EYE on Finance

FEBRUARI 2025 | EDITIE 1

BOARD MATTERS

Gezamenlijke certificeringen zijn de toekomst

MICHEL RUIJTERMAN
Volksbank

INTERVIEW

MET AI KREGEN WE SNELLER INZICHT IN HONDERDEN CONTRACTEN

MARCEL PRINS
COO van Robeco

DUURZAAMHEID

Welke risico's kleven aan duurzaamheidsdata?

DICK DE WAARD
Emeritus hoogleraar aan de Rijksuniversiteit Groningen

DORA

Wat heeft Nederland met DORA te winnen?

EY
Shape the future with confidence

INHOUD

04

VOORWOORD
Wat heeft Nederland met DORA te winnen?
Marc Welters (EY): "Is een organisatie die alle vereisten van DORA afvinkt *resilient*? Dat is nog maar de vraag."

06

BOARD MATTERS
Alles wat aandacht krijgt groeit Michel Ruijterman (Volksbank): "De tijd dat bankieren draaide om mensen die de beste deals sloten, ligt achter ons. Alles is IT."

12

KORT NIEUWS

14

INTERVIEW
Met AI kregen we sneller inzicht in honderden contracten
Marcel Prins (Robeco) bespreekt hoe DORA bijdraagt aan beter inzicht in risico's en benadrukt het belang van transparantie en AI in de financiële sector.

20

DUURZAAMHEID
Financiële instellingen zuigen zich vol met duurzaamheidsdata, maar dat brengt ook risico's met zich mee Dick de Waard (emeritus hoogleraar aan de Rijksuniversiteit Groningen) pleit ervoor dat bedrijven, accountants en toezichthouders zich niet laten leiden door de letter van de wet en vooral op zoek gaan naar het echte verhaal met de bijbehorende dilemma's.

24

ESSAY
Hoe DORA de relatie met leveranciers verandert
Saskia Vermeer (HVG Law): "DORA vraagt om een andere mindset, zeker in organisaties waarin business units gewend zijn om redelijk onafhankelijk van elkaar in silo's te opereren."

28

ROUND TABLE
Sommige organisaties moeten van nul naar honderd in vijf seconden
Experts van DNB, AFM, EY en HVG Law gaan in gesprek over de interpretaties van de geest van de wet.

30

VIJF VRAGEN
5 vragen over DORA
Hoe verandert DORA het risicolandschap? We vroegen Florian Jacoby (EY) naar de impact van DORA op risicomanagement en operationele veerkracht binnen de financiële sector.

Colofon

EYE on Finance
is een periodieke uitgave van EY Accountants B.V. voor relaties in de financiële sector.

Contact
EY Accountants B.V.
T.a.v. EY Brand, Marketing and Communications
Postbus 2295
3000 CG Rotterdam

Tel. 088 407 10 00
E-mail: info@nl.ey.com
Internet: ey.com/nl

Redactie EY
Jennifer van Eekelen,
Joost Elsenburg (HVG Law),
Shokhan Masifi,
Jan Slager,
Annelies Termote,
Marc Welters.

Met medewerking van
Dirk van der Lit
en Nart Wielaard

Vormgeving & Fotografie
Clubgeist

Drukwerk
Damen Drukkers

VOORWOORD

MARC WELTERS
Partner EY Financial Services
T +31 (0)6 2125 2223
E marc.welters@nl.ey.com

Wat heeft Nederland met DORA te winnen?

Als een van de meest gedigitaliseerde landen ter wereld, zit IT in Nederland in de haarvaten van organisatieprocessen. Dat vereist een volwassen vorm van IT-beheersing.

We hebben nog moeite om risico's te mitigeren rond uitval van IT. Daardoor ontstaan problemen die vroeger ondenkbaar waren. Bijvoorbeeld het voorval van een kaasleverancier, die als gevolg van een computer hack, zodanige leverings-problemen had, dat er drie weken lang geen kaas in het schap lag bij de grootste supermarktketen van Nederland.

Waar bedrijfsprocessen (zoals inkoop) eigenlijk nauwelijks aan verandering onderhevig zijn, is dat bij IT voortdurend het geval. Denk aan nieuwe patches of updates van IT-leveranciers of de komst van nieuwe providers. Denk ook aan het verzoek van DNB aan de financiële sector om de risico's van *quantum* in kaart te brengen. Heel verstandig, want als we daadwerkelijk te maken krijgen met quantum-computers, kunnen we de bestaande maatregelen rond IT-beveiliging wel vergeten.

De komst van DORA is dan ook positief, omdat het organi-saties wettelijk verplicht om de IT-beheersing naar een hoger volwassenheidsniveau te brengen. Je kunt stellen dat de wet repareert wat we zelf hebben nagelaten te regelen. Is een organisatie die alle vereisten van DORA afvinkt *resilient*? Dat is nog maar de vraag. Prima dat voor het aantrekken van een IT-medewerker een VOG nodig is, maar er zijn ook IT'ers die uit hoofde van hun functie alles zien en overal bij kunnen komen. Zouden daar niet zwaardere eisen voor moeten gelden? In het licht van DORA kunnen organisaties dit ook oppakken.

In Nederland lopen we van oudsher voorop als het om resilience gaat. Nadat als gevolg van de kredietcrisis het nationale toezicht op systeembanken verhuisde naar de ECB, is de kwaliteit van het toezicht niet per se beter geworden. Zeker niet omdat ICT in het toezicht van de ECB, destijds, een ondergeschikte rol speelde. DNB liep met het *good practice information security* altijd voorop In Nederland.

Nog een positief inzicht. In het interview met Marcel Prins van Robeco (zie rubriek Klantinterview) kwam de inzet van AI bij de registratie van uitbestedingspartijen ter sprake. In plaats van het handmatig navlooien van honderden contracten blijkt AI de afdeling Legal bijzonder goed te ondersteunen. Op deze manier daagt DORA organisaties uit om hun IT in te zetten voor een grotere weerbaarheid. Lees vooral ook het artikel met Michel Ruijterman van de Volksbank, die aangeeft dat de implementatie van DORA bijdraagt aan een veiligere en robuustere financiële wereld. Mooie voorbeelden!

Ten slotte nog een mededeling van huishoudelijke aard. Met veel plezier heb ik de afgelopen tien jaar de hoofd-redactie van dit mooie magazine voor mijn rekening genomen. In de afgelopen tien jaar hebben we er met het hele redactieteam, de lezers en de te interviewen personen een strak en kwalitatief goed magazine van gemaakt. Met ingang van deze editie van Eye on Finance draag ik mijn functie over aan collega Jan Slager, die ik daarmee veel succes toewens en waarvan ik weet dat hij het magazine weer een grote stap verder brengt.

Ik wens u veel leesplezier en hoop dat wij met deze editie van Eye on Finance bijdragen aan *shape the future with confidence*.

Bedankt, Marc!

Marc Welters heeft de afgelopen tien jaar met veel toewijding de hoofdredactie van Eye on Finance gevoerd. We zijn hem enorm dankbaar voor zijn inzet en creativiteit.

Dankzij hem is Eye on Finance geworden wat het nu is: een magazine met aansprekende en actuele artikelen, dat met plezier wordt gemaakt en gelezen.

Nogmaals bedankt Marc, voor alles wat je voor het magazine hebt gedaan!

Met vriendelijke groet,

DE REDACTIE VAN EYE ON FINANCE

BOARD MATTERS

INZICHTEN IN UITDAGINGEN, TRENDS EN BEST PRACTICES VAN TOONAANGEVENDE BEDRIJVEN IN EEN COMPLEXE ZAKELIJKE OMGEVING. DE GESPREKKEN DIE DE KOERS BEPALEN EN ORGANISATIES RICHTING GEVEN IN EEN VERANDEREND LANDSCHAP STAAN CENTRAAL. DEZE RUBRIEK LAAT ZIEN HOE STRATEGISCHE KEUZES ORGANISATIES WEERBAAR EN TOEKOMSTBESTENDIG MAKEN.

MICHEL RUIJTERMAN
CIO van de Volksbank

Michel Ruijterman ziet hoe de invoering van DORA bijdraagt aan vertrouwen in de financiële sector. Met deze Europese wetgeving wordt de lat hoger gelegd op het gebied van IT-weerbaarheid, wat volgens Ruijterman niet alleen essentieel is voor banken, maar ook inspiratie biedt voor andere sectoren. In een gesprek deelt hij hoe DORA leidt tot een robuustere keten, betere samenwerking en een veiliger digitaal landschap.

Alles wat aandacht krijgt groeit

Michel Ruijterman is CIO van de Volksbank en lid van het Executive Committee. Hij was de trekker van de implementatie van DORA en ziet hoe deze wetgeving bijdraagt aan het vertrouwen in de financiële sector. Sterker nog, soortgelijke maatregelen mogen van hem best voor meer sectoren gaan gelden en juicht dan ook de komst van NIS2 toe, stelt hij in het gesprek met Marc Welters partner EY.

Water stroomt naar het laagste punt. Die metafoor maakt duidelijk waarom het voor een financiële instelling belangrijk is om kwetsbaarheden in de digitale infrastructuur goed te managen. Uiteraard wil je het meer dan moeilijk maken voor malafide partijen, variërend van een *lone wolf* die zijn kunsten laat zien tot goed georganiseerde cybercriminelen die met een duidelijk doel opereren. Dat is belangrijk want financiële instellingen zijn de afgelopen decennia natuurlijk – in oneerbiedige termen – bijna IT-fabrieken geworden. De tijd dat bankieren draaide om mensen die de beste deals sloten, ligt achter ons. Alles is IT.

Met de metafoor van het water in gedachten kun je heel egoïstisch redeneren dat je liever hebt dat niet jij, maar je buurman het laagste punt is. Maar beter is om de sector als geheel sterker te maken en ook dat is welbegrepen eigenbelang. Banken bestaan immers bij de gratie van het vertrouwen van hun klanten. En als er bij een collega wat grondig mis zou gaan, straalt dat ook op ons af. Heel praktisch: als mensen een week lang bij een bank niet bij hun geld zouden kunnen, heeft dat natuurlijk ook effect op andere banken. Precies daarom ben ik blij met de komst van DORA. Deze Europese wetgeving legt de op het gebied van IT-weerbaarheid lat een stuk hoger voor de hele sector. Er is sprake van een *Level Playing Field*.

De implementatie van DORA heeft wat mij betreft zeker bijgedragen aan een veiligere en robuustere financiële wereld. Dat is op meerdere terreinen te zien. We testen nieuwe systemen nog meer dan al het geval was. We monitoren bestaande systemen intensiever. We zetten in op penetratietesten door ethische hackers om eventuele kwetsbaarheden bloot te leggen. We hebben nadrukkelijker dan ooit ons Business Continuity Management georganiseerd: als er wat mis gaat weten we wat we moeten doen. En, misschien wel een van de belangrijkste thema's van DORA, we hebben meer focus gelegd op leveranciersmanagement.

> “Gezamenlijke certificeringen zijn de toekomst.
>
> **MICHEL RUIJTERMAN**
> *CIO van de Volksbank*

Een stabiele en weerbare financiële sector vergt meer dan ooit maatregelen in de hele keten, want door de digitalisering zijn we steeds meer verknoopt geraakt met technologieproviders, van de grote bekende partijen als Microsoft en Amazon tot kleinere partijen die gespecialiseerde diensten bieden. Ook in die keten geldt dat water het laagste punt zoekt en dus is het zaak de hele keten op het juiste niveau te krijgen.

Op dat punt leverde DORA een intensief traject op. We hebben hiervoor honderden contracten grondig geanalyseerd en/of herzien en daarbij ging het om een brede scope aan toeleveranciers, want DORA ziet niet alleen maar op outsourcing van IT, maar ook op partijen die hardware leveren. In die contracten speelde een veelheid van onderwerpen een rol. Denk aan het recht op monitoring en audit.

Maar denk ook aan het bepalen van een exit-strategie en een goede voorbereiding op wat er gebeurt als een partij in de keten omvalt. En dan mogen we natuurlijk data-integriteit en gegevensbescherming niet vergeten.

> “De tijd dat bankieren draaide om mensen die de beste deals sloten, ligt achter ons. Alles is IT.

Dit zijn zulke essentiële onderwerpen dat ze ook volwaardige aandacht verdienen op de agenda van de board. Ik ben als CIO weliswaar de trekker van het project maar we zijn nadrukkelijk verantwoordelijk met het hele Excutive Committee. Tijdens het traject hebben we dan ook met grote regelmaat sessies georganiseerd om iedereen op het vereiste niveau te krijgen qua kennis, en het is mooi om te zien hoe iedereen daar vanuit een eigen invalshoek naar het thema kijkt. Bij die brede aanpak hoort ook een goede voortgangsrapportage over wat er wel en niet goed gaat. Aangezien we het project via een *agile* methode hebben opgepakt, hebben we besloten om simpelweg inzicht te geven met een zandlopertje dat laat zien hoever we waren met het oppakken van de 200 *epics* (bundels van taken). Natuurlijk is dat arbitrair want de ene *epic* is belangrijker dan de andere. Maar waar het bij zo'n indicator om gaat is dat het leidt tot een goed gesprek erover. Alles wat aandacht krijgt groeit.

Het mooie van DORA is dat het in de hele Europese Unie van toepassing is en dat je toeleveranciers dus niet hoeft te overtuigen dat er aanpassingen nodig zijn in contracten en *service level agreements*. Bij andere (nationale) wetgeving was dat soms best lastig maar hier is echt sprake van een collectieve uitdaging. De uitdaging waar de sector nu voor staat is nog meer gezamenlijkheid aan te brengen. Ik moedig dan ook aan dat er gezamenlijke certificeringen en dergelijke komen zodat er collectief een efficiënte en effectieve aanpak ontstaat.

Verder heeft DORA ons tot verdere professionalisering van domeinen zoals Business Continuity Management heeft geleid. We zetten daar bijvoorbeeld software *tooling* in zodat we dat efficiënt kunnen aanpakken en daarmee maar beperkt menskracht hoeven in te zetten. Menskracht die schaars verkrijgbaar is.

Met dat alles komt wat mij betreft ook de vraag op of soortgelijke eisen niet van toepassing zouden moeten zijn voor andere sectoren. Voor de 'BV Europa' als geheel. Mijn antwoord is duidelijk: jazeker. Als we een manier kunnen vinden om dat proportioneel te doen – dus de eisen afstemmen op de specifieke risico's van de sector – zou dat enorm waardevol zijn voor een weerbare economie.

De waarde van DORA

Michel Ruijterman is in een gesprek over DORA positief over het effect:

- Een Level Playing Field in Europa waar alle financiële instellingen aan dezelfde eisen moeten voldoen
- Verhoogd bewustzijn over waarom het belangrijk is dat derde partijen aan strikte voorwaarden moeten voldoen
- Een mogelijke springplank om met dergelijke eisen ook in andere sectoren bij te dragen aan meer stabiliteit

Actualiteit pensioentransitie centraal op evenement Leaders in Finance

Wat zijn de belangrijkste lessen van de koplopers in pensioenland tijdens hun pensioentransitie?

Op deze prikkelende vraag volgt een antwoord tijdens het Leaders in Finance Pensioen Event, dat plaatsvindt op donderdag 10 april 2025 in conferentiehotel Kontakt der Kontinenten te Soesterberg. Dit evenement, waarvan EY de hoofdpartner is, richt zich op de brede doelgroep van pensioenprofessionals in Nederland. Onder leiding van dagvoorzitter Parcifal van Overbeek (Achmea) komen diverse actuele thema's aan bod. Bijvoorbeeld in de vorm van drie panels die zich buigen over technologische innovatie, legal & communicatie en het pensioenecosysteem. Twee interessante keynote sprekers zullen met hun bijdrage ongetwijfeld stof tot nadenken geven.

De openingsspeech wordt verzorgd door regeringscommissaris Fieke van der Lecq, die ingaat op de huidige stand van zaken met betrekking tot de pensioentransitie. De afsluitende keynote komt van pensioencoryfee Gerard van Olphen, die zijn licht laat schijnen over toekomstige ontwikkelingen in het pensioenlandschap.

HILDEGARD ELGERSMA
Sectorleider Pensioenen en WTP consulting lead EY
T +31 (0)6 2908 3018
E hildegard.elgersma@nl.ey.com

LEES MEER OVER
Leaders in Finance Pensions event 2025

Nieuwe IT-verslaggevingsstandaard van NOREA in februari 2025 definitief geïntroduceerd

De NRI-standaard voor IT-beheersing geeft holistische en kostenefficiënte impuls aan rapportages.

Het sluitstuk gedurende die aanloopperiode vormden twee geslaagde pilots met het *NOREA Reporting Initiative (NRI)* bij zorgverzekeraar CZ en infrabedrijf Arcadis. De bedoeling is dat de standaard gebruikt gaat worden door organisaties die zich over hun IT-beheersing willen verantwoorden. Door te voldoen aan de NRI-standaard zouden organisaties automatisch ook compliant zijn aan een lange reeks Europese uitvoeringswetten, zoals DORA, NIS2, de AI Act, de DS Act en de DM Act. "En mogelijk tientallen andere Europese wetten die nog in de pijplijn zitten", voegt voorzitter Marc Welters van NOREA eraan toe. "Op die manier verwachten we een forse administratieve last te voorkomen."

Interne urgentie

De NRI-standaard was aanvankelijk bedoeld voor het afleggen van verantwoording over IT-beheersing aan externe stakeholders, legt Welters uit. "De komst van DORA en NIS2 heeft de urgentie van interne verslaggeving vergroot. Bestuurders en commissarissen zijn gewend risicorapportages te ontvangen die zijn opgesteld door de tweede lijn en de interne accountantsdienst. Het zijn nuttige rapportages omdat ze iets zeggen over de IT-risicobeheersing. Wat evenwel ontbreekt is een holistische rapportage over Cybersecurity, *IT Continuity, Data Governance & Ethics, Outsourcing, Digital Innovation* en *Privacy*." Die gedachte vindt ook elders weerklank. NOREA is benaderd door ECP Platform voor de Informatie-Samenleving, onderdeel van het ministerie van Economische Zaken, voor doorontwikkeling van de standaard. Welters: "ECP is voornemens om een platform op te richten voor onderhoud van de NRI-standaard. Naar het voorbeeld van de structuur van de Raad voor de Jaarverslaggeving is het de bedoeling dat daarin auditors, verslaggevende entiteiten en gebruikers participeren." Het platform gaat monitoren of nieuwe wetgeving noodzaakt tot eventuele aanpassingen van de NRI-standaard. Ook de komst van nieuwe technologie, met name sterk groeiende deelsegmenten zoals *AI, Internet of Things en Operational IT*, kan daartoe aanleiding geven. Welters van NOREA is verheugd dat pilots de robuustheid van de nieuwe standaard hebben bevestigd. De bij CZ uitgevoerde pilot was vooral gericht op de interne informatievoorziening. Desgevraagd zei voorzitter Pieter Jongstra van de RvC van CZ daarover: "Dankzij deze rapportage over de NRI-standaard heb ik nu voor het eerst op één plaats een volledig beeld gekregen van de IT-beheersing van een organisatie waar ik als toezichthouder actief ben."

MARC WELTERS
Partner EY Financial Services en voorzitter NOREA
T +31 (0)6 2125 2223
E marc.welters@nl.ey.com

INTER-VIEW

GESPREKKEN MET TOONAANGEVENDE EXPERTS, BELEIDSMAKERS EN LEIDERS UIT DE FINANCIËLE SECTOR. HUN VISIE, UITDAGINGEN EN STRATEGIEËN BIEDEN EEN SCHERP INZICHT IN DE ONTWIK-KELINGEN DIE DE SECTOR VORMGEVEN.

MARCEL PRINS
COO van Robeco

Marcel Prins is COO van Robeco en was vanuit die rol verantwoordelijk voor de implementatie van DORA. In gesprek met Marc Welters (EY) waarschuwt hij dat we moeten oppassen voor *regulatory overreach* in Europa, maar is positief over het effect van DORA. "Het vertaalt zich in beter zicht op je risico's."

Met AI kregen we sneller inzicht in honderden contracten

Het is zover. DORA is van kracht geworden en dat was voor financiële instellingen een pittige kluif, al was het alleen maar vanwege de veelheid en complexiteit aan relaties met derde partijen. Wat is achteraf gezien een van de belangrijkste leerervaringen bij Robeco?

"Dat de timing bij zo'n wetgevingstraject erg lastig is. Het thema waar DORA op inspeelt is geen verrassing, we zijn bij Robeco immers altijd bezig om nog beter in control te raken over *third party risk* en we weten dat er veel afhankelijkheden zijn in een wereld waarin alles met alles is verbonden. Die inspanningen konden we mooi integreren in de aanpak voor de implementatie van DORA. Maar veel details van die wetgeving kwamen pas heel laat beschikbaar. En dat leverde dan stevige dilemma's op: gaan we bepaalde dingen doen voordat die details bekend zijn en daarom misschien moeten bijsturen? Of wachten we nog even, wetende dat dat ook problemen kan opleveren in een heel drukke verander-kalender?"

Third party risk is inderdaad niet nieuw, zoals je zelf ook aangeeft. Is DORA daarmee eigenlijk het repareren van iets wat allang gerepareerd had moeten zijn?

"Nee, die term zou ik niet gebruiken. DORA leverde bij ons vooral reflectie op over hoe afhankelijk we zijn van technologie, data en daarmee ook van andere partijen. DORA dwingt tot transparantie over die afhankelijkheden zodat iedereen goed zicht krijgt op de concentratierisico's. In de zomer van 2024 waren de gebeurtenissen rondom Cloudstrike natuurlijk een serieuze wake up call op dat thema. Veel partijen die op zwart gingen realiseerden zich waarschijnlijk vooraf niet eens dat ze last zouden ondervinden doordat ze zich niet bewust waren van de afhankelijkheden in de keten."

Zijn er derde partijen die gedurende het traject als gevolg van de vergaande DORA verplichtingen afzagen van een relatie met Robeco?

"Nee. En dat heeft alles te maken met ons beleid. Voor bedrijfskritische processen hebben we altijd ingezet op partners die topkwaliteit leveren en laten we geen ruimte voor opportunisme. We doen zaken met partijen die sowieso hun Europese markt niet willen verliezen en dus willen voldoen aan DORA."

Waar zaten de praktische uitdagingen in dit project?

"*The devil is in the detail*. In de zomer hebben we veel gesprekken met leveranciers gevoerd over de contracten die we met hen hebben. Dat leidde dan bijvoorbeeld tot aanvullende clausules of hoe de rapportage over hun eigen uitbestede processen eruit moet zien. Overigens heeft AI-tooling ons daarbij enorm geholpen om inzicht te krijgen."

Scherper zicht op ketenrisico's

Marcel Prins is positief over wat de implementatie van DORA heeft gebracht voor Robeco. In een financiële wereld die sterk met elkaar verknoopt is in lange ketens, is het essentieel om scherp zicht te hebben op de afhankelijkheden en daarmee ook de risico's in de keten. DORA heeft daar positief aan bijgedragen, al was het wel een arbeidsintensief traject.

“Je bent altijd kwetsbaarder dan je denkt.

Op wat voor manier?

“Een van de uitdagingen is dat we veel contracten moeten analyseren op een aantal aspecten die in DORA zijn opgenomen. Dat is heel veel werk. In ons geval gaat het om ongeveer 200 contracten. We hebben een test gedaan door drie contracten te laten analyseren door een vendor manager en een jurist – beide mensen – en dezelfde drie contracten te analyseren met 32 ‘AI-prompts’. Toen bleek dat het AI-model het veel sneller deed dan de mens, maar niet altijd 100% correct. AI heeft dus wel een enorme versnelling kunnen brengen in de analyse, waarbij de mensen wel altijd de eindcontrole deden. We gebruiken intern ook steeds meer de prompt buddy van Microsoft Copilot om van elkaar te leren hoe je de beste vragen kunt stellen aan de tool en passen dat ook op andere vlakken toe. Bijvoorbeeld op het vlak van quality assurance om verschillende interne documenten te analyseren op consistentie helpt AI ons heel goed. Dat is heel waardevol, zolang je er als mens maar supervisie op houdt. Onze centrale boodschap is dan ook: *don’t stop thinking*.”

Hoe kijk je aan tegen het wereldwijde level playing field vanuit de verplichtingen die DORA in Europa oplegt?

“De trend is wereldwijd hetzelfde. Ook in het Verenigd Koninkrijk en de Verenigde Staten zetten toezichthouders hoog in op *resilience*. En doordat de technologie zich in razend tempo ontwikkelt, zullen de toezichtkaders zich ook blijven ontwikkelen. Dat is goed, ik heb afgelopen jaar gezien dat DORA zorgt voor meer bewustwording en ook dat het leidt tot beter inzicht in je risico’s. Heel waardevol. Tegelijkertijd moeten we in Europa wel opletten dat we niet doorschieten in *regulatory overreach*.”

Zou DORA in aangepaste vorm ook voor andere sectoren moeten gelden? Resilience is bijvoorbeeld ook voor de voedselvoorziening en daarmee voor supermarkten belangrijk?

“Elk bedrijf moet zich bewust zijn van de risico’s en je bent eigenlijk altijd kwetsbaarder dan je denkt. Maar er is wel een verschil tussen een kaasleverancier en een bank. Als je drie weken geen kaas hebt, is dat heel vervelend, maar als er drie weken geen financieel systeem is, dan is dat rampzalig. Het vertrekpunt van DORA is het zorgen voor stabiliteit in het financiële systeem. Het goede nieuws is dat met de toekomstige implementatie van de Network and Information security Directive (NIS2) een Europese richtlijn wordt toegepast voor beveiliging van informatiesystemen van alle vitale sectoren, zoals telecom, cloud providers en voedselvoorziening. Daarmee wordt onze hele samenleving meer *resilient*.”

DUURZAAMHEID

IN ELKE EDITIE VAN EYE ON FINANCE BESTEDEN WE AANDACHT AAN DUURZAAMHEID. WE VERKENNEN DE NIEUWSTE TRENDS, INZICHTEN EN BEST PRACTICES DIE FINANCIËLE PROFESSIONALS HELPEN OM DUURZAAMHEID TE INTEGREREN IN HUN WERKZAAMHEDEN. ONTDEK HOE DE SECTOR BIJDRAAGT AAN EEN DUURZAMERE TOEKOMST EN WELKE STAPPEN ER WORDEN GENOMEN OM POSITIEVE IMPACT TE REALISEREN.

DICK DE WAARD
Emeritus hoogleraar Rijksuniversiteit Groningen

Dick de Waard leerde in dertig jaar tijd als accountant, met vallen en opstaan, hoe om te gaan met duurzaamheidsrapportages.

Hij pleit ervoor dat bedrijven, accountants en toezichthouders zich niet laten leiden door de letter van de wet en vooral op zoek gaan naar het echte verhaal met de bijbehorende dilemma's. Boerenverstand gebruiken dus en stel vooral veel vragen.

Financiële instellingen nemen duurzaamheidsdata op, maar tegen welk risico?

Decennialang hebben politici, zowel nationaal als internationaal, geprobeerd het bedrijfsleven in beweging te brengen op het vlak van duurzaamheid. Het SER-rapport *De Winst van Waarde* uit 2000 is nog steeds inhoudelijk actueel. In die decennia was er af en toe succes, maar was er vooral ook de nodige traagheid. Om deze traagheid te doorbreken, is er nu op Europees niveau een stevige golf aan wetgeving, waaronder de bekende Corporate Sustainability Reporting Directive (CSRD), die hoge eisen stelt aan het rapporteren over duurzaamheid.

Volgens De Waard, die zelf al betrokken was bij de controle van duurzaamheidsverslagen toen deze nog voornamelijk opmerkingen over 'geitenwollen sokken' opleverden, zijn accountants nu pas echt wakker geworden over het nut en de noodzaak van duurzaamheidsrapportages.

"Accountants zitten nu met veel vraagtekens over wat ze met die rapportages moeten. Dat is begrijpelijk, want het onderliggende informatielandschap is nog niet volwassen. Maar het grootste probleem is dat het vakgebied gewend is met checklists te werken, terwijl dit terrein nu juist vraagt om veel eigen inschattingen en professional judgement. Mijn advies: gebruik je verstand, stel vragen en durf gewoon te beginnen. Vooral voor kleinere organisaties is er wettelijk gezien een ingroeimodel; het hoeft dus niet meteen perfect te zijn. Overigens moeten ook toezichthouders een nieuw terrein onder de knie krijgen. Zij hebben nu ook geen idee hoe ze naar de rapportages moeten gaan kijken."

Waarvan acte. De Waard die ook betrokken is bij de financiële sector – onder andere als lid van de Sustainability Advisory Board van ABN AMRO MeesPierson – weet dat financiële instellingen 'datafabrieken' zijn geworden, met tentakels die tot diep in de keten reiken. Dit brengt echter risico's met zich mee. Met de komst van DORA wordt de lat voor risicobeheersing hoger gelegd, wat gezien de ontwikkelingen geen overbodige luxe is. De Waard wijst erop dat er een directe relatie bestaat tussen DORA en de eerder genoemde duurzaamheidswetgeving. Concreet verwijst hij naar ESRS S4, die regelt hoe bedrijven de belangen van de consument behartigen en hoe transparant ze hierover zijn. Dezelfde duurzaamheidswetgeving vereist ook veel informatie over de klanten, waaraan diensten worden geleverd. Op een breed terrein zien we dan ook dat financiële instellingen als een stofzuiger alle informatie opzuigen die ze hiervoor nodig hebben. Denk bijvoorbeeld heel concreet aan data over de isolatie van het huis waarin je woont. Maar denk ook aan informatie over hoe duurzaam de vrachtwagens van een transportonderneming bij de fabrikant worden geproduceerd.

Bij het gebruik van deze informatie spelen verschillende dilemma's. Tot hoever moet je klanten bijvoorbeeld aanmoedigen om duurzame keuzes te maken, zowel in hun beleggingen als voor hun woning? Wat mogen we van

bedrijven in sterk concurrerende markten verwachten, als de klanten van deze bedrijven niet willen bijdragen aan de investeringen in duurzaamheid? De Waard meent dan ook dat vooral die dilemma's een prominente plek in de rapportage moeten krijgen. En dat accountants juist daar veel aandacht aan moeten besteden. Maar dat terzijde. Want zijn belangrijkste punt is: door die verantwoordelijkheid heeft een financiële instelling beschikking over een enorme rijkdom aan informatie. En die informatie kan gevoelig zijn vanuit privacyperspectief – bijvoorbeeld, je wilt niet met de wereld delen hoe je huis geïsoleerd is of dat je in een oude diesel rijdt – maar ook vanuit strategische overwegingen: de genoemde truckfabrikant wil niet dat de concurrent meer weet dan noodzakelijk.

De Waard: "Wetgevers en beleidsmakers geven financiële instellingen een belangrijke rol in de transitie naar een duurzame wereld. En om die rol te pakken zijn ze hongerig naar duurzaamheidsinformatie. Ze moeten zich goed realiseren welke risico's daarmee gepaard gaan."

> "Ook toezichthouders moeten een nieuw terrein onder de knie krijgen. Zij hebben nu ook nog geen idee hoe ze naar de rapportages moeten gaan kijken.

ESSAY

Hoe DORA de relatie met leveranciers verandert

Er bestaat helaas geen *one-size-fits-all* aanpak voor financiële instellingen die de Digital Operational Resilience Act (DORA) moeten implementeren. Integendeel, het is een complexe exercitie om leveranciers te screenen op potentiële risico's. Dat vraagt ook iets van de interne organisatie: van werken in silo's naar een uniforme governance en samenwerking.

DORA bouwt voort op eerdere *guidelines* van Europese toezichthouders. Regelgeving op het gebied van (IT-)uitbesteding is natuurlijk niet nieuw. DORA is dat wel, omdat het een verordening is die zich exclusief richt op de financiële sector. Deze legt talrijke verplichtingen op ten aanzien van digitale operationele weerbaarheid. Een verordening heeft directe werking, en daarmee is de impact veel groter dan die van Europese richtlijnen, de bekende *directives*. DORA, onderdeel van de *Digital Finance Strategy* van de Europese Unie, brengt veel onderwerpen onder één paraplu en legt de lat daarmee aanzienlijk hoger dan in het verleden. Niet eerder trokken Europese lidstaten op het gebied van digitale weerbaarheid zo gemeenschappelijk op.

MAATWERK BLIJFT NODIG

Waar in de financiële wereld de focus voorheen vooral lag op kapitaalbeheersing en financiële soliditeit, is digitale weerbaarheid nu ook uitgegroeid tot een belangrijk thema. Verwonderlijk is dat niet, want de gevolgen van digitale disrupties zoals *ransomware* of gegevensverlies bij financiële instellingen, zijn uitermate omvangrijk. Klanten van deze instellingen vormen de meest kwetsbare doelgroep om ten prooi te vallen aan *phishing* en andere vormen van digitale criminaliteit. Bovendien is de financiële sector van groot belang voor het maatschappelijk verkeer en daarom is gereguleerd toezicht noodzakelijk. Met de komst van DORA is nu sprake van een overkoepelend framework. De verordening is tevens een nieuwe maatstaf voor het risicobeheer van derde partijen, in het bijzonder partijen die IT-diensten leveren: de *third party service providers*. Meer specifiek volgen uit DORA verschillende verplichte bepalingen die een financiële instelling moet opnemen in elk contract met een partij die hen IT-diensten levert.

Bij nieuwe wetgeving ligt het ontstaan van een vinkjescultuur op de loer, waarbij de implementatie gemakkelijk wordt afgedaan. Maar een standaardcontracttekst die alle vereisten voor alle derde partijen dekt, bestaat niet. DORA draait om een risicogebaseerde aanpak. Het is geen *one-size-fits-all*. Eén allesomvattend template om alle risico's af te dekken, is in de praktijk niet beschikbaar en ook niet wenselijk. Neem bijvoorbeeld het ontwerp van een exitstrategie om de samenwerking met een IT-leverancier op te zeggen zonder dat dit de continuïteit van de organisatie schaadt. Je kunt voor zo'n complexe exercitie misschien wel een checklist hanteren, maar maatwerk blijft nodig.

INTENSIEF SAMENSPEL EXPERTISES

Vanaf begin 2024 zien we een versnelling in het tempo waarmee financiële instellingen zich met DORA bezighouden. Onder juristen, riskmanagers, CIO's, CFO's en CRO's is het bewustzijn sterk gegroeid dat DORA impact heeft op hun werk. Als gevolg van een verzwaarde aansprakelijkheid geldt dit inmiddels ook voor (overige) bestuurders en commissarissen. DORA is daarom tegenwoordig in veel organisaties onderwerp van gesprek bij de koffieautomaat.

> "Eén allesomvattend template om alle risico's af te dekken, is in de praktijk niet beschikbaar en ook niet wenselijk.

> DORA vraagt om een andere mindset, zeker in organisaties waarin business units gewend zijn om in silo's te opereren.

De belangrijkste doelstelling van DORA is de continuïteit van dienstverlening door digitale operationele weerbaarheid. Dat vraagt om uitvoerige *due diligence* bij ICT-relaties en de bijbehorende leveranciers. Er zijn assessments nodig om te beoordelen of een dienstverlener een prestatie nog kan leveren als er bijvoorbeeld calamiteiten zijn. Met andere woorden: hoe waarborgen we dat de kritieke infrastructuur onder alle omstandigheden kan voortbestaan? Dat vraagt om een intensief samenspel van allerlei expertises binnen organisaties, waaronder juristen.

Er gaan geluiden op dat een verordening zoals DORA een 'verdienmodel' voor juristen zou zijn. Dit doet echter geen recht aan de cruciale rol die juristen spelen in het waarborgen van een solide juridische basis voor de implementatie en naleving van dergelijke regelgeving. Hoewel DORA veel raakvlakken heeft met ICT, risk en governance, is de betrokkenheid van juristen essentieel. DORA creëert niet alleen nieuwe verplichtingen, maar ook een geheel nieuw speelveld van samenwerking en onderhandelingen. Juridische expertise is nodig om ervoor te zorgen dat DORA niet slechts een technische oefening blijft, maar een geïntegreerde aanpak oplevert die organisaties als geheel versterkt.

STAP NAAR DE RECHTER

De verordening DORA bestaat uit ongeveer zeventig artikelen verdeeld over vijf pijlers en daaronder hangen in totaal zo'n 1.200 individuele verplichtingen. Deze verplichtingen zijn nader uitgewerkt in *Regulatory* en *Implementation Technical Standards*. Ze geven aan wat er specifiek in een IT-contract moet staan, hoe je audits inricht en ICT-incidenten classificeert en rapporteert. Ook de wijze van selecteren van IT-leveranciers en verplichtingen naar de toezichthouder zijn in deze standaarden geregeld.

DORA verplicht financiële instellingen om in hun contracten met IT-leveranciers duidelijke afspraken te maken over onderaannemers en de beveiliging van gegevens. Deze eisen versterken de nadruk op het risicomanagement in de gehele IT-keten en creëren een juridisch afdwingbaar kader voor de rechter. Hoewel het lastig te voorspellen is of dit zal leiden tot meer juridische procedures, wordt het voor instellingen cruciaal om hun contractuele verplichtingen grondig te herzien. Veelal zal het noodzakelijk zijn om contracten open te breken en afspraken met leveranciers te onderwerpen aan onderhandelingen. Al met al is het een gigantische screenings- en onderhandelingsoperatie.

Financiële instellingen moeten diensten van IT-leveranciers kunnen opschorten of zelfs beëindigen als ze risico's voor de continuïteit van hun dienstverlening identificeren. In sommige gevallen leveren IT-leveranciers een kleine hoeveelheid diensten aan een beperkt aantal partijen.

Als die diensten worden beëindigd, is dat funest voor hun businessmodel. Dat benadrukt het belang van een goede overeenkomst waarin cybersecurityrisico's tijdig zijn geïdentificeerd en afgedekt. Hoewel IT-geschillen veelal via schikkingen worden opgelost, zou DORA wel eens een verschuiving kunnen inluiden naar meer juridische procedures.

ANDERE MINDSET NODIG

Instellingen moeten DORA mede vanuit groepsniveau benaderen. Kwetsbaarheden dienen gezamenlijk te worden getackeld volgens een uniform stramien. Eventuele boetes worden immers ook op groepsniveau opgelegd, waardoor instellingen lokale incidenten niet kunnen of mogen negeren. In het kader van mogelijke reputatieschade is het sowieso onverstandig om te denken dat eventuele incidenten zich lokaal vanzelf wel oplossen.

Financiële instellingen beschikken doorgaans al over een governance en (IT-)infrastructuur om aan deelvereisten van DORA te voldoen. Een van de grootste uitdagingen is echter om te komen tot een holistische benadering. Daarbij wordt in kaart gebracht hoe de organisatie opereert en waar lacunes zitten ten opzichte van de verplichtingen van DORA. Er moeten ook verbindingen worden gelegd tussen de vijf pijlers van DORA. Dat vraagt om een andere *mindset*, zeker in organisaties waarin business units gewend zijn om redelijk onafhankelijk van elkaar in silo's te opereren.

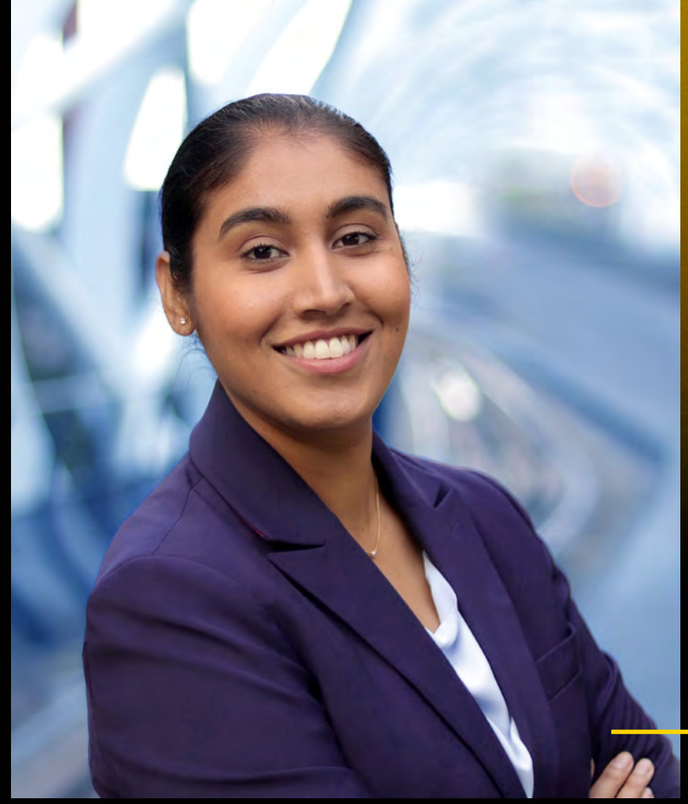
DORA markeert een nieuwe fase in de regulering van digitale operationele weerbaarheid binnen de financiële sector. Een succesvolle implementatie hangt af van gedegen governance, maatwerk in contracten en een nauwe samenwerking tussen juristen, IT-specialisten en riskmanagers.

SASKIA VERMEER-DE JONGH
Partner HVG Law
T +31 (06) 2908 3850
E saskia.vermeer@hvglaw.nl

Maatwerk blijft nodig

- Eén allesomvattend template om alle risico's af te dekken, is in de praktijk niet beschikbaar en ook niet wenselijk.
- Een succesvolle implementatie hangt af van gedegen governance, maatwerk in contracten en een nauwe samenwerking tussen juristen, IT-specialisten en riskmanagers.

TOM VAN DE VEN
Manager Operational & IT Risk bij Autoriteit Financiële Markten



RUDRANI DJWALAPERSAD
Partner Technology Consulting bij EY

ROUND TA BLE

IN ELKE EDITIE VAN EYE ON FINANCE GAAN DIVERSE EXPERTS OM DE TAFEL OM HUN INZICHTEN EN ERVARINGEN UIT TE WISSELEN OVER DE ONTWIKKELINGEN IN DE FINANCIËLE SECTOR. HIER WORDEN IDEEËN EN INNOVATIEVE STRATEGIEËN BESPROKEN DIE DE SECTOR VOORUIT HELPEN. LEES MEE EN ONTDEK HOE DEZE GESPREKKEN BIJDRAGEN AAN EEN VOORUITSTREVENDE FINANCIËLE TOEKOMST.

JACCO JACOBS
Department head operational & IT risk bij De Nederlandsche Bank

Sommige organisaties moeten van nul naar honderd in vijf seconden

Toezichthouders DNB en AFM hebben vanaf begin dit jaar met DORA een nieuw thema in het vizier. Al is het thema ook weer niet heel nieuw. In een roundtable met Jacco Jacobs (DNB), Tom van de Ven (AFM) en Rudrani Djwalapersad (EY) onder leiding van gespreksleider Joost Elsenburg (HVG Law) blijkt dat zij de geest van de wet centraal willen stellen en graag in gesprek zijn met instellingen over interpretaties.

Cyberweerbaarheid is belangrijk. En vla is meestal geel. Dit is geen nieuws, hoewel de wereld soms verrast is wanneer incidenten blootleggen hoe afhankelijk de financiële wereld is van stabiele en betrouwbare technologie achter de schermen. De Europese wetgeving van DORA heeft op dit vlak ook een taak in petto voor toezichthouders. Wat betekent dit voor de teams die zich specifiek met dit thema bezighouden?

VAN DE VEN: "Het aantal collega's binnen AFM dat zich hiermee bezighoudt, is verdubbeld naar vijftien mensen. Een belangrijke reden is dat de AFM intensiever dan voorheen toezicht op IT risico's zal gaan houden bij de ondernemingen die onder deze wet vallen, denk bijvoorbeeld aan vermogensbeheerders. Financiële instellingen in Nederland vallen voor de beheersing van hun IT risico's tot op heden veelal onder de Wet op het financieel toezicht (Wft), maar de eisen op dat vlak zijn niet erg specifiek. De komst van DORA heeft dat veranderd: deze instellingen hebben nu te maken met behoorlijk gedetailleerde eisen op dat vlak. Vooral voor de wat kleinere partijen geldt soms dat zij van nul naar honderd moeten in vijf seconden. We hebben daar in 2024 dan ook veel aandacht aan besteed en campagnes gevoerd om het bewustzijn en de kennis in de sector te verhogen."

DJWALAPERSAD: "Oorspronkelijk was de groep organisaties die onder DORA viel nog groter en vielen ook accountantskantoren zoals EY eronder. Ook deze groep zou te maken krijgen met een compleet nieuwe realiteit. Het is niet ondenkbaar dat dat alsnog zal gebeuren, aangezien de Europese Commissie DORA binnen twee jaar gaat evalueren."

JACOBS: "In het geval van DNB is de verandering minder ingrijpend. De onder toezicht staande instellingen waren al jaren bezig met cyberweerbaarheid. Het grote verschil is dat we met DORA van een open norm naar precieze voorschriften zijn gegaan. Financiële instellingen moeten bijvoorbeeld een informatieregister bijhouden voor alle contractuele overeenkomsten met derde partijen. En wat ook veel impact had: de *Threat Led Penetration Testing* (TLPT), een test voor het identificeren van kwetsbaarheden waar een selectie instellingen aan wordt onderworpen. En meer in algemene zin willen instellingen natuurlijk weten hoe streng we als toezichthouder zijn."

> "Vanuit onze toezichtstaak vinden we het heel belangrijk om te zien dat het 'three lines' model binnen organisaties goed werkt.

En? Hoe streng zijn jullie?

JACOBS: "Niet strenger of minder streng dan partijen van ons gewend zijn. En er zit ook geen verrassing in de middelen die we gebruiken. Het gaat ook bij deze wet om het bekende toezicht-arsenaal, van het beoordelen van rapportages tot deep dives op bepaalde aspecten, tot het voeren van normoverdragende gesprekken indien nodig. We leggen wel bepaalde accenten als het om DORA gaat. Begin 2025 letten we vooral op of de instellingen hun informatieregisters op orde hebben en of ze goede procedures hebben voor het rapporteren van incidenten. Maar de werkwijze is niet anders dan ze gewend zijn voor het toezicht vanuit de Wet Financieel Toezicht (Wft). In het verleden maakten we onder meer gebruik van de *'good practice'* informatiebeveiliging, een open norm. Die is nu ingehaald door de komst van DORA, en we gebruiken nu het wettelijk kader zoals DORA ons biedt."

VAN DE VEN: "Ook bij ons is er geen sprake van een koerswijziging in hoe we toezicht houden. Het wordt weliswaar intensiever, maar het blijft risico-gebaseerd, en met proportionaliteit als centraal uitgangspunt. De instellingen weten welke middelen we hebben om toezicht te houden. Wat ik belangrijk vind, is een goed gesprek. Zeker bij de komst van nieuwe wetgeving is er soms sprake van onzekerheden en interpretaties. En ook wij zijn niet alwetend. Als toezichthouder gaan we graag het gesprek aan en instellingen hoeven dan ook geen enkele schroom te hebben om zaken aan te kaarten, zij hoeven niet bang te zijn dat ze daarna extra kritisch bekeken zullen worden. Ons emailadres werkt gewoon!"

JACOBS: "Eens, we pogen als toezichthouder toegankelijk en transparant te zijn en dragen onze interpretaties ook uit in bijvoorbeeld seminars en roundtables."

DJWALAPERSAD: "Dat neemt niet weg dat veel instellingen met lastige vraagstukken te maken hebben of hadden. Vaak is *professional judgement* door de instellingen nodig voor de naleving van één wet, maar zij hebben te maken met toezichthouders in verschillende landen die andere interpretaties kunnen hebben. Daar zijn zorgen over."

Delen jullie die zorgen bij AFM en DNB?

JACOBS: "Voor de grootbanken maken we deel uit van internationale joint supervisory teams van het SSM. En er is veel internationaal overleg en afstemming tussen toezichthouders. Maar natuurlijk zal er altijd enige vorm van interpretatie zijn. Onze basisgedachte is en blijft dat het gaat om het zo goed mogelijk mitigeren van risico's, en daar gaan we het gesprek over aan.

VAN DE VEN: "Laten we niet vergeten waar we vandaan komen qua wetgeving. Er was juist veel wildgroei en grote verschillen tussen de 27 lidstaten. Nu hebben we één wet – bereikt na veel internationaal overleg en compromissen – en dat is pure winst, ook al omdat je op een thema als weerbaarheid geen concurrentie tussen landen wilt hebben. Het is een wet die behoorlijk voorschrijvend is en waar dus weinig ruimte is voor interpretaties."

DJWALAPERSAD:
"Goed punt. Een wetgevingstraject als NIS2 kent veel meer verschillen. Misschien was het goed geweest om die ook op deze leest te schoeien."

In hoeverre kunnen jullie gebruik maken van (rapportages van) de accountant of IT-auditor in het toezicht op dit thema?

VAN DE VEN: "Als onafhankelijke toezichthouders moeten we onze eigen toezichtwerkzaamheden verrichten, maar we nemen uiteraard ook kennis van relevante werkzaamheden van de accountant of IT auditors. We zijn zeker niet blind voor hun bevindingen en juichen toe dat er meer aandacht komt van hen voor onderwerpen als cyberweerbaarheid."

JACOBS: "Vanuit onze toezichtstaak vinden we het heel belangrijk om te zien dat het *'three lines'*-model binnen organisaties goed werkt, en we nemen zeker kennis van de rapportages van accountants en IT-auditors al was het maar omdat we daarmee beter focus in ons eigen werk kunnen aanbrengen."

DJWALAPERSAD: "NOREA heeft het *NOREA Reporting Initiative* gelanceerd, een nieuwe manier om inzicht te bieden in de beheersing van IT. Dat levert toezichthouders op dit terrein heel waardevolle informatie op. En minstens even belangrijk: het geeft het management handvatten om te verbeteren en aan te sturen."

JACOBS: "Als bestuurder moet je echt bezig zijn met cyberweerbaarheid, je kunt dit niet weg delegeren. En dat betekent dat je ook de kennis moet hebben om de juiste vragen te stellen, bijvoorbeeld over dit IT-beheersingsverslag. En dat kennisniveau verdient hier en daar nog wel wat aandacht. De komst van de NRI juichen we zeker toe, dit draagt bij aan bewustwording en inzicht aan de bestuurstafel, alsmede bij toezichthouders als RvC-leden."

Het perspectief van de toezichthouder

- De basisgedachte is en blijft dat het gaat om het zo goed mogelijk mitigeren van risico's.
- Graag samen met onder toezicht staande instellingen het gesprek aangaan over hoe risico's worden beheerst
- Gebruik maken van het werk (en de bevindingen) van IT auditors en accountants waar dat mogelijk is

5 vragen over DORA

Begin 2024 is Florian Jacoby overgestapt van de Franse naar de Nederlandse EY adviespraktijk, waar hij zich bezighoudt met risk management in combinatie met operational *resilience*. We vroegen hem naar zijn ervaringen.

1

Hoe verandert DORA het risicolandschap voor digitale en operationele veerkracht binnen de financiële sector?
"DORA heeft zeker de potentie om dat landschap fundamenteel te wijzigen op basis van een uniform regelgevingskader. Deze harmonisering door middel van standaardisering van vereisten voor financiële instellingen is cruciaal. Dat zorgt voor een uniforme wijze van bijvoorbeeld het melden van incidenten en risico's in relatie tot derde partijen. Daarvoor moet iedere financiële instelling een robuust raamwerk implementeren voor het identificeren, inschatten en mitigeren van kwetsbaarheden. Dat gaat echt veel verder dan bijvoorbeeld de European Banking Authority-richtlijnen voor het managen van uitbestedingsrisico's rond derde partijen. Mede daarom voldoen veel instellingen nog niet volledig aan de DORA-eisen."

2

Welke stappen moeten financiële instellingen minimaal zetten om compliant te blijven?
"Instellingen hebben zich tot nu toe vooral gefocust op DORA *gap assessments* en het opstellen van *road maps* om aan de regels te voldoen. Dat zijn zinvolle exercities voorafgaand aan de implementatie van een *ICT Risk Management Framework*. Daarnaast moet een heldere governancestructuur zijn ingericht die precies aangeeft waar welke verantwoordelijkheden liggen. Bovendien moeten er processen en protocollen aanwezig zijn om het ICT Risk Management Framework te versterken, de testvereisten te beheren en incidenten tijdig te kunnen melden."

3

Welke belangrijkste openstaande problemen zie je nog?
"De implementatie van DORA stelt financiële instellingen voor verschillende uitdagingen. Kleinere instellingen kunnen problemen ondervinden door beperkte middelen en expertise, wat leidt tot verschillen in nalevingsniveaus. Bovendien wordt het harmoniseren van DORA voor alle EU-lidstaten bemoeilijkt door verschillen in nationale regelgeving en toezichtspraktijken. Het beheersen van risico's van derden, met name van wereldwijde serviceproviders, maakt de zaak nog ingewikkelder omdat instellingen de naleving van DORA in verschillende regelgevende omgevingen moeten waarborgen."

4

Hoe verhoudt DORA zich tot andere wetgeving, zoals GDPR en NIS2?
"Deze wetgevingen zijn naar mijn mening bijzonder verweven met elkaar. Sommige instellingen benaderen regelgeving liever afzonderlijk en proberen daar dan aan te voldoen door individuele vereisten af te vinken. Zo werkt het niet. In mijn optiek is het noodzakelijk om een integrale visie te ontwikkelen op *operational resilience* in relatie tot regelgeving als DORA, GDPR en NIS2. Daartussen moet je verbindingen maken. Er is van nature al een verbinding tussen GDPR en DORA, waar de gemeenschappelijk focus ligt op het beschermen van data en het melden van incidenten. NIS2 legt meer de nadruk op cyber security en *resilience*, en ook die elementen komen we tegen in DORA. Wel hanteren DORA en NIS2 ieder hun eigen verslaggevingskader; waar DORA de impact van incidenten op financiële stabiliteit meeneemt, vereist NIS2 inzicht in de impact op de continuïteit van de dienstverlening."

5

Wat komt er na DORA nog op ons af aan resilience?
"Als het gaat om cyberveiligheid zullen instellingen in de toekomst ongetwijfeld geconfronteerd worden met nieuwe risico's. Bijvoorbeeld door de toepassing van kunstmatige intelligentie. Dat zal zeker leiden tot het ontstaan van nu nog onbekende risico's waarvoor de huidige regelgeving onvoldoende bescherming biedt. Het ligt voor de hand dat daarvoor aanvullende wetgeving nodig zal zijn. Ik denk in dat verband ook aan één van de pijlers van DORA over het tussen financiële instellingen onderling op vrijwillige basis delen van informatie over beveiligingsincidenten. Dat zou op termijn best een verplichting kunnen worden."

FLORIAN JACOBY
Senior Manager EY Financial Services Risk Consulting
T +31 (06) 5544 2465
E florian.jacoby@nl.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

ED None
155010984

ey.com/nl


Will you shape the future
or be shaped by it?
With our full spectrum of services, skills and ecosystem partners, EY teams help create new value across sectors.
ey.nl
The better the question.
The better the answer.
The better the world works.
EY
Shape the future with confidence
© 2025 EYGM Limited. All Rights Reserved. ED None.