DORA-compliance:
gedeeld probleem, gedeelde oplossingen?

De Europese verordening DORA is sinds een jaar van kracht. Organisaties moeten daarmee aan nieuwe regels voldoen om de digitale weerbaarheid te vergroten. Kunnen we daar niet meer in samenwerken? Daar gingen verzekeraars over in gesprek tijdens een rondetafel van MeasureWorks en DEI.



Jan-Dirk Rundervoort
Leveranciersmanager, ONVZ



Roelof Muis
Projectleider, Stichting VbV



Marcel Schipper
Sales Director, MeasureWorks

DORA staat voor de Digital Operational Resilience Act. Deze verordening moet de digitale weerbaarheid van de financiële sector vergroten. Daarvoor zijn tal van nieuwe regels ingevoerd, zoals de verplichte melding van IT-incidenten en het regelmatig uitvoeren van ethische hacktests.

Maar de focus ligt niet alleen op financiële organisaties zelf. Zij moeten ook grip hebben op hun kritieke ketenpartners. Een storing bij een IT-leverancier kan immers net zo ontwrichtend zijn als een storing bij de organisatie zelf.

Impact op verzekeraars

DORA geldt ook voor verzekeraars. Tijdens een rondetafel van DEI en MeasureWorks op 19 maart 2026 deelden zij hun ervaringen.

Neem ONVZ. Leveranciersmanager Jan-Dirk Rundervoort legt uit dat uitbestedende partijen vroeger als kritiek of belangrijk werden bestempeld, maar dat DORA ook het aanmerken van kritieke functies verplicht stelt. "Wij hebben het hoofdprocessenmodel gepakt en gezegd: dit zijn al onze functies. Een deel daarvan hebben we als kritiek gelabeld."

Daarnaast gelden er nieuwe eisen aan de selectie, contractering en dienstuitvoering van IT-dienstverleners, en zijn er inhoudelijke vereisten voor IT-contracten. ONVZ pakte dit praktisch op: een addendum bij bestaande contracten, bijgewerkte risicoanalyses en een vernieuwd control-framework.

Ook gaat er nu een kwartaalrapportage naar de Raad van Bestuur. Waardoor deze altijd geïnformeerd blijven over de kritieke of belangrijke uitbestedingen en de eventuele uitstaande acties daarbij.

Kan dat niet samen?

De uitdagingen bij ONVZ spelen bij vrijwel alle verzekeraars. Toch wordt er maar beperkt samengewerkt. Het Verbond van Verzekeraars heeft een standaard addendum voor DORA-compliance, en ervaringen worden gedeeld via CIO Platform en CIO-overleggen.

Maar het addendum moet door iedere verzekeraar nog organisatie-specifiek worden gemaakt, wat de tijdswinst beperkt. Bovendien vragen alle verzekeraars afzonderlijk informatie op bij hun leveranciers, ook als ze dezelfde leveranciers hebben. "Kun je geen gemeenschappelijk register maken?", vraagt Rundervoort zich af.

Vrees bij ketenpartners

Verzekeraars hebben zo hun uitdagingen rondom de DORA, maar ketenpartners ook. Bijvoorbeeld Stichting VbV, een gezamenlijk initiatief van Nederlandse schadeverzekeraars. Deze stichting ondersteunt schadeverzekeraars, verzekerden, leasemaatschappijen en verhuurbedrijven om vermiste en gestolen voertuigen terug te vinden en terug te bezorgen.

Stichting VbV is dus geen financiële organisatie, wat betekent dat het zelf niet onder de DORA valt. Maar het is een ketenpartner van verzekeraars, die wél DORA-verplichtingen hebben. "De vrees die wij hebben is: hoe gaan verzekeraars straks hun eisen doorzetten en opleggen aan leveranciers en derde partijen?", zegt Roelof Muis, Projectleider bij Stichting VbV. "Als al die partijen straks hun eigen eisen aan ons op gaan leggen, wordt dit voor ons heel groot."

Stichting VbV is immers een kleine organisatie en heeft in tegenstelling tot grote verzekeraars geen hele afdeling om hiermee aan de slag te gaan. De uitdagingen blijken al wel bij de invoering van ISO 27001, waar de organisatie nu voor gecertificeerd wordt. "We zitten nu nog in de fase van het uitrollen van het juiste gedrag. Denk aan: je moet je computer echt even vergrendelen als je naar de WC gaat. Voor grote partijen is dat al routine, maar voor ons nog niet".

"WIJ HEBBEN LIEVER ÉÉN SOFTWAREPROGRAMMA WAAR ALLES IN STAAT."

Muis roept dan ook op veel te standaardiseren, zoals governance, technologie onboarding en leveranciersbeheer. “Er zijn ontzettend veel Excel-lijsten waar wij graag vanaf willen. Eén wijziging moet je op wel acht plekken doorvoeren, en daar allemaal versiebeheer voor bijhouden. Wij hebben liever één softwareprogramma waar alles in staat.”

Onderling vertrouwen

Rundervoort zag de samenwerkingsuitdaging met eigen ogen. "Ik was in 2024 bij een bijeenkomst met veel partijen. Daar was de stelling: we moeten van alles, laten we nu één manier bedenken om dat te doen. Dan kunnen we het werk verdelen en richting toezichthouders hetzelfde verhaal met bijbehorende bewijslast vertellen." Daar werd enthousiast op gereageerd en er kwam een tweede sessie. Daar werd besloten om het addendum van het Verbond van Verzekeraars zo aan te passen dat iedereen dezelfde kan gebruiken. Ook werd bedacht om samen een register op te zetten, met een generieke vragenlijst voor leveranciers. Zij hoeven de vragenlijst dan maar één keer in te vullen, en verzekeraars werken met dezelfde informatie.

“Dat addendum heb ik aangepast, de vragenlijst is opgesteld en dat heb ik naar iedereen gestuurd. Wat volgde? Doodse stilte.” Het initiatief bloedde dood en iedereen ging alsnog zelf het wiel uitvinden.

“De crux is vertrouwen”, concludeert Rundervoort. “Vaak is de houding toch: als een andere verzekeraar iets voor ons gezamenlijk maakt en ik daar ook op aangesproken kan worden, dan wil ik het toch controleren.”

Vinkjes halen

DORA is in eerste instantie een *license to operate*, wordt aan de rondetafel vastgesteld. Organisaties zijn bang dat zij onder toezicht komen te staan en er heerst angst over de bestuurlijke aansprakelijkheid. Met als gevolg dat organisaties vooral bezig zijn om te voldoen aan de DORA, zonder na te denken waarom bepaalde eisen worden gesteld, concluderen de aanwezigen. Daarmee ontstaat een soort schijnzekerheid.

John de Voogd van Klaverblad ziet dat ook. “We hebben zoveel focus op bewijsvoering dat alle energie daarheen gaat. Er dreigt minder energie te gaan naar de daadwerkelijke controle, waardoor juist daar risico kan ontstaan. Het blijft het allerbelangrijkst om te denken over waarom we dit eigenlijk doen?”

Intern leidt dat ook tot problemen. Iedereen binnen de organisatie, van de eerstelijn tot aan de derde lijn, wil wat vinden van de nieuw ingevoerde processen, regels en beleid. “Die zijn daar soms nog strakker op dan externe toezichthouders” concludeert Michiel van Dijk van VGZ. “Het wordt er niet soepeler en wendbaarder door. Iedereen wil er wat van vinden en er dingen aan toevoegen.”

Hoe verder?

Een samenwerking is mogelijk, maar werkt beter als er klein begonnen wordt. Twee partijen die samen optrekken, of één concreet project, zoals een gezamenlijk register. Een klein succes is makkelijker intern te rapporteren, en smaakt mogelijk naar meer. De aanwezigen voelen daar wel wat voor.



MeasureWorks:
Zorg dat je niet verrast wordt

Dat DORA soms als papieren tijger wordt gezien, herkent ook Marcel Schipper, Sales Director bij MeasureWorks. “We zien dat organisaties vooral bezig zijn met het afvinken van de eisen, terwijl de echte uitdaging ligt in het daadwerkelijk vergroten van de digitale weerbaarheid in de keten. DORA vraagt om operationele grip: weten wat er gebeurt en weten wat je moet doen als er iets misgaat.”

Veel organisaties werken met een groot aantal leveranciers, die op hun beurt weer afhankelijk zijn van andere partijen. Gaat er bij één van die schakels iets mis, dan heeft dat impact op de hele keten. Als verzekeraar wil je dan direct weten waar het probleem zit, zodat je snel kunt ingrijpen. “Digital operational resilience stopt niet bij je eigen IT-landschap, maar bij de afhankelijkheden daarbuiten,” aldus Schipper.

MeasureWorks pakt dit aan met observability: ketenmonitoring over alle schakels heen. “We analyseren de volledige keten, technisch, organisatorisch en operationeel. We kijken niet alleen naar systemen, maar ook naar processen en verantwoordelijkheden. Weet iedereen wat hij moet doen bij een incident? Wie reageert? Wat is de impact als iets uitvalt?“

Alleen met dit inzicht kun je snel reageren en verstoringen beperken. “Observability helpt organisaties niet alleen om aan DORA te voldoen, maar ook om aantoonbaar grip te krijgen op hun digitale keten. Diezelfde inzichten worden straks ook cruciaal onder de AI Act, waar transparantie en beheersbaarheid van systemen centraal staan.”

“DOOR JE KETEN INZICHTELIJK TE MAKEN EN CONTINU TE MONITOREN, BEN JE NIET ALLEEN COMPLIANT. JE VOORKOMT VOORAL DAT JE VERRAST WORDT.”

Klein clubje, grote les

ONVZ heeft de DORA-implementatie bewust kleinschalig aangepakt: een klein team, nauwe afstemming met de risicoafdeling en een externe partij die met frisse ogen meekeek. "Dat heeft heel veel vertrouwen gewekt, ook bij de Raad van Bestuur", zegt leveranciersmanager Jan-Dirk Rundervoort. De aanpak loonde: 92 van de 94 controls waren in Q4 2025 behaald.

Bij grotere organisaties ziet Rundervoort hoe het anders kan gaan. "DIE HEBBEN DERTIG MENSEN MET EEN MENING, DIE WILLEN ALLEMAAL HUN STOKPAARDJES ERIN HEBBEN. DAN WORDT HET OOK EEN STUK GROTER DAN HET HOEFT TE ZIJN."

Rundervoort heeft een duidelijke visie op wanneer samenwerken tussen verzekeraars wél werkt. Volgens hem zijn daarvoor twee dingen nodig. "Ten eerste een concrete case, niet iets abstracts. Daarnaast wil je één partij die het voortouw neemt. Met tien partijen bereik je doorgaans alleen consensus op hoofdlijnen", zegt Rundervoort. De concrete invulling vraagt dan om interne afstemming bij al die partijen, en dat vertraagt of blokkeert het proces.