EUROPA-
KOMMISSIONEN

Bruxelles, den 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:

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF RAPPORTEN OM KONSEKVENSANALYSEN

Ledsagedokument til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om ændring af direktiv 2006/43/EF, 2009/65/EF, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341

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

Resumé

Konsekvensanalyse af forslaget til forordning om digital operationel modstandsdygtighed i den finansielle sektor

A. Behov for handling

Hvorfor? Hvad er problemstillingen?

Den finansielle sektor er i høj grad afhængig af informations og kommunikationsteknologier (IKT). Den nuværende covid-19-pandemi vil sandsynligvis øge denne afhængighed i betragtning af de fordele, det giver at sikre løbende fjernadgang til finansielle tjenesteydelser. Afhængighed af digitale teknologier indebærer dog problemstillinger: Virksomheder skal være i stand til modstå potentielle IKT-forstyrrelser, således at digitale hændelser og trusler imødegås og tjenester opretholdes. Til trods for at dette gælder for alle økonomiske sektorer, er svagheder på grund af IKT-afhængighed særligt udprægede i en finansiel sektor med stor indbyrdes forbundethed, hvor der anvendes grænseoverskridende væsentlige tjenester, som realøkonomien er afhængig af, som følge af 1) dybtgående og omfattende brug af IKT og 2) risikoen for, at virkningerne af en driftshændelse i en finansiel virksomhed eller finansiel delsektor hurtigt kan sprede sig til andre virksomheder eller dele af den finansielle sektor og i sidste ende til resten af økonomien.

Selv om den finansielle sektor er meget langt fremme med hensyn til sin markeds- og reguleringsintegration og er velfungerende på grundlag af et fælles sæt harmoniserede regler — EU's fælles regelsæt — har EU's reaktion på øgede behov for operationel modstandsdygtighed på både horisontalt niveau og sektorniveau været enten

- baseret på minimal harmonisering og dermed givet plads til national fortolkning og fragmentering på det indre marked eller
- for generel og med begrænset anvendelse, idet den i varierende grad imødegår overordnede operationelle risici, navnlig ved at regulere visse elementer af digital operationel modstandsdygtighed (f.eks. IKT-risikostyring, indberetning af hændelser og IKT-risici for tredjeparter).

EU's indgriben har hidtil ikke imødegået operationelle risici på en måde, der modsvarer finansielle virksomheders behov for at modstå, reagere på og afhjælpe IKT-svagheder; den giver heller ikke finansielle tilsynsmyndigheder værktøjerne til at opfylde deres mandat til dæmme op for finansiel ustabilitet, som skyldes sådanne IKT-svagheder.

De nuværende mangler og uoverensstemmelser har ført til udbredelse af ukoordinerede nationale initiativer (f.eks. vedrørende afprøvning) og tilsynsmæssige tilgange (f.eks. til IKT-afhængighed af tredjeparter), som giver udslag enten i overlapninger, duplikeringer af krav og høje administrative omkostninger og overholdelsesomkostninger for grænseoverskridende virksomheder eller af IKT-risici, der ikke bliver opdaget og imødegået. Samlet set er der ingen garanti for stabilitet og integritet i den finansielle sektor, og det indre marked for finansielle tjenesteydelser er fortsat fragmenteret med en svækkelse af forbruger- og investorbeskyttelsen til følge.

Hvilke resultater forventes der af initiativet?

Det overordnede mål er at øge den digitale operationelle modstandsdygtighed i EU's finansielle sektor ved at strømline og ajourføre den eksisterende finansielle EU-lovgivning og indføre nye krav, hvor der er mangler, med det formål at

- forbedre finansielle virksomheders styring af IKT-risici,
- øge tilsynsmyndigheders kendskab til trusler og hændelser,
- forbedre finansielle virksomheders afprøvning af IKT-systemer og
- sikre bedre tilsyn med risici, som skyldes finansielle virksomheders afhængighed af tredjepartsudbydere af IKT-tjenester.

Nærmere betegnet vil forslaget skabe mere sammenhængende og ensartede mekanismer til indberetning af hændelser og dermed mindske de administrative byrder for finansielle institutioner og styrke den tilsynsmæssige effektivitet.

Hvad er merværdien ved at handle på EU-plan?

EU's indre marked for finansielle tjenesteydelser reguleres af et stort regelsæt, der er fastsat på EU-plan, og som giver finansielle virksomheder, der er meddelt tilladelse i en given medlemsstat, mulighed for at udbyde tjenesteydelser på hele det indre marked takket være en EU-pasordning. Derfor vil regler på nationalt plan ikke være en effektiv metode til at styrke den operationelle modstandsdygtighed i finansielle virksomheder, der anvender pasordningen. Som følge af den finansielle krise indeholder EU's fælles regelsæt desuden særdeles detaljerede og normative regler, der vedrører mere "traditionelle" risici såsom kredit-, markeds-, modparts- og likviditetsrisici. De eksisterende bestemmelser om operationelle risici er fortsat generelle. Styrkelse af digital operationel modstandsdygtighed kræver tilpasninger af bestemmelser om operationelle risici, som allerede er fastlagt på EU-plan — og som dermed kun kan ajourføres og suppleres på EU-plan.

B. Løsninger

Hvilke lovgivningsmæssige og ikkelovgivningsmæssige løsninger er overvejet? Foretrækkes en bestemt løsning frem for andre? Hvorfor?

I konsekvensanalysen overvejes tre løsninger, foruden et referencescenarie, hvor der ikke træffes foranstaltninger med hensyn til EU-lovgivningen om finansielle tjenesteydelser. Nærmere bestemt:

- **"Ingen foranstaltninger"**: Regler om operationel modstandsdygtighed vil fortsat være fastsat i det nuværende, forskelligartede sæt EU-bestemmelser om finansielle tjenesteydelser, som delvist findes i NIS-direktivet, og i eksisterende eller fremtidige nationale ordninger.
- **Løsning 1 — Styrkelse af kapitalbuffere**: Der indføres en supplerende kapitalbuffer for at øge finansielle virksomheders evne til at absorbere tab, der kan opstå som følge af manglende operationel modstandsdygtighed.
- **Løsning 2 — En retsakt om digital operationel modstandsdygtighed i forbindelse med finansielle tjenesteydelser**: Der indføres en omfattende ramme på EU-plan, som fastsætter regler vedrørende digital operationel modstandsdygtighed for alle regulerede finansielle institutioner, og som
  - i mere omfattende grad vil imødegå IKT-risici,
  - vil give finansielle tilsynsmyndigheder adgang til oplysninger om IKT-relaterede hændelser,
  - vil sikre, at finansielle virksomheder vurderer, om deres foranstaltninger vedrørende forebyggelse og modstandsdygtighed er effektive, og identificerer IKT-svagheder,
  - vil styrke de bestemmelser om outsourcing, som regulerer det indirekte tilsyn med tredjepartsudbydere af IKT-tjenester,
  - vil muliggøre direkte tilsyn med de aktiviteter, som tredjepartsudbydere af IKT-tjenester udfører, når de udbyder deres tjenesteydelser til finansielle virksomheder, og
  - desuden vil give incitament til udveksling af efterretningsoplysninger om trusler i den finansielle sektor.
- **Løsning 3 — Retsakt om modstandsdygtighed kombineret med centraliseret tilsyn med kritiske tredjepartsudbydere**: Foruden en retsakt om operationel modstandsdygtighed (løsning 2) oprettes der en ny myndighed, der skal føre tilsyn med tredjepartsudbydere af kritiske IKT-tjenester til finansielle virksomheder. Den vil også sikre en klarere afgræsning af den finansielle sektor i forhold til NIS-direktivets anvendelsesområde.

Løsning 2 er den foretrukne løsning. I sammenligning med de andre løsninger er det den løsning, der opfylder flest af initiativets mål, samtidig med at der tages hensyn til kriteriet om effektivitet og sammenhæng. Denne løsning har også størst opbakning blandt interessenterne.

Hvem støtter hvilken løsning?

De fleste interessenter (private, offentlige) er enige om, at der er behov for EU-foranstaltninger til at sikre bedre beskyttelse af finansielle virksomheders operationelle modstandsdygtighed. Mange mener også, at EU-foranstaltninger er nødvendige for at tackle den reguleringsmæssige byrde, der følger af, at finansielle virksomheder er underlagt overlappende og inkonsekvente regler, som er fastsat i NIS-direktivet, EU-lovgivningen om finansielle tjenesteydelser og nationale ordninger (f.eks. med hensyn til indberetning af hændelser). Ganske få interessenter støtter altså, at der ikke træffes foranstaltninger. Nogle få interessenter mener, at det er hensigtsmæssigt at beskytte operationel modstandsdygtighed ved hjælp af øgede kapitalbuffere (løsning 1). Dette er dog den traditionelle tilgang til operationelle risici, navnlig på bankområdet, og betragtes som sådan af f.eks. internationale standardsættere. Den type kvalitative foranstaltninger, der indgår i løsning 2, og som vil strømline og ajourføre den finansielle EU-lovgivning og indføre nye krav, hvor der er mangler, samtidig med at forbindelserne til det horisontale NIS-direktiv opretholdes, opnår bred støtte blandt de interessenter, der besvarede den offentlige høring. Mens nogle interessenter (navnlig offentlige) mener, at øget tilsyn med tredjepartsudbydere af IKT-tjenester som i løsning 3 er hensigtsmæssigt, opnår oprettelsen af en ny EU-myndighed til dette formål kun begrænset støtte blandt interessenterne, og det samme gælder det mere fuldstændige brud med rammen under NIS-direktivet.

C. Den foretrukne løsnings virkninger

Hvilke fordele er der ved den foretrukne løsning (hvis en bestemt løsning foretrækkes – ellers fordelene ved de vigtigste af de mulige løsninger)?

Løsning 2 vil imødegå **IKT-risici** i hele den finansielle sektor ved at øge finansielle institutioners kapaciteter til at modstå IKT-hændelser. Dette vil mindske risikoen for, at en cyberhændelse hurtigt spreder sig på tværs af finansielle markeder. Mens det er vanskeligt at foretage et skøn over omkostninger forbundet med operationelle hændelser i den finansielle sektor (ikke alle hændelser indberettes, omfanget af omkostninger er usikkert), tyder industriens vurderinger på, at omkostningerne for EU's finansielle sektor ligger på mellem 2-27 mia. EUR om

året. Den foretrukne løsning vil begrænse disse direkte omkostninger og eventuelle bredere virkninger, som store cyberhændelser kan få for den finansielle stabilitet. Elimineringen af overlappende **indberetningskrav** vil mindske de administrative byrder. F.eks. kan de dermed forbundne besparelser for nogle af de største banker ligge på mellem 40-100 mio. EUR om året. Direkte indberetning vil også øge tilsynsmyndighedernes kendskab til IKT-hændelser. **Harmoniseret afprøvningspraksis** vil sikre, at ukendte svagheder og risici opdages. Den vil også nedbringe omkostningerne, navnlig for grænseoverskridende virksomheder. F.eks. kan de samlede forventede fordele ved en fælles tilgang til afprøvning for de 44 største grænseoverskridende banker ligge på mellem 11 og 88 mio. EUR. Ved at indføre et sammenhængende regelsæt om styring af risici forbundet med **tredjepartsudbydere af IKT-tjenester** vil finansielle virksomheder have mere kontrol med, hvordan tredjepartsudbydere efterlever lovrammen, hvilket kan berolige tilsynsmyndighederne. Der vil også være tilsynsmæssige fordele som følge af tilsynet med tredjepartsudbydere af IKT-tjenester. Samlet set medfører den foretrukne løsning bredere samfundsmæssige fordele, som skyldes et mere modstandsdygtigt operationelt miljø for alle finansielle markedsdeltagere, samt styrket forbruger- og investorbeskyttelse.

Hvilke omkostninger er der ved den foretrukne løsning (hvis en bestemt løsning foretrækkes — ellers omkostningerne ved de vigtigste af de mulige løsninger)?

Den foretrukne løsning vil medføre en stigning i både engangsomkostninger og tilbagevendende omkostninger. Med hensyn til sidstnævnte skyldes de investeringer i IT- systemer, og de er vanskelige at sætte tal på, da virksomheders nedarvede systemer er i forskellig forfatning. I mangel af reguleringsindgreb har nogle finansielle virksomheder allerede foretaget betydelige investeringer i IKT-systemer. Dette betyder, at omkostninger forbundet med gennemførelsen af foranstaltningerne i dette forslag sandsynligvis vil være begrænsede for store finansielle virksomheder. For mindre virksomheder forventes omkostningerne også være begrænsede, da de vil være omfattet af mindre strenge krav, som står i rimeligt forhold til deres lavere risici. Med hensyn til afprøvning har de europæiske tilsynsmyndigheder anslået, at omkostningerne forbundet med trusselsbaserede indtrængningstests ligger på mellem 0,1 % og 0,3 % af de pågældende virksomheders samlede IKT-budget. Omkostninger forbundet med indberetning af hændelser vil blive kraftigt reduceret, da der ikke vil være nogen overlapninger med indberetning i henhold til NIS-direktivet. Tilsynsmyndigheder vil også pådrage sig yderligere omkostninger som følge af de supplerende opgaver, som de vil skulle varetage. For tilsynsmyndigheder, som deltager i det direkte tilsyn med tredjepartsudbydere af IKT-tjenester, forventes f.eks. den anslåede stigning i årsværk at ligge på mellem 1-5 årsværk for den førende myndighed og på ca. 0,25 årsværk for de deltagende myndigheder.

Hvordan påvirker den foretrukne løsning virksomhederne, herunder de små og mellemstore virksomheder og mikrovirksomhederne?

Den foretrukne løsning vil omfatte alle finansielle virksomheder for at øge den operationelle modstandsdygtighed i sektoren som helhed. Dette brede anvendelsesområde er vigtigt set i lyset af den finansielle sektors indbyrdes forbundethed og det dertil svarende behov for en solid grad af overordnet operationel modstandsdygtighed. Når de centrale krav på tværs af de vigtigste indsatsområder defineres, vil proportionalitetsprincippet imidlertid finde anvendelse såvel i delsektorer som inden for de enkelte sektorer. Dermed tages der hensyn til bl.a. forskellige forretningsmodeller, størrelse, profil, systemisk betydning osv. F.eks. vil foranstaltninger vedrørende indberetning af hændelser og afprøvning være mindre strenge for mindre finansielle virksomheder.

Vil den foretrukne løsning få væsentlige virkninger for de nationale budgetter og myndigheder?

Nej. Som vist ovenfor kan det supplerende tilsyn udføres med en begrænset grad af yderligere tilsynsressourcer, som helt eller delvist (hvis der pålægges tilsynsgebyrer) kan afholdes over de offentlige budgetter.

Vil den foretrukne løsning få andre væsentlige virkninger?

De socioøkonomiske konsekvenser af covid-19-pandemien illustrerer den afgørende betydning af digitale finansielle markeder og deres operationelle modstandsdygtighed. Den foretrukne løsning vil skabe et solidt grundlag for at høste fordelene ved den digitale omstilling, idet den sikrer, at det indre marked for finansielle tjenesteydelser, herunder bankunionen og kapitalmarkedsunionen, har operationel modstandsdygtighed baseret på et sæt regler og krav, som tjener til at opnå sikkerhed, kapacitet, stabilitet og lige vilkår. Dette vil også styrke Europas stilling som globalt førende aktør på det finansielle og digitale område, hvilket er et mål, som Kommissionen har fastsat i sin meddelelse "Europas digitale fremtid i støbeskeen".

D. Opfølgning

Hvornår vil foranstaltningen blive taget op til fornyet overvejelse?

Den første gennemgang vil finde sted tre år efter det retlige instruments ikrafttræden. Kommissionen vil aflægge rapport til Europa-Parlamentet og Rådet om sin gennemgang. Gennemgangen kan alt efter relevans underbygges af en offentlig høring, undersøgelser, ekspertdrøftelser, spørgeundersøgelser og workshops.