Europeiska unionens råd

Bryssel den 24 september 2020
(OR. en)

11052/20
ADD 2

Interinstitutionellt ärende:
2020/0268(COD)

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

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	24 september 2020
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	SWD(2020) 204 final
Ärende:	ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN Följedokument till Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv 2006/43/EG, 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 och (EU) 2016/2341

För delegationerna bifogas dokument – SWD(2020) 204 final.

Bilaga: SWD(2020) 204 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 24.9.2020
SWD(2020) 204 final

NOTE
This language version reflects the corrections done to the original EN version retransmitted under SWD(2020) 204 final/2 of 16.10.2020

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGSRAPPORTEN

Följedokument till

Förslag till Europaparlamentets och rådets direktiv

om ändring av direktiv 2006/43/EG, 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 och (EU) 2016/2341

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

Sammanfattning

Konsekvensbedömning av förslaget till förordning om digital operativ motståndskraft i finanssektorn

A. Behov av åtgärder

Varför? Vilket problem behöver åtgärdas?

Finanssektorn är mycket beroende av informations- och kommunikationsteknik (IKT). Detta beroende kommer sannolikt att öka i och med den rådande covid-19-pandemin, med tanke på de fördelar som det innebär att garantera kontinuerlig fjärråtkomst till finansiella tjänster. Beroendet av digital teknik är dock förenat med vissa problem: företagen måste kunna klara eventuella IKT-störningar, för att hantera digitala incidenter och hot samt upprätthålla tjänster. Alla ekonomiska sektorer är utsatta för de sårbarheter som följer av beroendet av IKT, men framför allt den mycket sammankopplade finanssektorn som utnyttjar vitala gränsöverskridande tjänster som realekonomin är beroende av, på grund av 1) den omfattande och breda IKT-användningen och 2) potentialen för att effekterna av en operativ incident vid ett finansföretag eller en finansiell undersektor snabbt sprider sig till andra företag eller delar av finanssektorn och i slutändan till övriga ekonomin.

Finanssektorn har kommit mycket långt när det gäller att integrera marknader och regelverk och åtnjuta fördelarna av en gemensam uppsättning harmoniserade bestämmelser – det enhetliga europeiska regelverket. Trots detta har EU:s svar på behoven av ökad operativ motståndskraft på såväl horisontell nivå som sektorsnivå antingen

- baserats på minimiharmonisering och således gett utrymme för nationell tolkning och splittring på den inre marknaden, eller
- haft ett alldeles för allmänt och därmed begränsat tillämpningsområde och åtgärdat den övergripande operativa risken i varierande grad, genom en partiell reglering av vissa delar av digital operativ *motståndskraft* (t.ex. hantering av IKT-risker, incidentrapportering och IKT-risk för tredje parter) medan andra delar inte reglerats (testning).

EU har hittills inte åtgärdat den operativa risken på ett sådant sätt som motsvarar finansföretagens behov att klara, svara på och återhämta sig från IKT-relaterade sårbarheter. EU förser inte heller finansiella tillsynsmyndigheter med de verktyg som de behöver för att fullgöra sitt uppdrag att begränsa den finansiella instabilitet som uppstår till följd av sådana IKT-relaterade sårbarheter.

De befintliga luckorna och inkonsekvenserna har lett till en spridning av osamordnade nationella initiativ (t.ex. i fråga om testning) och tillsynsmetoder (t.ex. i fråga om beroende av tredje parter för IKT), vilket leder antingen till överlappningar, dubbla uppsättningar krav samt stora administrativa och efterlevnadsmässiga kostnader för gränsöverskridande finansföretag eller till oupptäckta och oåtgärdade IKT-risker. Finanssektorns stabilitet och integritet är generellt sett inte säkerställd och den inre marknaden för finansiella tjänster är fortfarande fragmenterad, med ett försvagat konsument- och investerarskydd som följd.

Vad förväntas initiativet leda till?

Det allmänna syftet är att stärka den digitala operativa motståndskraften inom EU:s finanssektor genom att harmonisera och uppdatera EU:s befintliga finanslagstiftning och införa nya krav där luckor finns, i syfte att

- förbättra finansföretagens hantering av IKT-risker,
- öka tillsynsmyndigheternas kunskap om hot och incidenter,
- förbättra finansföretagens testning av sina IKT-system, och
- bättre övervaka de risker som följer av finansföretagens beroende av tredjepartsleverantörer av IKT.

Förslaget skulle närmare bestämt leda till mer samstämmiga och enhetliga mekanismer för incidentrapportering och således till en mindre administrativ börda för de finansiella instituten och en mer effektiv tillsyn.

Vad är mervärdet med åtgärder på EU-nivå?

EU:s inre marknad för finanstjänster regleras genom en stor uppsättning bestämmelser som fastställts på EU-nivå och som innebär att finansföretag som har auktoriserats i en medlemsstat får tillhandahålla tjänster på hela den inre marknaden tack vare ett EU-pass. Nationella bestämmelser skulle följaktligen inte vara effektivt för att stärka den operativa motståndskraften hos företag som använder sig av passet. Till följd av finanskrisen innehåller det enhetliga europeiska regelverket dessutom mycket utförliga och normativa bestämmelser som rör mer ”traditionella” risker som kredit-, marknads-, motparts- och likviditetsrisker. De befintliga bestämmelserna om operativ risk är fortfarande av generell karaktär. För att stärka den digitala operativa motståndskraften krävs ändringar av de bestämmelser om operativ risk som redan har fastställts på EU-nivå – och som således endast kan uppdateras och kompletteras på EU-nivå.

B. Lösningar

Vilka alternativ, både lagstiftning och andra åtgärder, har övervägts? Finns det ett rekommenderat alternativ? Varför?

Vid konsekvensbedömningen beaktades tre alternativ, utöver ett grundscenario där inga åtgärder vidtas beträffande EU:s lagstiftning om finansiella tjänster. Närmare bestämt följande:

- **”Inga åtgärder”**: Bestämmelser om operativ motståndskraft fortsätter att fastställas genom de nuvarande skiljaktiga EU-bestämmelserna om finansiella tjänster, delvis genom NIS-direktivet, och genom befintliga eller framtida system på nationell nivå.
- **Alternativ 1 – stärkta kapitalbuffertar**: En ytterligare kapitalbuffert införs för att öka finansföretagens förmåga att absorbera förluster som skulle kunna uppstå till följd av bristande operativ motståndskraft.
- **Alternativ 2 – en akt om digital operativ motståndskraft hos finansiella tjänster**: Här införs en omfattande ram på EU-nivå med bestämmelser om digital operativ motståndskraft för alla reglerade finansinstitut, vilken skulle
    - åtgärda IKT-risker på ett mer heltäckande sätt,
    - göra det möjligt för tillsynsmyndigheter att få tillgång till information om IKT-relaterade incidenter,
    - säkerställa att finansföretag bedömer ändamålsenligheten i deras förebyggande och motståndskraftsrelaterade åtgärder samt identifierar sårbarheter i fråga om IKT,
    - stärka utkontrakteringsbestämmelserna om den indirekta tillsynen av tredjepartsleverantörer av IKT,
    - möjliggöra direkt tillsyn av den verksamhet som tredjepartsleverantörer av IKT bedriver när de tillhandahåller sina tjänster till finansföretag, och
    - uppmuntra utbyte av hotinformation inom finanssektorn.
- **Alternativ 3 – akt om motståndskraft tillsammans med central tillsyn av kritiska tredjepartsleverantörer**: Utöver att införa en akt om operativ motståndskraft (alternativ 2) inrättas en ny myndighet som ska övervaka tredjepartsleverantörer av IKT som tillhandahåller kritiska IKT-tjänster till finansföretag. Det innebär även en tydligare avgränsning av NIS-direktivets tillämpningsområde för finanssektorn.

Alternativ 2 är det som rekommenderas. Jämfört med de andra alternativen uppnås de flesta av initiativets syften med detta alternativ, samtidigt som effektivitets- och samstämmighetskriterierna beaktas. Detta alternativ får dessutom mest stöd från berörda parter.

Vem stöder vilket alternativ?

De flesta berörda parter (privata och offentliga) är överens om att EU-åtgärder behövs för att bättre trygga finansföretagens operativa motståndskraft. Många anser dessutom att EU-åtgärder krävs för att åtgärda de tillsynsmässiga bördor som följer av att finansföretag omfattas av överlappande och oförenliga bestämmelser i NIS-direktivet, EU:s lagstiftning om finansiella tjänster och nationella system (t.ex. i fråga om incidentrapportering). Endast ett fåtal berörda parter stöder således alternativet att inte vidta några åtgärder. Några berörda parter ser värdet i att trygga den operativa motståndskraften genom ökade kapitalbuffertar (alternativ 1). Detta är dock den traditionella åtgärden mot operativ risk, särskilt inom banksektorn, och övervägs exempelvis av internationella normgivande organ. De berörda parter som deltog i det offentliga samrådet stöder i hög grad den typ av kvalitativa åtgärder som anges i alternativ 2 som skulle leda till en harmonisering och uppdatering av EU:s finansiella lagstiftning och till ett införande av nya krav där luckor kvarstår samtidigt som kopplingar till det övergripande NIS-direktivet upprätthålls. Vissa berörda parter (särskilt offentliga sådana) ser värdet i en stärkt tillsyn av tredjepartsleverantörer av IKT enligt alternativ 3, men endast ett begränsat antal berörda parter stöder inrättandet av en ny EU-myndighet för ändamålet liksom den mer fullständiga brytningen med NIS-lagstiftningen.

C. Det rekommenderade alternativets konsekvenser

Vad är nyttan med det rekommenderade alternativet (om ett sådant alternativ finns, annars anges för huvudsakliga alternativ)?

Med alternativ 2 hanteras **IKT-risker** i hela finanssektorn genom att finansinstituten får stärkt kapacitet att klara IKT-incidenter. Detta minskar risken för att en it-incident snabbt sprids på finansmarknaderna. Det är svårt att uppskatta kostnaderna för operativa incidenter inom finanssektorn (inte alla incidenter rapporteras och kostnaderna är av okänd omfattning), men uppskattningar från branschen tyder på att kostnaderna för EU:s finanssektor skulle kunna motsvara 2–27 miljarder euro per år. Det rekommenderade alternativet skulle leda till en begränsning av dessa direkta kostnader och den mer omfattande påverkan som stora it-incidenter kan ha på den finansiella stabiliteten. De administrativa bördorna skulle minska om de överlappande **rapporteringskraven** tas bort. Detta kan till exempel leda till årliga besparingar på mellan 40 och 100 miljoner euro för några av de största bankerna. Med direkt rapportering skulle tillsynsmyndigheterna dessutom få större kunskap om IKT-incidenter. Metoder för **harmoniserad testning** skulle leda till en större upptäckt av okända sårbarheter och

risker. Det skulle även medföra lägre kostnader, framför allt för gränsöverskridande företag. De totala förväntade vinsterna med en gemensam testningsmetod skulle till exempel kunna uppgå till 11–88 miljoner euro för de 44 största gränsöverskridande bankerna. Genom att införa enhetliga bestämmelser för att hantera risker med **tredjepartsleverantörer av IKT-tjänster** skulle finansföretagen få större kontroll över hur tredjepartsleverantörer följer regelverket, vilket skulle vara betryggande för tillsynsmyndigheterna. Den tillsynsmässiga övervakningen av tredjepartsleverantörer av IKT skulle även innebära tillsynsmässiga fördelar. Det rekommenderade alternativet innebär överlag större samhällsmässiga fördelar, till följd av en mer motståndskraftig operativ miljö för alla finansmarknadsaktörer och ett stärkt konsument- och investerarskydd.

Vad är kostnaderna för de rekommenderade alternativen (om sådana alternativ finns, annars anges för huvudsakliga alternativ)?

Det rekommenderade alternativet skulle medföra såväl engångskostnader som återkommande kostnader. De förstnämnda är en följd av investeringar i it-system och är svåra att beräkna med tanke på skicket på företagens befintliga system. Vissa finansföretag har redan gjort stora investeringar i IKT-system, utan regleringsåtgärder. Detta innebär att stora finansföretag sannolikt inte kommer att ha problem med att genomföra åtgärderna i detta förslag. Kostnaderna förväntas bli låga även för de mindre företagen, eftersom de skulle omfattas av mindre hårda åtgärder som står i proportion till deras lägre risk. När det gäller testning har de europeiska tillsynsmyndigheterna uppskattat att kostnaderna för hotstyrd penetrationstestning motsvarar mellan 0,1 % och 0,3 % av de berörda företagens totala IKT-budget. Kostnaderna för incidentrapportering skulle minska markant, eftersom inga överlappningar skulle finnas med NIS-rapporteringen. Tillsynsmyndigheterna kommer också att ådra sig vissa kostnader, till följd av de tillkommande arbetsuppgifter som de skulle utföra. För tillsynsmyndigheter som deltar i direkt tillsyn av tredjepartsleverantörer av IKT skulle till exempel antalet heltidsekvivalenter kunna förväntas öka med uppskattningsvis 1 till 5 heltidsekvivalenter för den ledande myndigheten och med cirka 0,25 heltidsekvivalenter för de deltagande myndigheterna.

Hur påverkas företagen, särskilt små och medelstora företag och mikroföretag?

Det rekommenderade alternativet skulle omfatta alla finansföretag, för att stärka den operativa motståndskraften i sektorn som helhet. Detta breda tillämpningsområde är viktigt med tanke på finanssektorns sammankopplade karaktär och det tillhörande behovet att ha en sund nivå av operativ motståndskraft överlag. Proportionalitetsprincipen skulle dock tillämpas både för samtliga undersektorer och enskilt inom respektive undersektor, när de grundläggande kraven fastställs för alla de viktigaste insatsområdena. Hänsyn skulle bland annat tas till skillnader i företagsmodeller, storlek, riskprofil, systemvikt och så vidare. Mindre finansföretag skulle till exempel omfattas av mildare åtgärder för incidentrapportering och testning.

Påverkas medlemsstaternas budgetar och förvaltningar i betydande grad?

Nej. Den ytterligare tillsynen kan, såsom framgår ovan, kräva ytterligare tillsynsresurser i viss mån, vilka helt eller delvis (om tillsynsavgifter införs) bärs av den offentliga budgeten.

Uppstår andra betydande konsekvenser?

De socioekonomiska effekterna av covid-19-pandemin påvisar den stora vikten av digitala finansmarknader och av att dessa är operativt motståndskraftiga. Det rekommenderade alternativet skulle utgöra en solid grund för att ta tillvara den digitala omvandlingen genom att säkerställa att den inre marknaden för finansiella tjänster, inbegripet inom bank- och kapitalmarknadsunionen, är operativt motståndskraftig, utifrån en gemensam uppsättning bestämmelser och krav med säkerhet, prestation, stabilitet och lika villkor som mål. Detta kommer dessutom att stärka Europas ställning som en global finansiell och digital ledare, ett mål som kommissionen fastställde i sitt meddelande *Att forma EU:s digitala framtid*.

D. Uppföljning

När kommer åtgärderna att ses över?

Den första översynen kommer att äga rum tre år efter det rättsliga instrumentets ikraftträdande. Kommissionen kommer att överlämna en rapport till Europaparlamentet och rådet om översynen. Ett offentligt samråd, studier, expertdiskussioner, undersökningar och seminarier skulle kunna användas som underlag till översynen, beroende på vad som är lämpligt.