbasis)
- Inwerkingtreding medio begin 2023 – implementatietermijn van 24 maanden

# Grijp nu je kans om je voor te bereiden

## Wat wordt er van je verwacht?

### DORA bestaat uit vijf zuilen

**IT-risicomanagement**

- Governance: verantwoordingsplicht leidinggevend orgaan
- Risicobeheersingskader en bijbehorende activiteiten (identificatie, bescherming en preventie, opsporing, reactie en herstel, leren en evolueren, crisiscommunicatie)

**IT-incidentrapportage**

- Gestandaardiseerde classificatie van incidenten
- Verplichte en gestandaardiseerde melding van ernstige incidenten
- Geanonimiseerde rapporten voor de hele EU

**IT tests, inclusief geavanceerde tests**

- Uitgebreid testprogramma, met de nadruk op technische tests, zoals pen-testing
- Voor significante instellingen om de 3 jaar grootschalige live tests (TLPT-tests zoals TIBER), uitgevoerd door onafhankelijke testers

**IT-uitbestedingsrisico's**

- Strategie, beleid, gestandaardiseerd informatieregister van IT-uitbestedingen
- Richtsnoeren voor precontractuele beoordeling, contractinhoud (lijst van standaardbepalingen), beëindiging, gestreste exit
- Opzetten van een kader voor toezicht op kritieke aanbieders in de hele EU, met duidelijke eisen en sancties

**Informatie-uitwisseling**

- Richtsnoeren inzake regelingen voor informatie-uitwisseling over cyberdreigingen en -kwetsbaarheden

# DORA (Digital Operational Resilience Act)


## Grijp nu je kans om je voor te bereiden

### Hoe bereid je je voor?

Inventariseer je huidige relevante beheersmaatregelen (controls)

- Gap analysis
- Plan van aanpak
- Implementatie van beheersmaatregelen

Heb je de juiste kennis in huis? Denk aan…

- Technische IT kennis
- Compliance/juridisch
- IT risico beheersing

Begin zo spoedig mogelijk! DORA wordt medio begin 2023 van kracht, met een implementatietermijn van 24 maanden.

## Wrap up van vandaag

- Wat kan je nu al doen inzake cyberrisks en digitale weerbaarheid:
  - Identity access management (IAM): gebruikersnamen, wachtwoorden, rechten. Wie mag waar bij? In kaart brengen en periodiek controleren, wijzigen. MultiFactor.
  - Malware / Ransomware / Fishing mail. Awareness training, Backups
  - Verlies van Data (datalek/databreach). Back-ups, maar ook, hoe snel ben je weer in de lucht. Beoordeel met name eigen procedures en uitbestedingsrelaties.
  - Cyber verzekering voor het eigen bedrijf. Financiële schade en professionele hulp

Einde presentatie

# Vragen