

|  |
| --- |
| **Sammanfattning** |
| Konsekvensbedömning av förslaget till förordning om digital operativ motståndskraft i finanssektorn |
| **A. Behov av åtgärder** |
| **Varför? Vilket problem behöver åtgärdas?**  |
| Finanssektorn förlitar sig i stor utsträckning på informations- och kommunikationsteknik (IKT). Den pågående covid-19-pandemin kommer sannolikt att påskynda denna utveckling, med tanke på fördelarna med att säkerställa kontinuerlig fjärråtkomst till finansiella tjänster. Beroendet av digital teknik väcker dock även vissa farhågor. Företagen måste kunna stå emot potentiella IKT-avbrott, så att digitala incidenter och hot åtgärdas och tjänster kan upprätthållas. Sårbarheter till följd av IKT-beroende finns visserligen i alla ekonomiska sektorer, men de är särskilt uttalade i en starkt sammanlänkad finanssektor med gränsöverskridande vitala tjänster som den reala ekonomin är beroende av, på grund av 1) den djupgående och omfattande användningen av IKT, och 2) risken för att effekterna av en operativ incident vid ett finansiellt företag eller i en finansiell delsektor snabbt sprider sig till andra finansiella företag eller delsektorer och i förlängningen till resten av ekonomin. Trots att finanssektorn har kommit mycket långt i sin marknads- och regleringsintegration och har gynnats av en gemensam uppsättning harmoniserade regler – EU:s enhetliga regelverk – har EU:s svar på de ökade behoven av operativ motståndskraft på såväl horisontell som sektoriell nivå antingen varit* baserat på minimiharmonisering, vilket ger utrymme för nationell tolkning och fragmentering på den inre marknaden, eller
* alltför allmänt och haft en begränsad tillämpning, där den övergripande operativa risken har hanterats i varierande grad, genom att vissa delar av den digitala operativa motståndskraften (t.ex. IKT-riskhantering, incidentrapportering och IKT-tredjepartsrisk) har reglerats delvis, medan andra delar har utelämnats (testning).

EU:s insatser har hittills inte avhjälpt operativa risker på ett sätt som motsvarar de finansiella företagens behov av att stå emot, åtgärda och återhämta sig från IKT-sårbarheter, och har inte heller gett de finansiella tillsynsmyndigheterna verktyg för att uppfylla sitt uppdrag att begränsa finansiell instabilitet till följd av dessa IKT-sårbarheter. De nuvarande luckorna och inkonsekvenserna har lett till en ökning av icke samordnade nationella initiativ (t.ex. om testning) och tillsynsstrategier (t.ex. när det gäller beroende av IKT-tredjeparter), vilket leder till överlappningar, dubbleringar av krav och höga administrativa kostnader och efterlevnadskostnader för gränsöverskridande finansiella företag eller till att IKT-risker förblir oupptäckta och oåtgärdade. Den finansiella sektorns stabilitet och integritet garanteras inte som helhet, och den inre marknaden för finansiella tjänster är fortfarande fragmenterad, vilket leder till att skyddet för konsumenter och investerare försvagas.  |
| **Vad förväntas initiativet leda till?**  |
| Det övergripande målet är att stärka den digitala operativa motståndskraften hos EU:s finanssektor genom att rationalisera och uppgradera EU:s befintliga finansiella lagstiftning och införa nya krav där det finns luckor, i syfte att * förbättra finansföretagens hantering av IKT-risker,
* öka tillsynsmyndigheternas kunskaper om hot och incidenter,
* förbättra finansföretagens testning av sina IKT-system, och
* förbättra övervakningen av risker som härrör från finansföretags beroende IKT-tredjepartsleverantörer.

Mer specifikt skulle förslaget skapa mer enhetliga och konsekventa mekanismer för incidentrapportering, vilket skulle minska den administrativa bördan för finansinstitut och stärka tillsynens effektivitet.  |
| **Vad är mervärdet med åtgärder på EU-nivå?**  |
| EU:s inre marknad för finansiella tjänster styrs av ett stort antal regler på EU-nivå som gör det möjligt för finansiella företag som är auktoriserade i en medlemsstat att tillhandahålla tjänster på hela den inre marknaden på grundval av ett EU-pass. Därför skulle regler på nationell nivå inte vara en effektiv metod för att stärka den operativa motståndskraften hos de finansiella företag som använder passet. Till följd av finanskrisen innehåller EU:s enhetliga regelverk dessutom mycket detaljerade och föreskrivande regler för att hantera mer ”traditionella” risker såsom kredit-, marknads-, motparts- och likviditetsrisker. De befintliga bestämmelserna om operativ risk är fortfarande allmänna. För att stärka den digitala operativa motståndskraften krävs anpassningar av de bestämmelser om operativa risker som redan har fastställts på EU-nivå – och som därför endast kan uppgraderas och kompletteras på EU-nivå.  |

|  |
| --- |
| **B. Lösningar** |
| **Vilka alternativ, både lagstiftning och andra åtgärder, har övervägts? Finns det ett rekommenderat alternativ? Varför?**  |
| I konsekvensbedömningen har tre alternativ övervägts, utöver ett grundscenario där inga åtgärder vidtas när det gäller EU:s lagstiftning om finansiella tjänster. Närmare bestämt är det fråga om följande: * **”Inga åtgärder”**: regler om operativ motståndskraft skulle även i fortsättningen fastställas genom de nuvarande, fragmenterade EU-bestämmelserna om finansiella tjänster, delvis genom direktivet om säkerhet i nätverks- och informationssystem och genom befintliga eller framtida nationella system.
* **Alternativ 1 – att stärka kapitalbuffertar**: en ytterligare kapitalbuffert skulle införas för att öka finansföretagens förmåga att absorbera förluster som skulle kunna uppstå på grund av bristande operativ motståndskraft.
* **Alternativ 2 – en rättsakt om digital operativ motståndskraft för finansiella tjänster**: med en sådan skulle det införas en övergripande ram på EU-nivå med regler för den digitala operativa motståndskraften för alla reglerade finansinstitut, vilket skulle
	+ hantera IKT-risker på ett mer övergripande sätt,
	+ ge de finansiella tillsynsmyndigheterna tillgång till information om IKT-relaterade incidenter,
	+ säkerställa att finansiella företag bedömer effektiviteten i sina förebyggande åtgärder och åtgärder för motståndskraft och identifierar IKT-sårbarheter,
	+ stärka de regler för utkontraktering som styr den indirekta tillsynen av tredjepartsleverantörer inom IKT-sektorn,
	+ möjliggöra en direkt tillsyn över den verksamhet som utförs av IKT-tredjepartsleverantörer sektorn när de tillhandahåller sina tjänster till finansiella företag, och
	+ dessutom ge incitament för utbyte av hotbildsinformation inom finanssektorn.
* **Alternativ 3 – rättsakt om motståndskraft i kombination med centraliserad tillsyn av kritiska tredjepartsleverantörer**: utöver en rättsakt om operativ motståndskraft (alternativ 2) skulle en ny myndighet inrättas för att övervaka tredjepartsleverantörer av kritiska IKT-tjänster till finansiella företag. En sådan skulle också tydligare avgränsa finanssektorn från tillämpningsområdet för nätverks- och informationssäkerhetsdirektivet.

Alternativ 2 är det alternativ som föredras. Jämfört med de andra alternativen är det genom detta alternativ som de flesta av initiativets mål kan uppnås, samtidigt som effektivitets- och samstämmighetskriterierna beaktas. Detta alternativ får också störst stöd från de berörda parterna. |
| **Vem stöder vilka alternativ?**  |
| De flesta berörda parter (privata och offentliga) håller med om att EU-åtgärder behövs för att bättre skydda finansföretagens operativa motståndskraft. Många anser också att det är nödvändigt att vidta EU-åtgärder för att ta itu med de regelbördor som uppstår till följd av att finansiella företag omfattas av överlappande och inkonsekventa regler i direktivet om säkerhet i nätverks- och informationssystem, EU:s lagstiftning om finansiella tjänster och nationella system (t.ex. när det gäller incidentrapportering). Följaktligen är det få berörda parter som stöder alternativet att inga åtgärder vidtas. Få berörda parter ser fördelar med att skydda den operativa motståndskraften genom ökade kapitalbuffertar (alternativ 1). Detta är dock den traditionella metoden för att hantera operativa risker, särskilt inom banksektorn och den övervägs därför av t.ex. internationella standardiseringsorgan. Den typ av kvalitativa åtgärder som anges i alternativ 2 och som skulle effektivisera och uppgradera EU:s finansiella lagstiftning och införa nya krav där det finns luckor samtidigt som kopplingarna till det övergripande direktivet om säkerhet i nätverks- och informationssystem upprätthålls får brett stöd av de berörda parter som deltog i det offentliga samrådet. Vissa berörda parter (särskilt offentliga) ser fördelar med att stärka tillsynen av tredjepartsleverantörer inom IKT enligt alternativ 3, men inrättandet av en ny EU-myndighet för detta ändamål stöds endast av ett begränsat antal berörda parter, liksom en mer fullständig frikoppling från reglerna om säkerhet i nätverks- och informationssystem. |
| **C. Det rekommenderade alternativets konsekvenser** |
| **Vad är nyttan med det rekommenderade alternativet (om ett sådant alternativ finns, annars anges för huvudsakliga alternativ)?**  |
| Genom alternativ 2 kan **IKT-risker** hanteras i hela finanssektorn genom att finansinstitutens förmåga att stå emot IKT-incidenter förstärks. Detta skulle minska risken för en cyberincident som snabbt sprids över finansmarknaderna. Det är svårt att uppskatta kostnaderna för operativa incidenter inom finanssektorn (inte alla incidenter rapporteras, det är osäkert hur stora kostnaderna är), men branschbedömningar tyder på att kostnaderna för EU:s finanssektor kan ligga på mellan 2 och 27 miljarder euro per år. Det rekommenderade alternativet skulle innebära en minskning av dessa direkta kostnader och de eventuella mer omfattande effekter som större cyberincidenter kan ha på den finansiella stabiliteten. Den administrativa bördan skulle minskas genom att överlappande **rapporteringskrav** tas bort. För några av de största bankerna skulle detta kunna ge besparingar på mellan 40 och 100 miljoner euro per år. Direkt rapportering skulle också öka tillsynsmyndigheternas kunskaper om IKT-incidenter. **Harmoniserade testmetoder** skulle leda till att okända sårbarheter och risker upptäcks i högre grad. Detta skulle också minska kostnaderna, särskilt för gränsöverskridande företag. För de 44 största gränsöverskridande bankerna skulle t.ex. de totala förväntade fördelarna med en gemensam testmetod kunna ligga på mellan 11 och 88 miljoner euro. Genom att en samstämmig uppsättning regler införs för riskhantering i samband med **tredjepartsleverantörer av IKT-tjänster** skulle de finansiella företagen få mer kontroll över hur tredjepartsleverantörer följer regelverket, vilket skulle kunna underlätta för tillsynsmyndigheterna. Tillsynen av IKT-tredjepartsleverantörer skulle också ge tillsynsmässiga fördelar. Sammantaget leder det rekommenderade alternativet till mer omfattande samhällsfördelar tack vare 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 ge upphov till både engångskostnader och återkommande kostnader. De förstnämnda kostnaderna beror på investeringar i it-system och är svåra att kvantifiera med tanke med tanke på att företagens tidigare system har olika status. I avsaknad av regleringsåtgärder har vissa finansiella företag redan gjort betydande investeringar i IKT-system. Det innebär att kostnaderna för att genomföra detta förslag sannolikt kommer att bli låga för större finansiella företag. Kostnaderna förväntas bli lägre även för mindre företag, eftersom de skulle omfattas av mindre stränga åtgärder som står i proportion till deras lägre risk. När det gäller testning har de europeiska tillsynsmyndigheterna uppskattat att kostnaderna för hotstyrd penetrationstestning ligger på mellan 0,1 % och 0,3 % av de berörda företagens totala IKT-budget. Kostnaderna för incidentrapportering skulle minska drastiskt, eftersom det inte skulle finnas några överlappningar med rapporteringen om säkerhet i nätverks- och informationssystem. Tillsynsmyndigheterna kommer också att ådra sig vissa kostnader på grund av de ytterligare uppgifter som de skulle åta sig. För tillsynsmyndigheter som deltar i den direkta tillsynen över IKT-tredjepartsleverantörer kan den uppskattade ökningen av heltidsekvivalenter t.ex. förväntas uppgå till mellan 1 och 5 heltidsekvivalenter för den ledande myndigheten och omkring 0,25 heltidsekvivalenter för de deltagande myndigheterna. |
| **Hur påverkas företagen, särskilt små och medelstora företag och mikroföretag?**  |
| Det rekommenderade alternativet skulle omfatta alla finansiella företag för att öka den operativa motståndskraften i sektorn som helhet. Detta breda tillämpningsområde är viktigt med tanke på sammanlänkningen inom den finansiella sektorn och det motsvarande behovet av en sund övergripande operativ motståndskraft. Vid fastställandet av centrala krav inom de viktigaste insatsområdena skulle dock proportionalitetsprincipen tillämpas såväl mellan delsektorer som inom varje delsektor. Därvid skulle hänsyn bl.a. tas till skillnader i affärsmodeller, storlek, riskprofil, systemvikt osv. Bestämmelser om incidentrapportering och testning skulle t.ex. vara mindre stränga för mindre finansiella företag.  |
| **Påverkas medlemsstaternas budgetar** **och förvaltningar i betydande grad?**  |
| Nej. Den ytterligare tillsynen kan, som visats ovan, kräva en begränsad grad av ytterligare tillsynsresurser, som helt eller delvis kan täckas av offentliga budgetar (om tillsynsavgifter tas ut).  |
| **Uppstår andra betydande konsekvenser?**  |
| De socioekonomiska konsekvenserna av covid-19-pandemin illustrerar de digitala finansmarknadernas avgörande karaktär och deras operativa motståndskraft. Det rekommenderade alternativet skulle utgöra en stabil grund för att hantera den digitala omvandlingen genom att säkerställa att den inre marknaden för finansiella tjänster, inbegripet inom bank- och kapitalmarknadsunionen, är operativt motståndskraftig, på grundval av en gemensam uppsättning regler och krav för att skapa säkerhet, prestanda, stabilitet och lika villkor. Detta kommer också att stärka Europas ställning som finansiell och digital ledare i världen, ett mål som kommissionen fastställde i sitt meddelande ”Att forma Europas digitala framtid”.  |
| **D. Uppföljning** |
| **När kommer åtgärderna att ses över?**  |
| Den första översynen skulle äga rum tre år efter det att rättsakten trätt i kraft. Kommissionen skulle lägga fram en rapport om sin översyn för Europaparlamentet och rådet. Översynen skulle kunna stödjas av ett offentligt samråd, studier, expertdiskussioner, enkäter och workshoppar, beroende på vad som är lämpligt.  |