Raad van de
Europese Unie

Brussel, 24 september 2020
(OR. en)

Interinstitutioneel dossier:
2020/0268(COD)

11052/20
ADD 2

EF 229
ECOFIN 847
TELECOM 160
CYBER 169
IA 62
CODEC 872

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	SWD(2020) 204 final
Betreft:	WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG bij voorstel voor een Richtlijn van het Europees Parlement en de Raad tot wijziging van de Richtlijnen 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 en EU/2016/2341

Hierbij gaat voor de delegaties document SWD(2020) 204 final.

Bijlage: SWD(2020) 204 final

EUROPESE
COMMISSIE

Brussel, 24.9.2020
SWD(2020) 204 final

This document corrects document SWD(2020) 204 final of 24.09.2020
Two references in the title of the cover page have been corrected.
Concerns the EN version only.
The text shall read as follows:

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG

bij

Voorstel voor een Richtlijn van het Europees Parlement en de Raad

tot wijziging van de Richtlijnen 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 en EU/2016/2341

{COM(2020) 596 final} - {SEC(2020) 309 final} - {SWD(2020) 203 final}

Samenvatting

Effectbeoordeling van het voorstel voor een verordening betreffende digitale operationele veerkracht in de financiële sector

A. Behoefte aan actie

Waarom? Wat is het probleem?

De financiële sector is in grote mate afhankelijk van informatie- en communicatietechnologieën (ICT). De huidige COVID-19-pandemie zal deze afhankelijkheid waarschijnlijk nog vergroten, gezien de voordelen van permanente toegang op afstand tot financiële diensten. Afhankelijkheid van digitale technologieën geeft echter aanleiding tot bezorgdheid; ondernemingen moeten in staat zijn potentiële ICT-verstoringen te weerstaan, d.w.z. dat digitale incidenten en bedreigingen worden aangepakt en de dienstverlening gehandhaafd blijft. In een sterk verweven financiële sector die cruciale grensoverschrijdende diensten aanbiedt waarvan de reële economie afhankelijk is, zijn de kwetsbaarheden als gevolg van ICT-afhankelijkheid – waarmee alle economische sectoren te maken hebben – bijzonder uitgesproken vanwege 1) het intensieve en grootschalige gebruik van ICT en 2) de kans dat de effecten van een operationeel incident bij één financiële onderneming of financiële subsector zich snel verspreiden naar andere ondernemingen of delen van de financiële sector, en uiteindelijk naar de rest van de economie.

Hoewel de financiële sector qua markt- en regelgevingsintegratie ver gevorderd is en wel vaart bij één set geharmoniseerde regels – het gemeenschappelijke rulebook van de EU – is de EU-respons op de toegenomen behoefte aan operationele veerkracht op horizontaal en sectoraal niveau tot dusver:

- ofwel gebaseerd op minimale harmonisatie, waardoor ruimte wordt gelaten voor nationale interpretatie en versnippering van de eengemaakte markt;
- ofwel te algemeen en van beperkte toepassing, waarbij het algehele operationele risico in verschillende mate wordt aangepakt en sommige onderdelen van digitale operationele veerkracht (bv. ICT-risicobeheer, incidentrapportage en ICT-derdenrisico) gedeeltelijk worden gereguleerd, terwijl andere onderdelen (tests) buiten beschouwing worden gelaten.

Het EU-optreden heeft operationeel risico tot dusver niet aangepakt op een wijze die strookt met de behoeften van financiële ondernemingen om ICT-kwetsbaarheden te weerstaan, tegen te gaan en te boven te komen. Aan financiële toezichthouders zijn evenmin de instrumenten geboden om zich te kwijten van hun taak om de uit die ICT-kwetsbaarheden voortvloeiende financiële instabiliteit te beperken.

De huidige leemten en inconsistenties hebben geleid tot een veelheid aan ongecoördineerde nationale initiatieven (bv. inzake tests) en toezichtbenaderingen (bv. inzake ICT-afhankelijkheid van derden), wat overlappingen, dubbele vereisten en hoge administratieve en nalevingskosten voor grensoverschrijdende financiële ondernemingen meebrengt, of ertoe leidt dat ICT-risico's onontdekt blijven en niet worden aangepakt. Over het geheel genomen zijn de stabiliteit en integriteit van de financiële sector niet gewaarborgd en blijft de eengemaakte markt voor financiële diensten versnipperd, met als gevolg dat de bescherming van consumenten en beleggers wordt verzwakt.

Wat moet met dit initiatief worden bereikt?

De algemene doelstelling is het versterken van de digitale operationele veerkracht van de financiële sector van de EU door de bestaande financiële wetgeving van de EU te stroomlijnen en te verbeteren en nieuwe vereisten in te voeren waar leemten bestaan, teneinde:

- het beheer van ICT-risico's door financiële ondernemingen te verbeteren;
- de kennis van toezichthouders over dreigingen en incidenten te vergroten;
- het testen van hun ICT-systemen door financiële ondernemingen te verbeteren; en
- beter toezicht te houden op de risico's die verbonden zijn aan het feit dat financiële ondernemingen afhankelijk zijn van derde aanbieders van ICT-diensten.

Meer in het bijzonder zou het voorstel zorgen voor een coherenter en consistenter mechanisme voor het melden van incidenten en zo de administratieve lasten voor financiële instellingen verlichten en de doelmatigheid van het toezicht versterken.

Wat is de meerwaarde van maatregelen op EU-niveau?

De eengemaakte markt voor financiële diensten van de EU is onderworpen aan een groot geheel van op EU-niveau vastgestelde regels, dat financiële ondernemingen met een vergunning uit een lidstaat in staat stelt in de hele eengemaakte markt diensten aan te bieden dankzij hun EU-paspoort. Bijgevolg zouden regels op nationaal niveau geen doeltreffende manier zijn om de operationele veerkracht te versterken van financiële ondernemingen die gebruikmaken van het paspoort. Voorts bevat het gemeenschappelijke rulebook als gevolg van de financiële crisis zeer gedetailleerde voorschriften voor het aanpakken van meer "traditionele" risico's als krediet-, markt-, tegenpartij- en liquiditeitsrisico's. De bestaande bepalingen inzake operationeel risico blijven

algemeen. Voor de versterking van de digitale operationele veerkracht zijn aanpassingen nodig in de bepalingen inzake operationeel risico die al op EU-niveau zijn vastgesteld en die dus alleen op EU-niveau kunnen worden verbeterd en aangevuld.

B. Oplossingen

Welke wetgevende en niet-wetgevende beleidsmaatregelen zijn overwogen? Heeft een bepaalde optie de voorkeur? Waarom?

In het kader van de effectbeoordeling zijn drie opties onderzocht, naast een basisscenario waarin geen actie wordt ondernomen met betrekking tot de EU-wetgeving inzake financiële diensten. Meer bepaald:

- **"Niets doen"**: de regels inzake operationele veerkracht zouden nog steeds worden vastgesteld door de huidige uiteenlopende reeks bepalingen inzake financiële diensten, gedeeltelijk door de NIS-richtlijn, en door bestaande of toekomstige nationale regelingen;
- **Optie 1 – versterking van de kapitaalbuffers**: er zou een extra kapitaalbuffer worden ingevoerd om financiële ondernemingen beter in staat te stellen verliezen op te vangen die zouden kunnen ontstaan als gevolg van een gebrek aan operationele veerkracht;
- **Optie 2 – een wetgevingshandeling inzake digitale operationele veerkracht**: er zou een alomvattend kader op EU-niveau worden ingevoerd met regels inzake digitale operationele veerkracht voor alle gereglementeerde financiële instellingen, teneinde
    - ICT-risico's grondiger aan te pakken;
    - financiële toezichthouders toegang te geven tot informatie over ICT-gerelateerde incidenten;
    - ervoor te zorgen dat financiële ondernemingen de doeltreffendheid van hun preventie- en veerkrachtmaatregelen beoordelen en ICT-kwetsbaarheden identificeren;
    - de uitbestedingsregels voor indirect toezicht op derde aanbieders van ICT-diensten aan te scherpen;
    - direct toezicht mogelijk te maken op de activiteiten van derde aanbieders van ICT-diensten wanneer zij hun diensten aan financiële ondernemingen verlenen; en
    - daarnaast ook de uitwisseling van inlichtingen over dreigingen in de financiële sector aan te moedigen.
- **Optie 3 – een wetgevingshandeling inzake veerkracht in combinatie met gecentraliseerd toezicht op cruciale derde aanbieders van diensten**: naast een wetgevingshandeling inzake operationele veerkracht (optie 2) zou een nieuwe autoriteit worden opgericht om toezicht te houden op derde aanbieders van cruciale ICT-diensten aan financiële ondernemingen. Bij deze optie zou de financiële sector eveneens duidelijker worden afgebakend van het toepassingsgebied van de NIS-richtlijn.

De voorkeur gaat uit naar optie 2. In vergelijking met de andere opties bereikt optie 2 de meeste doelstellingen van het initiatief, terwijl ook wordt voldaan aan de criteria van efficiëntie en samenhang. Deze optie krijgt ook de meeste steun van belanghebbenden.

Wie steunt welke optie?

De meeste belanghebbenden uit de particuliere en de overheidssector zijn het erover eens dat EU-optreden nodig is om de operationele veerkracht van financiële ondernemingen beter te beschermen. Velen zijn ook van mening dat EU-optreden nodig is om de regeldruk aan te pakken die voortvloeit uit het feit dat financiële ondernemingen zijn onderworpen aan dubbele en inconsistente regels in de NIS-richtlijn, de EU-wetgeving inzake financiële diensten en nationale regelingen (bv. inzake incidentrapportage). Er zijn dan ook maar weinig belanghebbenden voorstander van niets doen. Waarborging van de operationele veerkracht door middel van verhoogde kapitaalbuffers (optie 1) kan evenmin op veel steun onder belanghebbenden rekenen. Toch is dit de traditionele benadering van operationeel risico, met name in het bankwezen, en als zodanig wordt deze optie overwogen door bijvoorbeeld internationale normerende instellingen. Kwalitatieve maatregelen zoals beschreven in optie 2 die de financiële wetgeving van de EU zouden stroomlijnen en verbeteren en nieuwe vereisten zouden invoeren waar leemten bestaan, en die tegelijkertijd de banden met de horizontale NIS-richtlijn zouden behouden, genieten brede steun van de belanghebbenden die op de openbare raadpleging hebben gereageerd. Hoewel sommige belanghebbenden (met name uit de overheidssector) het versterkte toezicht op derde aanbieders van ICT-diensten van optie 3 zinvol achten, krijgt de oprichting van een nieuwe EU-autoriteit voor dat doel slechts beperkte steun van belanghebbenden, wat ook geldt voor een volledigere breuk met het NIS-kader.

C. Effecten van de voorkeursoptie

Wat zijn de voordelen van de voorkeursoptie (als er een voorkeursoptie is; zo niet, wat zijn de voordelen van de belangrijkste opties)?

Optie 2 zou de **ICT-risico's** in de hele financiële sector aanpakken door financiële instellingen beter in staat te

stellen om ICT-incidenten te weerstaan. Dit zou het risico verminderen dat een cyberincident zich snel over de financiële markten verspreidt. Hoewel het moeilijk is de kosten van operationele incidenten in de financiële sector in te schatten (niet alle incidenten worden gemeld; de omvang van de kosten is onzeker), blijkt uit beoordelingen van de sector dat de kosten voor de financiële sector van de EU kunnen variëren van 2 tot 27 miljard EUR per jaar. De voorkeursoptie zou deze directe kosten en de eventuele bredere gevolgen van grote cyberincidenten voor de financiële stabiliteit beperken. Door een einde te maken aan overlappende **rapportagevereisten**, zouden de administratieve lasten worden verminderd. Sommige van de grootste banken zouden op dit gebied bijvoorbeeld 40 tot 100 miljoen EUR per jaar kunnen besparen. Directe rapportage zou ook de kennis van de toezichthouders over ICT-incidenten vergroten. **Geharmoniseerde testpraktijken** zouden de opsporing van onbekende kwetsbaarheden en risico's verbeteren. Ook zouden hierdoor de kosten worden teruggedrongen, vooral voor grensoverschrijdende ondernemingen. Voor de 44 grootste grensoverschrijdende banken zouden de totale verwachte baten van een gemeenschappelijke testaanpak bijvoorbeeld kunnen variëren van 11 tot 88 miljoen EUR. Indien een coherent geheel van regels wordt ingevoerd voor het beheer van de risico's van **derde aanbieders van ICT-diensten**, zouden financiële ondernemingen meer controle hebben over de wijze waarop derde aanbieders het regelgevingskader naleven, wat de toezichthouders zou kunnen helpen. Toezicht op derde aanbieders van ICT-diensten door toezichthouders zou ook prudentiële voordelen hebben. Al met al heeft de voorkeursoptie bredere maatschappelijke voordelen als gevolg van een veerkrachtiger bedrijfsomgeving voor alle financiëlemarktdeelnemers en een sterkere bescherming voor consumenten en beleggers.

Wat zijn de kosten van de voorkeursoptie (als er een voorkeursoptie is; zo niet, wat zijn de voordelen van de belangrijkste opties)?

De voorkeursoptie zou eenmalige en vaste kosten meebrengen. De eenmalige kosten houden verband met investeringen in IT-systemen en zijn moeilijk te kwantificeren gezien de uiteenlopende staat van de oude IT-systemen van ondernemingen. Ook zonder regelgevende maatregelen hebben sommige ondernemingen al aanzienlijke investeringen in ICT-systemen gedaan. Voor grote financiële ondernemingen zal de uitvoering van de maatregelen van dit voorstel waarschijnlijk weinig extra kosten meebrengen.. Ook voor kleinere ondernemingen zullen de kosten naar verwachting lager zijn, aangezien voor hen minder strenge maatregelen zouden gelden die in verhouding staan tot hun lagere risico. Wat tests betreft, hebben de Europese toezichthoudende autoriteiten de kosten van dreigingsgestuurde penetratietests geraamd op 0,1 tot 0,3 % van de totale ICT-begroting van de betrokken ondernemingen. De kosten in verband met het melden van incidenten zouden drastisch worden verminderd, aangezien er geen overlappingen met de NIS-rapportage zouden zijn. De toezichthouders zullen ook bepaalde kosten moeten maken als gevolg van de extra taken die zij op zich zouden nemen. Voor toezichthouders die betrokken zijn bij direct toezicht op derde aanbieders van ICT-diensten, wordt de toename in vte geraamd op 1 tot 5 vte voor de leidende toezichthouder en ongeveer 0,25 vte voor de deelnemende autoriteiten.

Wat zijn de gevolgen voor bedrijven, waaronder kleine en middelgrote bedrijven en micro-ondernemingen?

De voorkeursoptie zou voor alle financiële ondernemingen gelden om de operationele veerkracht van de sector als geheel te vergroten. Dit brede toepassingsgebied is belangrijk gezien de onderlinge verwevenheid van de financiële sector en de bijbehorende behoefte aan een solide operationele veerkracht in het algemeen. Bij het vaststellen van de kernvereisten voor de belangrijkste actiegebieden zou het evenredigheidsbeginsel echter zowel voor alle subsectoren als binnen elke subsector van toepassing zijn. Hierbij zou rekening worden gehouden met verschillen in bedrijfsmodel, grootte, risicoprofiel, systeemrelevantie, enz. Maatregelen inzake incidentrapportage en tests zouden bijvoorbeeld minder streng zijn voor kleinere financiële ondernemingen.

Zijn er significante gevolgen voor de nationale begrotingen en overheden?

Nee. Met het extra toezicht kunnen, zoals hierboven is vermeld, in beperkte mate aanvullende middelen gemoeid zijn, die geheel of gedeeltelijk (bij toezichtvergoedingen) uit overheidsbegrotingen zullen worden betaald.

Zijn er andere significante gevolgen?

De sociaal-economische gevolgen van de COVID-19-pandemie illustreren het cruciale belang van de digitale financiële markten en hun operationele veerkracht. De voorkeursoptie zou een solide basis leggen voor het benutten van de digitale transformatie, door ervoor te zorgen dat de eengemaakte markt voor financiële diensten, inclusief de bankenunie en de kapitaalmarktenunie, operationeel veerkrachtig is en berust op een gemeenschappelijke reeks regels en vereisten die veiligheid, prestaties, stabiliteit en een gelijk speelveld nastreven. Dit zal ook de positie van Europa als financiële en digitale wereldleider versterken, een doelstelling die de Commissie heeft geformuleerd in haar mededeling "De digitale toekomst van Europa vormgeven".

D. Evaluatie
Wanneer wordt het beleid geëvalueerd?
De eerste evaluatie wordt drie jaar na de inwerkingtreding van het wettelijke instrument verricht. De Commissie zou over haar evaluatie verslag uitbrengen aan het Europees Parlement en de Raad. De evaluatie kan zo nodig worden ondersteund door een openbare raadpleging, studies, discussies met deskundigen, enquêtes en workshops.