FSMA
AUTORITEIT VOOR FINANCIËLE DIENSTEN EN MARKTEN

Mededeling

FSMA_2025_01 dd. 17-01-25

Een tweede survey van de FSMA toont aan dat financiële entiteiten nog inspanningen moeten leveren om te voldoen aan de verwachtingen van DORA

Toepassingsveld:

Financiële entiteiten die onderworpen zijn aan de Europese DORA-verordening

Samenvatting/Doelstelling:

De Autoriteit voor Financiële Diensten en Markten (FSMA) heeft in november 2024 een tweede survey georganiseerd om na te gaan in hoeverre financiële entiteiten voorbereid zijn op de inwerkingtreding van de Europese DORA-verordening op 17 januari 2025. De resultaten van de survey tonen aan dat vele financiële entiteiten op de goede weg zijn om te voldoen aan de doelstellingen zoals bepaald in de DORA verordening, maar niettemin nog belangrijke inspanningen zullen moeten leveren om helemaal conform te zijn met de DORA verordening.

De Autoriteit voor Financiële Diensten en Markten (FSMA) heeft in november 2024 een tweede survey georganiseerd om na te gaan in hoeverre financiële entiteiten voorbereid zijn op de inwerkingtreding van de Europese DORA-verordening (*"Digital Operational Resilience Act"*) op 17 januari 2025. De DORA verordening stelt ambitieuze doelstellingen vast op het vlak van digitale operationele weerbaarheid. Deze strekken ertoe de financiële entiteiten en hun cliënten te beschermen. De resultaten van de survey tonen aan dat vele financiële entiteiten op de goede weg zijn om te voldoen aan de doelstellingen zoals bepaald in de DORA verordening, maar niettemin nog belangrijke inspanningen zullen moeten leveren om helemaal conform te zijn met de DORA verordening. Gegeven de snel naderende inwerkingtreding zal dit voor veel entiteiten nog een belangrijke uitdaging betekenen. Door het vastgestelde lage deelnemingspercentage blijft het niveau van implementatie van DORA bij een belangrijk gedeelte van de aan DORA onderworpen entiteiten echter een blinde vlek.

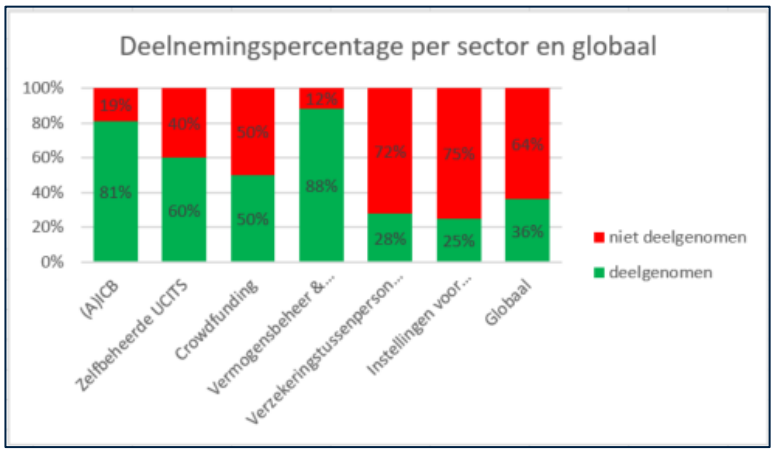
Na een eerste survey eind 2023, lanceerde de FSMA een tweede, uitgebreidere survey in oktober 2024 met als doel te peilen naar het implementatieniveau bij financiële entiteiten van de verschillende vereisten die bepaald worden in de DORA-verordening. Tegelijk hoopte de FSMA met deze survey een hulpmiddel aan te reiken aan de financiële entiteiten om een *gap analyse* uit te voeren tussen de vereisten van DORA en de actuele implementatie hiervan binnen de financiële entiteit. Zo kon deze survey dienen als een hulpmiddel om te identificeren welke vereisten op gebied van ICT-risicobeheer, incident management, digitale weerbaarheidstesten en beheer van derde partij aanbieders van ICT-diensten, nog georganiseerd, ontwikkeld en geïmplementeerd dienden te worden voor de definitieve inwerkingtreding van DORA op 17 januari 2025.

Deze niet-bindende survey van de FSMA, die berust op een zelfbeoordeling door de entiteiten werd gelanceerd tussen 21 oktober 2024 en sloot 6 weken nadien af, op 29 november 2024. Uiteindelijke bleken 93 van de geviseerde entiteiten te hebben geantwoord. Dit betekent een algemeen deelnemingspercentage van 36%. Het is zorgwekkend vast te stellen dat het globale deelnemingspercentage 14 procentpunten lager ligt dan bij de eerste survey die de FSMA in 2023 georganiseerd heeft. Dit kan een indicatie zijn dat de voorbereidingen voor de inwerkintreding van DORA bij vele financiële entiteiten niet vlot genoeg verlopen. Indien zo, worden financiële entiteiten dringend verzocht om alsnog het nodige te doen om te conformeren met de voor hen geldende bepalingen van de Verordening.

Het deelnemingspercentage is globaal afgenomen in vergelijking met de eerste survey

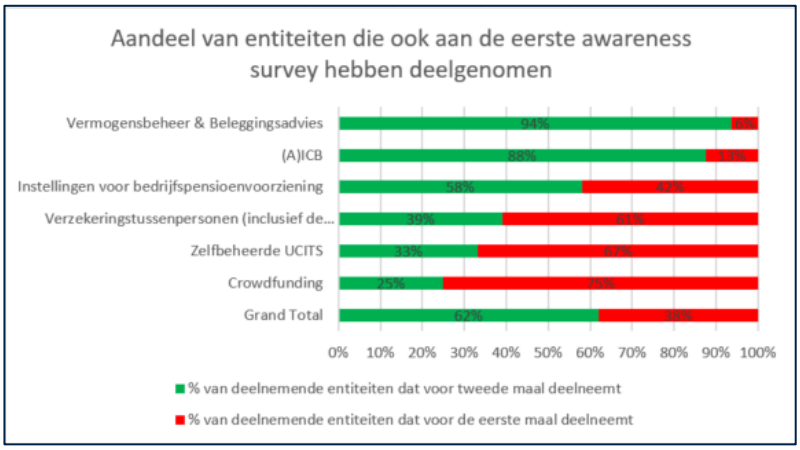
Uit de analyse van het deelnemingspercentage blijkt dat 60% van de Zelfbeheerde UCITS en 50% van de Crowdfundingdienstverleners heeft deelgenomen, terwijl deze bij de vorige survey in 2023 nog de grote afwezigen waren. Dit stemt de FSMA positief, net als het grotere deelnemingspercentage bij de verzekeringstussenpersonen (inclusief de nevenverzekeringstussenpersonen) en herverzekeringstussenpersonen (28% tgo. 19%). De FSMA verheugt zich eveneens over het nog steeds hoge deelnemingspercentage bij de vennootschappen voor vermogensbeheer en beleggingsadvies (88% tgo. 94% bij de eerste survey) en bij de beheerders van (A)ICB's (81% tgo. 88% bij de eerste survey).

Niettegenstaande deze positieve tendensen blijft het deelnemingspercentage bij de verzekeringstussenpersonen (inclusief de nevenverzekeringstussenpersonen) en herverzekeringstussenpersonen opmerkelijk laag. Ook de significante daling in de deelnemingsgraad bij Instellingen voor bedrijfspensioenvoorziening (25% terwijl dit bij de eerste survey nog 57% was) is opmerkelijk.



Figuur 1: Deelnemingspercentage per sector en globaal

Verdere analyse toonde aan dat 62% van de deelnemers aan deze tweede survey ook al hadden deelgenomen aan de eerste. De populaties bij de sectoren Vermogensbeheer & Beleggingsadvies en de (A)ICB bleven nagenoeg gelijk terwijl het percentage financiële entiteiten voor de overige sectoren significant gewijzigd is ten opzichte van de eerste survey.



Figuur 2: aandeel entiteiten die al dan niet aan beide surveys hebben deelgenomen

Gegeven deze vastgestelde verschillen in populatie, zowel qua grootte als type deelnemers, tussen de eerste en tweede survey was het voor de FSMA moeilijk om correcte vergelijkingen te maken in haar analyse van de resultaten. Wanneer dit toch gedaan werd, dient dus steeds het verschil in populatie in acht genomen te worden.

Het volwassenheidsniveau zoals ingeschat door de deelnemende entiteiten per thema van DORA gaat globaal genomen vooruit, met uitzondering van het Beheer van het ICT-risico van derde aanbieders

Net zoals bij de eerste survey werden financiële entiteiten verzocht om, op een schaal van 1 (laag) tot 5 (zeer hoog), hun 'volwassenheidsniveau' (of maturiteitsniveau) te beoordelen ten aanzien van de vier grote DORA-thema's die in de survey aan bod kwamen. Algemeen beschouwd lijkt het maturiteitsniveau in meer (*ICT-risicobeheer*) of mindere (*beheer, classificatie en rapportage van ICT-gerelateerde incidenten* en *testen van digitale operationele weerbaarheid*) mate te stijgen. Het thema *beheer van ICT-risico van derde aanbieder* is echter een uitzondering aangezien hier een daling van maturiteitsniveau vastgesteld wordt. Een reden kon hiervoor niet aangeduid worden. Mogelijk is deze evolutie te wijten aan het eerder aangehaalde verschil in populatie tussen de eerste en tweede survey.

In figuur 3 kunnen de tendensen globaal en per sector geconsulteerd worden.

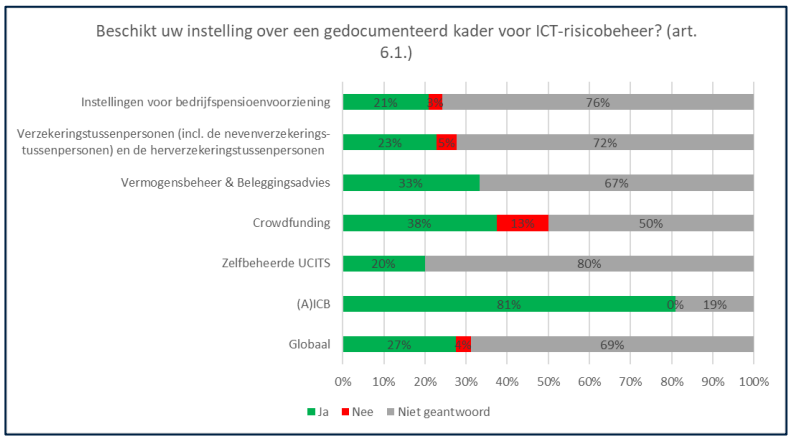
	ICT-Risicobeheer		Beheer, classificatie en rapportage van ICT-gerelateerde incidenten		Testen van digitale operationele weerbaarhei		Beheer van ICT-risico van derde aanbieder	
	2023	2024	2023	2024	2023	2024	2023	2024
(A)ICB	3,09	3,24	3,18	3,24	2,25	2,35	2,9	2,82
Vermogensbeheer & Beleggingsadvies	2,56	4	2,13	2,53	1,9	2,6	2,94	2,93
Crowdfundingplatformen	na	2,75	na	2,25	na	2,25	na	1,75
Instellingen voor bedrijfspensioen-voorziening	2,42	2,27	2,26	2,2	2,2	2,07	2,72	2,13
Verzekeringstussen-personen en herverzekerings-tussenpersonen	3,86	3,35	3,79	3,3	2,5	3,19	3,23	2,7
Zelfbeheerde UCITS	na	3	na	3	na	3	na	3
Globaal	2,67	2,87	2,49	2,74	2,38	2,5	2,766	2,53

Figuur 3: gemiddelde maturiteitsniveau globaal en per sector zoals aangegeven door de deelnemers (vergelijking 2023 en 2024

Alhoewel het deelnemingspercentage lager is, is de vastgestelde vooruitgang bij de deelnemende entiteiten eerder bemoedigend. Zij moeten zich echter onverminderd blijven inspannen om klaar te geraken voor DORA.

Net zoals bij de eerste survey werden de antwoorden op deze tweede survey geformuleerd na zelfevaluatie. De betrokken entiteiten werden niet gevraagd om hun verklaringen te onderbouwen met nadere toelichtingen of met documenten. De survey, waaraan de deelname vrijwillig was, is onderverdeeld in vier secties, die elk overeenstemmen met een van de thema's die in de DORA-verordening worden behandeld. In vergelijking met de eerste survey werden de vragen gesteld op een veel gedetailleerder niveau. Dit zorgde voor een veel uitgebreidere survey en stelde de FSMA en de deelnemende entiteiten in staat om de implementatie per artikel van DORA te onderzoeken en te beoordelen.

De meeste financiële entiteiten verklaren te beschikken over een ICT-risicobeheerkader, en meer bepaald over een ICT-bedrijfscontinuïteitsbeleid



Figuur 4: aandeel entiteiten met een goed gedocumenteerd kader voor ICT-risicobeheer

In elke sector verklaart de overgrote meerderheid van de respondenten die niet onder het vereenvoudigde regime vallen te beschikken over een **ICT-risicobeheerkader** dat gedocumenteerd is.

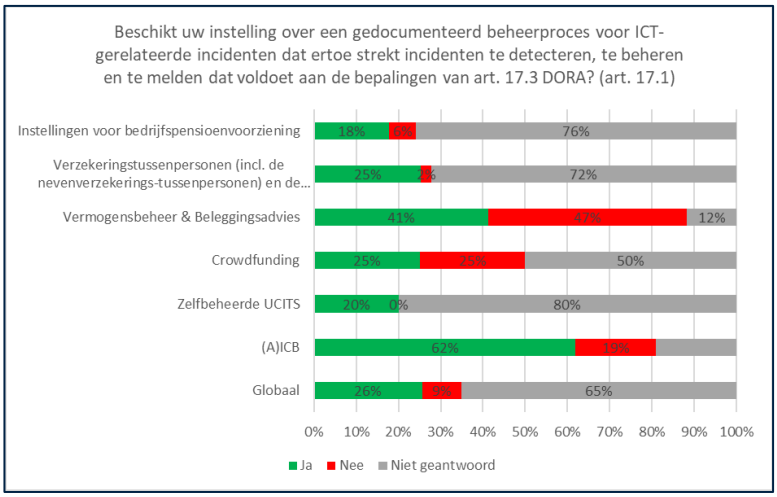
In vergelijking met de survey van 2023 is het percentage van entiteiten dat zegt hierover te beschikken ook significant toegenomen.

Dankzij de gedetailleerdere vraagstelling in deze tweede survey, is de FSMA ook kunnen nagaan of dit gedocumenteerd kader alle elementen bevat zoals opgenomen in art. 6.2 van de Verordening. Uit de resultaten blijkt dat het antwoord hierop minder positief is. Zo geeft globaal ongeveer 1 op 3 van de entiteiten aan dat dit kader niet alle elementen bevat. Hoewel dit geen bemoedigend resultaat betreft, stemt het wel positief dat hieruit blijkt dat deze entiteiten de beoordeling gemaakt hebben en dus ook weten welke punten nog extra aandacht verdienen.

Alle sectoren samen beschouwd, heeft meer dan 90% van de respondenten bevestigd over een **ICT-bedrijfscontinuïteitsbeleid** te beschikken, dat ook van toepassing is op kritieke ICT-functies die uitbesteedt zijn. Hoewel een lichte verbetering kan vastgesteld worden in vergelijking met de eerste survey, is deze echter weinig significant. Desalniettemin blijft het percentage positieve antwoorden ook bij deze tweede survey hoopgevend.

Minder hoopgevend is dat ongeveer 40% van de deelnemende entiteiten heeft aangegeven dat dit bedrijfscontinuïteitsplan niet voldoet aan de doelstellingen zoals opgenomen in artikel 11.2 van de Verordening. Dit artikel bepaalt onder meer dat het ICT-bedrijfscontinuïteitsplan uitgevoerd moet worden via specifieke, aangepaste en gedocumenteerde regelingen, plannen, procedures en mechanismen die er onder meer op gericht zijn de continuïteit van kritische en belangrijke functies te verzekeren, snel, passend en doeltreffend te reageren en oplossingen te bieden en de schade te beperken. Het feit dat slechts een kleine meerderheid aangeeft dat deze bepaling wordt nageleefd, doet vermoeden dat vele entiteiten nog inspanningen zullen moeten leveren om het aanwezige en gedocumenteerde bedrijfscontinuïteitsbeleid performanter en conform aan de verwachtingen van DORA te maken.

De financiële entiteiten moeten hun reactievermogen bij ICT-incidenten verbeteren



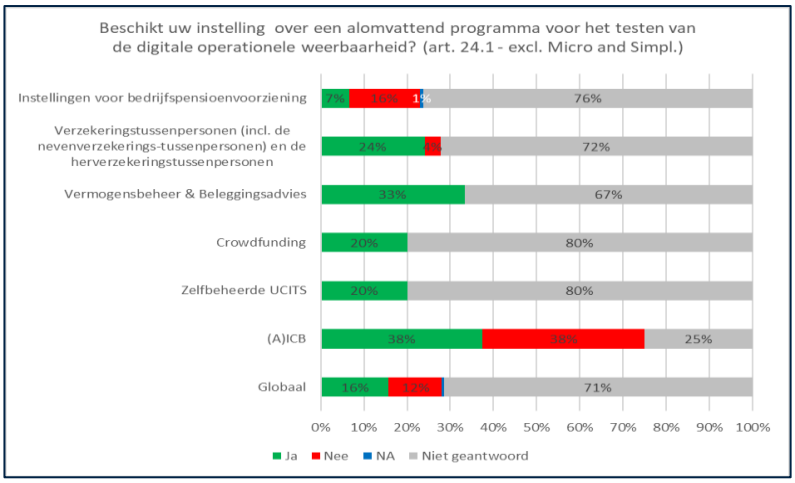
Figuur 5: beheersproces ICT-gerelateerde incidenten

Hoewel de meeste financiële entiteiten over een ICT-risicobeheerkader beschikken, geeft een kleinere groep aan in staat te zijn ICT-gerelateerde incidenten ook effectief te detecteren, beheren en, zo

nodig, te melden. De resultaten van deze tweede survey zijn erg vergelijkbaar met de resultaten van de eerste survey, in die zin dat er weinig positieve evolutie kan vastgesteld worden.

De FSMA wenst dus nogmaals te benadrukken dat dit reactievermogen en het beheer van ICT-gerelateerde incidenten een intrinsiek onderdeel betreft van de operationele weerbaarheid van financiële entiteiten tegen cyberdreigingen. Om de impact van die incidenten te beperken, alsook de kosten die ze veroorzaken aan banden te leggen en hun verdere verspreiding naar cliënten en andere financiële entiteiten te verhinderen, is het van cruciaal belang dat de entiteiten hun reactievermogen op dit vlak verder blijven aanscherpen.

ICT-risicobeheer en –beleidskaders uitwerken heeft enkel zin als deze ook aan de praktijk worden getoetst



Figuur 6: aandeel entiteiten met programma voor het testen van digitale operationele weerbaarheid

Noch het invoeren van een ICT-risicobeheerkader, noch het uitwerken van beleidslijnen en procedures ter zake volstaan op zich om de digitale operationele weerbaarheid van een financiële entiteit te waarborgen. Het is essentieel om de kwetsbaarheden en de ICT-risico's in kaart te brengen zodat doelmatige en doeltreffende maatregelen kunnen worden genomen.
Welnu, een substantieel deel van de deelnemende ondernemingen (ongeveer 43%) beschikken nog niet over een volledig programma voor het testen van de digitale operationele weerbaarheid. Dit is een verbetering in vergelijking met de vorige survey, maar blijft nog steeds een bijzonder laag percentage. In de bovenstaande berekening werden doelbewust de micro-ondernemingen en entiteiten die onder het vereenvoudigde kader weggelaten aangezien deze respectievelijk een proportioneel of geen testprogramma dienen te hebben.

Verder valt op dat in bepaalde sectoren alle deelnemende entiteiten hebben aangegeven over zo'n testprogramma te beschikken. Zowel voor de sector Vermogensbeheer & Beleggingsadvies als zelfbeheerd UCITS en Crowdfundingplatformen blijkt de volledige populatie over zo'n testprogramma te beschikken. . Enige nuance is hierbij wel op z'n plaats aangezien de meerderheid van de entiteiten onder Vermogensbeheer & Beleggingsadvies niet opgenomen werden in bovenstaande grafiek aangezien zij enkel dienen te voldoen aan het vereenvoudigde kader voor ICT-risicobeheer. Het absolute aantal entiteiten uit de twee overige sectoren ligt trouwens zeer laag.

Daarentegen is het wel heel opmerkelijk dat de grote meerderheid (84%) van de deelnemende verzekeringstussenpersonen (inclusief de nevenverzekeringstussenpersonen) en herverzekeringstussenpersonen aangeeft eveneens over zo'n plan te beschikken. Het moet evenwel in herinnering gebracht worden dat het deelnemingspercentage voor deze laatste sector zeer laag is.

De FSMA heeft daarnaast ook nagekeken welk percentage van deelnemende entiteiten welke tests uitvoert. Het resultaat van deze analyse kan geconsulteerd worden in onderstaande tabel. Ook hier valt het op dat de grote meerderheid van de deelnemende verzekeringstussenpersonen (inclusief de nevenverzekeringstussenpersonen) en herverzekeringstussenpersonen aangeeft dat zij bijna alle tests uitvoeren.

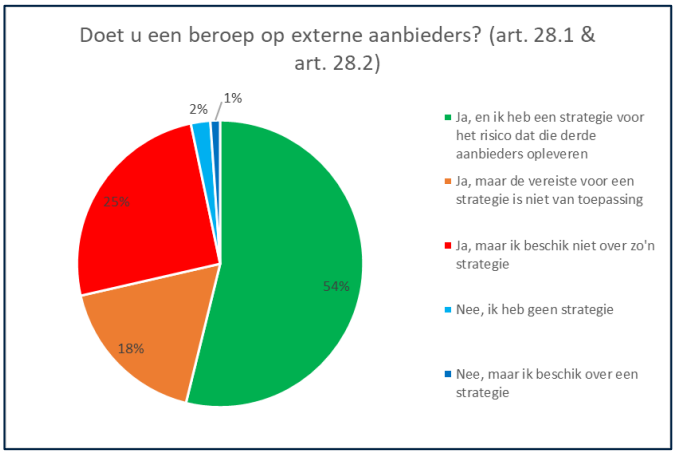
Sector	1.vulnera-bility_scan	2.open_source _analyses	3.source_ code	4.network _security	5.gap_ana-lyses	6.physical _security	7.detec-tietools	8.scenario	9.compa-tibiliteit	10.perfor-mance	11.end-2-end	12.pene-tratie	13.TLPT
(A)ICB	35%	18%	12%	29%	29%	35%	35%	24%	18%	12%	18%	29%	6%
Crowdfunding	25%	25%	25%	0%	0%	0%	0%	25%	0%	25%	0%	25%	0%
Instellingen voor bedrijfspensioenvoorziening	23%	19%	23%	26%	16%	16%	19%	19%	23%	23%	19%	19%	3%
Vermogensbeheer & Beleggingsadvies	40%	13%	7%	40%	33%	27%	40%	7%	20%	13%	7%	40%	13%
Verzekeringstussenpersonen (inclusief de nevenverzekerings-tussenpersonen) en de herverzekeringstussenpersonen	87%	48%	78%	78%	70%	83%	74%	74%	70%	78%	70%	78%	43%
Zelfbeheerde UCITS	100%	0%	0%	0%	100%	0%	0%	0%	0%	0%	0%	100%	0%
total	45%	25%	32%	41%	35%	37%	38%	32%	32%	33%	29%	41%	15%

Figuur 7: aandeel entiteiten dat specifieke testen uitvoert

De ondernemingen moeten het beheer verbeteren van het risico dat verbonden is aan externe aanbieders van ICT-diensten

97% van de respondenten geeft aan een beroep te doen op externe aanbieders van ICT-diensten. Van die groep verklaart 43% evenwel geen strategie te hebben voor het risico dat die aanbieders opleveren. Iets minder dan de helft van de entiteiten zonder strategie (42%) geeft echter terecht aan dat het hebben van zo'n strategie volgens de vereisten van de verordening niet op hen van toepassing is.

Dit betekent echter dat nog steeds ongeveer 1 op 3 van alle deelnemende entiteiten die wel onderworpen zijn aan deze bepaling in de Verordening aangeeft geen strategie ontwikkeld te hebben voor het het beheer van het risico van derde aanbieders, terwijl dit wel verwacht wordt. Aangezien een onderneming in elk geval volledig aansprakelijk blijft voor de naleving van de Verordening, is het van essentieel belang dat ze ook een strategie ontwikkelt die het beheer van deze risico's ondersteunt. Entiteiten die dit nog niet zouden gedaan hebben, worden dus aangeraden snel het nodige hiervoor doen.



Figuur 8: aandeel entiteiten dat beroep doet op externe aanbieders en hiervoor al dan niet over een strategie beschikt

Vandaag is DORA er echt!

Uit voorgaande resultaten blijkt dat veel entiteiten die hebben deelgenomen aan deze survey nog belangrijke stappen zullen moeten zetten om in overeenstemming te zijn met de vereisten die in de DORA verordening werden bepaald.

Het is bovendien jammer vast te stellen dat minder financiële entiteiten aan deze survey hebben deelgenomen in vergelijking met de eerste survey. Bovendien ligt het aandeel van entiteiten dat heeft deelgenomen voor sommige sectoren laag tot zeer laag. Het gevolg is dat er voor de FSMA een grote blinde vlek blijft wat betreft de graad van implementatie bij de entiteiten die niet hebben deelgenomen.

De FSMA hoopt desalniettemin dat alle betrokken financiële entiteiten de resterende tijd tussen het sluiten van deze survey en de inwerkingtreding van de Verordening goed gebruikt hebben om zich alsnog adequaat en voldoende voor te bereiden.

De FSMA zal zich deels baseren op deze eerste vaststellingen om richting te geven aan haar toekomstige superviserende acties. In de toekomst zal de FSMA overige verplichte surveys kunnen verrichten waarbij entiteiten kunnen gevraagd worden hun antwoorden te onderbouwen of bewijzen met extra documentatie. Op die manier zal de FSMA nauwgezetter kunnen beoordelen of de entiteiten voldoen aan de vereisten van de DORA-verordening. Ook die initiatieven zullen erop gericht zijn de digitale operationele weerbaarheid van de financiële marktdeelnemers te meten en blijvend te versterken.

Rekening houdende met de beperkingen van deze survey en de vaststellingen die hieruit getrokken kunnen worden, verzoekt de FSMA de financiële entiteiten om de implementatie van DORA als prioriteit te behandelen in 2025, en hierbij een nadruk te leggen op de volgende aspecten:

- Het blijvend vergroten van de maturiteit in het risicobeheer en meer specifiek het in lijn brengen van een bedrijfscontinuïteitsplan met art. 11.2 van DORA,
- Een adequaat en effectief beheer van ICT-gerelateerde incidenten ontwikkelen,
- De risico's die verbonden zijn aan het gebruik van externe aanbieders van ICT-diensten kunnen inschatten en beheren.