Europeiska unionens råd

Bryssel den 24 september 2020
(OR. en)

11051/20

Interinstitutionellt ärende:
2020/0266(COD)

EF 228
ECOFIN 846
TELECOM 159
CYBER 168
IA 61
CODEC 871

FÖRSLAG

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:	COM(2020) 595 final
Ärende:	Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014

För delegationerna bifogas dokument – COM(2020) 595 final.

Bilaga: COM(2020) 595 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014

(Text av betydelse för EES)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

- Motiv och syfte med förslaget

Detta förslag ingår i paketet för digitalisering av finanssektorn, som är ett åtgärdspaket för att ytterligare möjliggöra och stödja den digitala finanssektorns potential när det gäller innovation och konkurrens och samtidigt minska riskerna. Det ligger i linje med kommissionens prioriteringar att rusta Europa för den digitala tidsåldern och att bygga upp en framtidssäkrad ekonomi för människor. I paketet för digitalisering av finanssektorn ingår en ny strategi för digitalisering av finanssektorn inom EU[1] vars syfte är att se till att EU tar till sig den digitala revolutionen och driver den med innovativa europeiska företag i täten, så att fördelarna med en digital finanssektor blir tillgängliga för europeiska konsumenter och företag. Utöver detta förslag innehåller paketet också ett förslag till förordning om marknader för kryptotillgångar[2], ett förslag till förordning om ett pilotsystem för marknadsinfrastruktur för distribuerad databasteknik (DLT)[3] och ett förslag till direktiv för att förtydliga eller ändra vissa relaterade EU-regler för finansiella tjänster[4]. Digitalisering och operativ motståndskraft inom finanssektorn är två sidor av samma mynt. Digital teknik eller informations- och kommunikationsteknik (IKT) ger upphov till både möjligheter och risker. Dessa måste förstås och hanteras väl, särskilt i tider av stress.

Beslutsfattare och tillsynsmyndigheter har därför i allt högre grad fokuserat på risker som härrör från IKT-beroende. De har framför allt försökt stärka företagens motståndskraft genom att fastställa standarder och samordna reglerings- eller tillsynsarbetet. Detta arbete har utförts på både internationell och europeisk nivå, både inom olika branscher och för ett antal specifika sektorer, däribland finansiella tjänster.

IKT-risker fortsätter dock att utgöra en utmaning för den operativa motståndskraften, prestandan och stabiliteten i EU:s finansiella system. Den reform som följde på finanskrisen 2008 stärkte i första hand den finansiella motståndskraften[5] hos EU:s finanssektor och berörde endast indirekt IKT-risker på vissa områden, som en del av åtgärderna för att hantera operativa risker mer generellt.

Även om ändringarna av EU:s lagstiftning om finansiella tjänster efter krisen ledde till att det infördes ett enhetligt regelverk som reglerar stora delar av de finansiella risker som är förknippade med finansiella tjänster, togs inget helhetsgrepp om den digitala operativa motståndskraften. De åtgärder som vidtogs med avseende på de sistnämnda kännetecknades av ett antal särdrag som begränsade deras effektivitet. Till exempel utformades de ofta som minimidirektiv för harmonisering eller principbaserade förordningar, vilket gav stort utrymme

---

1 Meddelande från kommissionen till Europaparlamentet, Europeiska rådet, rådet, Europeiska centralbanken, Europeiska ekonomiska och sociala kommittén och Regionkommittén om en strategi för digital finansiering i EU, 23 september 2020, COM(2020) 591.

2 Förslag till Europaparlamentets och rådets förordning om marknader för kryptotillgångar och om ändring av direktiv (EU) 2019/1937, COM(2020) 593.

3 Förslag till Europaparlamentets och rådets förordning om en pilotordning för marknadsinfrastrukturer som bygger på teknik för distribuerade liggare, COM(2020) 594.

4 Förslag till Europaparlamentets och rådets direktiv om ändring av direktiven 2006/43/EG, 2009/65/EG, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 och EU/2016/2341, COM(2020) 596.

5 De olika åtgärder som har vidtagits syftade i grunden till att öka de finansiella enheternas kapitalresurser och likviditet samt att minska marknads- och kreditriskerna.

för olika tillvägagångssätt på den inre marknaden. Dessutom har IKT-risker endast uppmärksammats i begränsad eller ofullständig grad när det gäller täckningen av operativa risker. Slutligen har dessa åtgärder varierande utformning i den sektorsspecifika lagstiftningen om finansiella tjänster. Åtgärden på unionsnivå motsvarade således inte helt det som europeiska finansiella enheter behövde för att hantera operativa risker på ett sätt som gav dem förmåga att stå emot, reagera på och återhämta sig från effekterna av IKT-incidenter. Den gav inte heller de finansiella tillsynsmyndigheterna de mest ändamålsenliga verktygen för att fullgöra sina uppdrag att förhindra finansiell instabilitet till följd av att dessa IKT-risker materialiserades.

Avsaknaden av detaljerade och heltäckande regler om digital operativ motståndskraft på EU-nivå har lett till en mängd nationella lagstiftningsinitiativ (t.ex. om testning av digital operativ motståndskraft) och tillsynsstrategier (t.ex. hantering av beroende av tredje parter inom IKT-sektorn). Åtgärder på medlemsstatsnivå har dock endast en begränsad effekt med tanke på IKT-riskernas gränsöverskridande karaktär. Dessutom har de icke samordnade nationella initiativen lett till överlappningar, inkonsekvenser, överlappande krav, höga administrativa kostnader och efterlevnadskostnader – särskilt för gränsöverskridande finansiella enheter – eller till att IKT-risker förblir oupptäckta och därmed oåtgärdade. Denna situation splittrar den inre marknaden, undergräver stabiliteten och integriteten i EU:s finanssektor och äventyrar skyddet av konsumenter och investerare.

Det är därför nödvändigt att införa en detaljerad och heltäckande ram för digital operativ motståndskraft för finansiella enheter i EU. Denna ram kommer att leda till att den digitala riskhanteringsdimensionen fördjupas i det enhetliga regelverket. Framför allt kommer den att innebära förbättring och effektivisering av de finansiella enheternas hantering av IKT-risker, införande av en grundlig testning av IKT-system, ökad medvetenhet hos tillsynsmyndigheterna om cyberrisker och IKT-relaterade incidenter som finansiella enheter ställs inför och ge finansiella tillsynsmyndigheter befogenhet att övervaka risker som härrör från finansiella enheters beroende av tredjepartsleverantörer av IKT-tjänster. Förslaget kommer att skapa en enhetlig incidentrapporteringsmekanism som kommer att bidra till att minska de administrativa bördorna för finansiella enheter och stärka tillsynens effektivitet.

- Förenlighet med befintliga bestämmelser inom området

Detta förslag är en del av det bredare arbete som pågår på europeisk och internationell nivå för att stärka cybersäkerheten inom finansiella tjänster och ta itu med bredare operativa risker.[6]

Det är också ett svar på 2019 års gemensamma tekniska råd[7] från de europeiska tillsynsmyndigheterna (ESA-myndigheterna), där man efterlyste en mer enhetlig strategi för att hantera IKT-risker inom finanssektorn och rekommenderade kommissionen att på ett proportionerligt sätt stärka den digitala operativa motståndskraften inom sektorn för finansiella tjänster genom ett sektorsspecifikt EU-initiativ. De europeiska tillsynsmyndigheternas råd var ett svar på kommissionens handlingsplan för fintech från 2018.[8]

- Förenlighet med unionens politik inom andra områden

---

6 Baselkommittén för banktillsyn, *Cyber-resilience: Range of practices*, december 2018 och *Principles for sound management of operational risk (PSMOR)*, oktober 2014.

7 Gemensam rådgivning från de europeiska tillsynsmyndigheterna till Europeiska kommissionen om behovet av lagstiftningsförbättringar avseende IKT-riskhanteringskrav inom EU:s finanssektor, JC 2019 26 (2019).

8 Europeiska kommissionen, *Handlingsplanen för fintech* , COM(2018) 0109 final.

Som ordförande Ursula von der Leyen angav i sina politiska riktlinjer[9] och som anges i meddelandet ”Att forma EU:s digitala framtid”[10], är det av avgörande betydelse för Europa att dra nytta av den digitala tidsålderns alla fördelar och att stärka sin industri- och innovationskapacitet, inom säkra och etiska gränser. I EU-strategin för data[11] anges fyra pelare – dataskydd, grundläggande rättigheter, säkerhet och cybersäkerhet – som viktiga förutsättningar för ett samhälle som har inflytande över dataanvändningen. På senare tid har Europaparlamentet arbetat med ett betänkande om digital finansiering, där det bland annat efterlyser en gemensam strategi för cyberresiliens inom finanssektorn[12]. En rättslig ram som stärker den digitala operativa motståndskraften hos EU:s finansiella enheter är förenlig med dessa politiska mål. Förslaget skulle också stödja strategier för återhämtning efter coronaviruset, eftersom det skulle säkerställa att ökat beroende av digital finansiering går hand i hand med operativ motståndskraft.

Initiativet skulle innebära att fördelarna med den övergripande ramen för cybersäkerhet (t.ex. direktivet om säkerhet i nätverks- och informationssystem) kan bibehållas, genom att finanssektorn fortsätter att omfattas av dess tillämpningsområde. Finanssektorn skulle fortsätta att vara nära knuten till samarbetsorganet för säkerhet i nätverks- och informationssystem och de finansiella tillsynsmyndigheterna skulle kunna utbyta relevant information inom det befintliga ekosystemet för nätverks- och informationssäkerhet. Initiativet skulle vara förenligt med direktivet om europeisk kritisk infrastruktur, som för närvarande genomgår en översyn för att förbättra skyddet av och motståndskraften hos kritisk infrastruktur mot icke cyberrelaterade hot. Slutligen ligger detta förslag helt i linje med strategin för säkerhetsunionen[13], där det efterlystes ett initiativ om den digitala operativa motståndskraften för finanssektorn med tanke på dess stora beroende av IKT-tjänster och dess stora sårbarhet för it-attacker.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- Rättslig grund

Den rättsliga grunden för detta förslag till förordning är artikel 114 i EUF-fördraget.

Förslaget syftar till att undanröja hinder för upprättandet av den inre marknaden för finansiella tjänster och förbättra dess funktion genom att se till att de tillämpliga bestämmelserna för riskhantering, rapportering, testning inom IKT-området och IKT-risker i samband med tredje parter är helt harmoniserade. De nuvarande skillnaderna inom detta område, både på lagstiftnings- och tillsynsnivå, samt på nationell nivå och EU-nivå, utgör hinder för den inre marknaden för finansiella tjänster, eftersom finansiella enheter som bedriver

---

9 Ordförande Ursula von der Leyen, *Politiska riktlinjer för nästa Europeiska kommission, 2019–2024*, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_sv.pdf.

10 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *Att forma EU:s digitala framtid*, COM(2020) 67 final.

11 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén, *En EU-strategi för data*, COM(2020) 66 final.

12 *Betänkande med rekommendationer till kommissionen om digitala finanser: nya risker med kryptotillgångar – reglerings- och tillsynsutmaningar när det gäller finansiella tjänster, institut och marknader* (2020/2034 (INL)), https://www.europarl.europa.eu/doceo/document/A-9-2020-0161_SV.html

13 Meddelande från kommissionen till Europaparlamentet, Europeiska rådet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *Strategi för EU:s säkerhetsunion*, COM(2020) 605 final.

gränsöverskridande verksamhet ställs inför olika eller överlappande lagstadgade krav eller förväntningar på tillsynsområdet som kan hindra utövandet av deras etableringsfrihet och friheten att tillhandahålla tjänster. Olika regler snedvrider också konkurrensen mellan samma typ av finansiella enheter i olika medlemsstater. På områden där harmonisering saknas eller har genomförts delvis eller i begränsad omfattning kan dessutom utvecklingen av skiljaktiga nationella regler eller strategier, som redan har trätt i kraft eller håller på att antas och genomföras på nationell nivå, fungera som ett hinder för friheterna på den inre marknaden för finansiella tjänster. Detta är särskilt fallet när det gäller regelverk för digitala operativa tester och tillsyn över kritiska tredjepartsleverantörer av IKT-tjänster.

Eftersom förslaget påverkar flera av Europaparlamentets och rådets direktiv som har antagits på grundval av artikel 53.1 i EUF-fördraget antas samtidigt också ett förslag till direktiv för att återspegla de nödvändiga ändringarna av dessa direktiv.

- Subsidiaritetsprincipen

En hög grad av sammanlänkning mellan finansiella tjänster, en betydande gränsöverskridande verksamhet för finansiella enheter och ett omfattande beroende inom hela finanssektorn av tredjepartsleverantörer av IKT-tjänster innebär att det är nödvändigt att möjliggöra en stark digital operativ motståndskraft och att detta är en fråga av gemensamt intresse för att bibehålla sunda finansmarknader i EU. Skillnader till följd av ojämna eller ofullständiga system, överlappningar eller flera krav som gäller för samma finansiella enheter som bedriver gränsöverskridande verksamhet eller innehar flera tillstånd[14] på hela den inre marknaden kan endast hanteras effektivt på unionsnivå.

Genom detta förslag harmoniseras den digitala operativa komponenten i en djupt integrerad och sammanlänkad sektor som redan omfattas av en enhetlig uppsättning regler och tillsyn på de flesta andra nyckelområden. När det gäller frågor som IKT-relaterad incidentrapportering kan endast harmoniserade unionsregler minska den administrativa bördan och de ekonomiska kostnaderna i samband med rapportering av samma IKT-relaterade incident till olika unionsmyndigheter och nationella myndigheter. EU-åtgärder behövs också för att underlätta ömsesidigt erkännande av avancerade testresultat för digital operativ motståndskraft för enheter som bedriver gränsöverskridande verksamhet, vilka i avsaknad av unionsregler omfattas av eller kan bli föremål för olika regelverk i olika medlemsstater. Endast åtgärder på unionsnivå kan avhjälpa de skillnader i testmetoder som medlemsstaterna har infört. EU-omfattande åtgärder behövs också för att ta itu med bristen på lämpliga tillsynsbefogenheter för att övervaka risker som härrör från tredjepartsleverantörer av IKT-tjänster, inbegripet koncentrations- och spridningsrisker för EU:s finanssektor.

- Proportionalitetsprincipen

De föreslagna bestämmelserna går inte utöver vad som är nödvändigt för att uppnå målen i förslaget. De täcker endast de aspekter som medlemsstaterna inte kan uppnå på egen hand och där den administrativa bördan och kostnaderna står i proportion till de specifika och allmänna mål som ska uppnås.

När det gäller omfattning och intensitet har proportionaliteten utformats genom kvalitativa och kvantitativa bedömningskriterier. Syftet är att se till att de nya reglerna täcker alla

[14] Samma finansiella enhet kan ha tillstånd för bankverksamhet, värdepappersföretag och betalningsinstitut, som vart och ett har utfärdats av olika tillsynsmyndigheter i en eller flera medlemsstater.

finansiella enheter samtidigt som de anpassas till risker och behov med hänsyn till enheternas särskilda egenskaper i fråga om storlek och affärsprofiler. Även reglerna om IKT-riskhantering, testning av digital motståndskraft, rapportering av större IKT-relaterade incidenter och tillsyn av kritiska tredjepartsleverantörer av IKT-tjänster är proportionerliga.

- Val av instrument

De åtgärder som krävs för att reglera IKT-riskhantering, IKT-relaterad incidentrapportering, testning och tillsyn av kritiska tredjepartsleverantörer av IKT-tjänster måste ingå i en förordning för att säkerställa att de detaljerade kraven blir effektivt och direkt tillämpliga på ett enhetligt sätt, utan att det påverkar proportionalitetsprincipen och de särskilda regler som föreskrivs i denna förordning. Konsekvens i hanteringen av digitala operativa risker bidrar till att öka förtroendet för det finansiella systemet och upprätthåller dess stabilitet. Eftersom användningen av en förordning bidrar till att minska lagstiftningens komplexitet, främjar konvergens i tillsynen och ökar rättssäkerheten, bidrar denna förordning också till att begränsa de finansiella enheternas efterlevnadskostnader, särskilt för dem som bedriver gränsöverskridande verksamhet, vilket i sin tur skulle bidra till att undanröja snedvridningar av konkurrensen.

Genom denna förordning undanröjs också skillnader i lagstiftning och olika nationella reglerings- eller tillsynsstrategier för IKT-risker, vilket innebär att hinder avlägsnas för den inre marknaden för finansiella tjänster, särskilt för ett smidigt utövande av etableringsfriheten och tillhandahållandet av tjänster för finansiella enheter med gränsöverskridande närvaro.

Slutligen har det enhetliga regelverket till största delen utvecklats genom förordningar, och samma val av rättsligt instrument bör användas för att uppdatera regelverket i fråga om digital operativ motståndskraft.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning

Ingen unionslagstiftning om finansiella tjänster har hittills varit inriktad på operativ motståndskraft och ingen har på ett heltäckande sätt hanterat de risker som uppstår till följd av digitaliseringen, inte ens den lagstiftning som mer generellt behandlar den operativa riskdimensionen med IKT-risk som en delkomponent. Unionens åtgärder hittills har bidragit till att möta de behov och problem som fanns efter finanskrisen 2008: kreditinstituten var inte tillräckligt kapitaliserade, finansmarknaderna var inte tillräckligt integrerade och harmoniseringen fram till dess hade varit minimal. IKT-risker ansågs inte vara en prioriterad fråga, och till följd av detta har de rättsliga ramarna för de olika finansiella delsektorerna utvecklats på ett osamordnat sätt. Ändå har unionens åtgärder uppnått målen att säkerställa finansiell stabilitet och införa en enhetlig uppsättning harmoniserade tillsyns- och marknadsuppföranderegler som är tillämpliga på finansiella enheter i hela EU. Eftersom de faktorer som drev unionens lagstiftningsåtgärder tidigare inte möjliggjorde specifika eller heltäckande regler för att hantera den utbredda användningen av digital teknik och de därav följande riskerna inom finanssektorn, verkar det vara svårt att göra en uttrycklig utvärdering. En underförstådd utvärdering och efterföljande ändringar av lagstiftningen återspeglas i varje pelare i denna förordning.

- Samråd med berörda parter

Kommissionen har samrått med berörda parter under hela processen när detta förslag har utarbetats. I synnerhet har den gjort följande:

i) Kommissionen genomförde ett särskilt öppet offentligt samråd (den 19 december 2019–19 mars 2020).[15]

ii) Kommissionen rådfrågade allmänheten genom en inledande konsekvensbedömning (den 19 december 2019–16 januari 2020).[16]

iii) Kommissionens avdelningar har samrått med medlemsstaternas experter i expertgruppen för bankverksamhet, betaltjänster och försäkring (EGBPI) vid två tillfällen (den 18 maj 2020 och den 16 juli 2020).[17]

iv) Kommissionens avdelningar höll ett särskilt webbseminarium om digital operativ motståndskraft, som en del av utåtriktade 2020-evenemang om digital finansiering (den 19 maj 2020).

Syftet med det offentliga samrådet var att informera kommissionen om utvecklingen av en potentiell sektorsövergripande ram för digital operativ motståndskraft i EU på området finansiella tjänster. Svaren visade på ett brett stöd för införandet av en särskild ram med åtgärder inriktade på de fyra områden som samrådet gällde, samtidigt som man betonade behovet av att säkerställa proportionalitet och noggrant behandla och förklara samspelet med de övergripande reglerna i direktivet om säkerhet i nätverks- och informationssystem. Kommissionen fick in två svar på den inledande konsekvensbedömningen, där de svarande tog upp specifika aspekter som rör deras verksamhetsområde.

Medlemsstaterna uttryckte vid EGBPI-mötet den 18 maj 2020 stort stöd för att stärka finanssektorns digitala operativa motståndskraft genom de åtgärder som planeras i de fyra delar som kommissionen beskriver. Medlemsstaterna betonade också behovet av en tydlig koppling mellan de nya reglerna och reglerna om operativa risker (inom EU:s lagstiftning om finansiella tjänster) och de övergripande bestämmelserna om cybersäkerhet (direktivet om säkerhet i nätverks- och informationssystem). Under det andra mötet betonade vissa medlemsstater behovet av att säkerställa proportionalitet och beakta den särskilda situationen för små företag eller dotterbolag till större koncerner samt behovet av att ha ett starkt mandat för de nationella behöriga myndigheter som är involverade i tillsynen.

Förslaget bygger också på och integrerar återkoppling från möten med berörda parter och EU:s myndigheter och institutioner. Berörda parter, inbegripet tredjepartsleverantörer av IKT-tjänster, har överlag varit positiva. En analys av den mottagna återkopplingen visar att man bör bevara proportionaliteten och följa en princip- och riskbaserad metod vid utformningen av reglerna. På den institutionella sidan kom de viktigaste bidragen från Europeiska systemrisknämnden (ESRB), de europeiska tillsynsmyndigheterna, Europeiska unionens cybersäkerhetsbyrå (Enisa) och Europeiska centralbanken (ECB) samt medlemsstaternas behöriga myndigheter.

---

15 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

16 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

17 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

- Insamling och användning av sakkunnigutlåtanden

Vid utarbetandet av detta förslag förlitade sig kommissionen på kvalitativa och kvantitativa bevis som samlats in från erkända källor, däribland de två gemensamma tekniska råden från de europeiska tillsynsmyndigheterna. Detta har kompletterats med konfidentiella synpunkter och offentligt tillgängliga rapporter från tillsynsmyndigheter, internationella standardiseringsorgan och ledande forskningsinstitut samt kvantitativa och kvalitativa synpunkter från identifierade berörda parter inom hela den globala finanssektorn.

- Konsekvensbedömning

Detta förslag åtföljs av en konsekvensbedömning[18] som lades fram för nämnden för lagstiftningskontroll den 29 april 2020 och godkändes den 29 maj 2020. Nämnden rekommenderade förbättringar på vissa områden för att uppnå följande syften: i) Lämna mer information om hur proportionaliteten kan garanteras. ii) Bättre belysa i vilken utsträckning det rekommenderade alternativet skiljer sig från de europeiska tillsynsmyndigheternas gemensamma tekniska rådgivning, och varför det alternativet är det bästa. iii) Ytterligare betona hur förslaget samverkar med befintlig EU-lagstiftning, bl.a. med de regler som för närvarande är under översyn. Konsekvensbedömningen anpassades för att ta itu med dessa punkter och tog också upp nämndens mer detaljerade kommentarer.

Kommissionen övervägde ett antal politiska alternativ för att utveckla ett regelverk för digital operativ motståndskraft:

- ”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: Förstärkning av kapitalbuffertar: ytterligare kapitalbuffertar skulle införas för att öka de finansiella enheternas förmåga att absorbera förluster som skulle kunna uppstå på grund av bristande digital operativ motståndskraft.
- Alternativ 2: Införande av en rättsakt om digital operativ motståndskraft: möjliggöra en heltäckande ram på EU-nivå med konsekventa regler som tillgodoser behoven av digital operativ motståndskraft hos alla reglerade finansiella enheter och inrätta en tillsynsram för kritiska tredjepartsleverantörer inom IKT.
- Alternativ 3: en rättsakt om digital operativ motståndskraft för finansiella tjänster i kombination med centraliserad tillsyn av kritiska tredjepartsleverantörer av IKT-tjänster: utöver en rättsakt om digital operativ motståndskraft (alternativ 2) skulle en ny myndighet inrättas för att övervaka tillhandahållandet av tjänster från tredjepartsleverantörer av IKT-tjänster.

Det andra alternativet valdes, eftersom det innebär att de flesta av de avsedda målen kommer att uppnås på ett sätt som är ändamålsenligt, effektivt och förenligt med annan unionspolitik. De flesta berörda parter föredrar också detta alternativ.

[18] Arbetsdokument från kommissionens avdelningar – Konsekvensbedömningsrapport – följedokument till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014, SWD(2020) 198, 24.9.2020.

Det valda alternativet skulle ge upphov till både engångskostnader och återkommande kostnader[19]. Engångskostnaderna beror främst på investeringar i it-system och är därför svåra att kvantifiera med tanke på de olika företagens komplexa it-landskap och i synnerhet deras befintliga it-system. Trots detta kommer dessa kostnader sannolikt att vara begränsade för stora företag, med tanke på de betydande IKT-investeringar som de redan har gjort. Kostnaderna förväntas också vara begränsade för mindre företag, eftersom proportionella åtgärder skulle tillämpas med tanke på deras lägre risk.

Det valda alternativet skulle få positiva effekter för små och medelstora företag som är verksamma inom sektorn för finansiella tjänster när det gäller ekonomiska, sociala och miljömässiga konsekvenser. Förslaget kommer att skapa klarhet för små och medelstora företag om vilka regler som gäller, vilket kommer att minska efterlevnadskostnaderna.

De viktigaste sociala konsekvenserna av det valda alternativet skulle påverka konsumenter och investerare. Högre nivåer av digital operativ motståndskraft i EU:s finansiella system skulle minska antalet incidenter och deras genomsnittliga kostnader. Samhället som helhet skulle gynnas av det ökade förtroendet för sektorn för finansiella tjänster.

När det gäller miljöpåverkan skulle det valda alternativet slutligen uppmuntra en ökad användning av den senaste generationen IKT-infrastrukturer och IKT-tjänster, som förväntas bli miljömässigt mer hållbara.

- Lagstiftningens ändamålsenlighet och förenkling

Avskaffandet av överlappande IKT-relaterade incidentrapporteringskrav skulle minska den administrativa bördan och därmed sammanhängande kostnader. Dessutom kommer harmoniserade tester av den digitala operativa motståndskraften med ömsesidigt erkännande på hela den inre marknaden att minska kostnaderna, särskilt för gränsöverskridande företag som annars skulle behöva genomgå flera tester i medlemsstaterna[20].

- Grundläggande rättigheter

EU har åtagit sig att säkerställa en hög skyddsnivå för de grundläggande rättigheterna. Alla frivilliga arrangemang för informationsutbyte mellan finansiella enheter som denna förordning främjar skulle genomföras i betrodda miljöer med full respekt för unionens dataskyddsregler, särskilt Europaparlamentets och rådets förordning (EU) 2016/679[21], särskilt när behandling av personuppgifter är nödvändig för ändamål som rör berättigade intressen hos den registeransvarige.

4. BUDGETKONSEKVENSER

Eftersom det i den nuvarande förordningen föreskrivs en förstärkt roll för de europeiska tillsynsmyndigheterna genom de befogenheter som de tilldelas för att på lämpligt sätt övervaka kritiska tredjepartsleverantörer av IKT-tjänster, skulle förslaget när det gäller budgetkonsekvenser innebära användning av ökade resurser, särskilt för att fullgöra

---

19 *Ibid, s. 89.*

20 *Ibid*.

21 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

tillsynsuppdragen (t.ex. kontroller och revisioner på plats och online) och användning av personal med särskild sakkunskap inom IKT-säkerhet.

Omfattningen och fördelningen av dessa kostnader kommer att bero på omfattningen av de nya tillsynsbefogenheterna och de (exakta) uppgifter som ska utföras av de europeiska tillsynsmyndigheterna. När det gäller tillhandahållandet av nya personalresurser kommer EBA, Esma och Eiopa att behöva totalt 18 heltidsanställda (heltidsekvivalenter) – 6 heltidsekvivalenter för varje myndighet – när de olika bestämmelserna i förslaget träder i kraft (uppskattningsvis 15,71 miljoner euro för perioden 2022–2027). De europeiska tillsynsmyndigheterna kommer också att ådra sig ytterligare it-kostnader, kostnader för tjänsteresor för kontroller på plats och översättning (uppskattningsvis 12 miljoner euro för perioden 2022–2027) samt andra administrativa utgifter (uppskattningsvis 2,48 miljoner euro för perioden 2022–2027). Den beräknade totala kostnaden uppskattas därför till cirka 30,19 miljoner euro för perioden 2022–2027.

Det bör också noteras att även om den personalstyrka (t.ex. ny personal och andra utgifter i samband med de nya uppgifterna) som krävs för direkt tillsyn över tiden kommer att bero på utvecklingen i antalet och storleken på de kritiska tredjepartsleverantörer av IKT-tjänster som ska övervakas, kommer respektive utgifter att finansieras helt genom avgifter som tas ut av dessa marknadsaktörer. Därför förväntas inga konsekvenser för EU:s budgetanslag (utom för ytterligare personal), eftersom dessa kostnader kommer att finansieras helt genom avgifter.

De ekonomiska och budgetmässiga konsekvenserna av detta förslag förklaras i detalj i den finansieringsöversikt som åtföljer detta förslag.

5. ÖVRIGA INSLAG

- Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering

Förslaget innehåller en allmän plan för övervakning och utvärdering av effekterna på de specifika målen, enligt vilken kommissionen ska göra en översyn minst tre år efter ikraftträdandet och rapportera till Europaparlamentet och rådet om sina viktigaste slutsatser.

Översynen ska genomföras i enlighet med kommissionens riktlinjer för bättre lagstiftning.

- Ingående redogörelse för de specifika bestämmelserna i förslaget

Förslaget är uppbyggt kring flera viktiga politikområden som utgör centrala ömsesidigt samverkande pelare och som genom överenskommelser har inkluderats i europeiska och internationella riktlinjer och bästa praxis som syftar till att förbättra finanssektorns cyberresiliens och operativa motståndskraft.

Förordningens tillämpningsområde och proportionalitetsprincipens tillämpning på de åtgärder som krävs (artikel 2)

För att säkerställa enhetlighet i fråga om de IKT-riskhanteringskrav som är tillämpliga på finanssektorn omfattar förordningen en rad finansiella enheter som regleras på unionsnivå, nämligen kreditinstitut, betalningsinstitut, institut för elektroniska pengar, värdepappersföretag, leverantörer av kryptotillgångstjänster, värdepapperscentraler, centrala motparter, handelsplatser, transaktionsregister, förvaltare av alternativa investeringsfonder och förvaltningsbolag, leverantörer av datarapporteringstjänster, försäkrings- och återförsäkringsföretag, försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet, tjänstepensionsinstitut,

kreditvärderingsinstitut, lagstadgade revisorer och revisionsföretag, administratörer av kritiska referensvärden och leverantörer av gräsrotsfinansieringstjänster.

En sådan täckning underlättar en enhetlig och samstämmig tillämpning av alla delar av riskhanteringen inom IKT-relaterade områden, samtidigt som lika villkor säkerställs för finansiella enheter när det gäller deras lagstadgade skyldigheter i fråga om IKT-risker. Samtidigt erkänns det i förordningen att det finns betydande skillnader mellan finansiella enheter i fråga om storlek, affärsprofiler och deras exponering för digital risk. Eftersom större finansiella enheter har mer resurser är det t.ex. enbart finansiella enheter som inte kan betraktas som mikroföretag som att inrätta komplexa styrformer, särskilda ledningsfunktioner, göra djupgående bedömningar efter större förändringar i nätverks- och informationssysteminfrastrukturer, regelbundet genomföra riskanalyser av befintliga IKT-system, utöka testningen av planer för driftskontinuitet och åtgärds- och återställningsplaner för att fånga upp övergångsscenarier mellan deras primära IKT-infrastruktur och reservanläggningar. Dessutom kommer endast finansiella enheter som har identifierats som betydande i samband med den avancerade testningen av digital motståndskraft att åläggas att utföra hotbaserade penetrationstester.

Trots denna breda omfattning är förordningen inte heltäckande. I synnerhet omfattar den inte systemoperatörer enligt definitionen i artikel 2 p i direktiv 98/26/EG[22] om slutgiltig avveckling i system för överföring av betalningar och värdepapper (nedan kallat *direktivet om slutgiltig avveckling*), och inte heller systemdeltagare, såvida inte en sådan deltagare själv är en finansiell enhet som regleras på unionsnivå och som sådan skulle omfattas av denna förordning i egen rätt (dvs. kreditinstitut, värdepappersföretag, central motpart). Det unionsregister över utsläppsrätter som drivs under kommissionens överinseende i enlighet med direktiv 2003/87/EG[23] faller också utanför tillämpningsområdet.

Genom dessa undantag från direktivet om slutgiltig avveckling går det att ta hänsyn till behovet av en ytterligare översyn av de rättsliga och politiska frågor som rör systemoperatörer och systemdeltagare i direktivet om slutgiltig avveckling och samtidigt beakta effekterna av de regelverk som för närvarande tillämpas på betalningssystem[24] som drivs av centralbanker. Eftersom dessa frågor kan beröra aspekter som skiljer sig från de frågor som omfattas av denna förordning kommer kommissionen att fortsätta att bedöma behovet och konsekvenserna av en ytterligare utvidgning av förordningens tillämpningsområde till enheter och IKT-infrastrukturer som för närvarande ligger utanför dess område.

Styrningsrelaterade krav (artikel 4)

Denna förordning är utformad för att förbättra anpassningen av de finansiella enheternas affärsstrategier och hur IKT-riskhanteringen genomförs. För detta ändamål kommer det att krävas att ledningsorganet bibehåller en avgörande och aktiv roll i styrningen av IKT-riskhanteringsramen och strävar efter att upprätthålla en sträng it-hygien. Ledningsorganets fulla ansvar för att hantera den finansiella enhetens IKT-risk kommer att utgöra en

---

22 Europaparlamentets och rådets direktiv 98/26/EG av den 19 maj 1998 om slutgiltig avveckling i system för överföring av betalningar och värdepapper (EGT L 166, 11.6.1998, s. 45).

23 Europaparlamentets och rådets direktiv 2003/87/EG av den 13 oktober 2003 om ett system för handel med utsläppsrätter för växthusgaser inom gemenskapen och om ändring av rådets direktiv 96/61/EG (EGT L 275 , 25.10.2003, s. 32).

24 Särskilt Europeiska centralbankens förordning (EU) nr 795/2014 av den 3 juli 2014 om krav på övervakning av systemviktiga betalningssystem.

övergripande princip som ytterligare omsätts i en uppsättning specifika krav, såsom tilldelning av tydliga roller och ansvarsområden för alla IKT-relaterade funktioner, ett kontinuerligt engagemang i kontrollen av övervakningen av IKT-riskhanteringen samt i alla godkännande- och kontrollprocesser och en lämplig fördelning av IKT-investeringar och IKT-utbildning.

Krav på IKT-riskhantering (artiklarna 5–14)

Den digitala operativa motståndskraften bygger på en uppsättning centrala principer och krav för IKT-riskhanteringsramen, i linje med de europeiska tillsynsmyndigheternas gemensamma tekniska råd. Dessa krav, som bygger på relevanta internationella, nationella och branschspecifika standarder, riktlinjer och rekommendationer, kretsar kring specifika funktioner inom IKT-riskhantering (identifiering, skydd och förebyggande, upptäckt, åtgärd och återställning, lärande och utveckling samt kommunikation). För att hålla jämna steg med ett snabbt föränderligt cyberhotlandskap måste finansiella enheter inrätta och upprätthålla motståndskraftiga IKT-system och IKT-verktyg som minimerar effekterna av IKT-risker, fortlöpande identifiera alla källor till IKT-risker, vidta skyddsåtgärder och förebyggande åtgärder, snabbt upptäcka onormal verksamhet, införa särskilda och heltäckande kontinuitetsplaner och katastrof- och återställningsplaner som en integrerad del i de operativa kontinuitetsplanerna. De sistnämnda komponenterna krävs för en snabb återställning efter IKT-relaterade incidenter, särskilt it-attacker, genom skadebegränsning och prioritering av ett säkert återupptagande av verksamheten. I förordningen i sig föreskrivs inte någon särskild standardisering, utan den baseras på europeiska och internationellt erkända tekniska standarder eller bästa branschpraxis, i den mån de är helt förenliga med tillsynsinstruktioner om användning och införlivande av sådana internationella standarder. Denna förordning omfattar även integritet, säkerhet och motståndskraft hos fysiska infrastrukturer och anläggningar som stöder användningen av teknik och relevanta IKT-relaterade processer och personer, som en del av det digitala fotavtrycket för en finansiell enhets verksamhet.

IKT-relaterad incidentrapportering (artiklarna 15–20)

Harmonisering och effektivisering av rapporteringen av IKT-relaterade incidenter uppnås genom, för det första, ett allmänt krav på att finansiella enheter ska inrätta och genomföra en förvaltningsprocess för att övervaka och registrera IKT-relaterade incidenter, följt av en skyldighet att klassificera dem på grundval av de kriterier som anges i förordningen och vidareutvecklas av de europeiska tillsynsmyndigheterna, och slutligen genom att väsentlighetströsklar specificeras. För det andra ska endast IKT-relaterade incidenter som bedöms vara allvarliga rapporteras till de behöriga myndigheterna. Rapporteringen bör behandlas med hjälp av en gemensam mall och enligt ett harmoniserat förfarande som utarbetas av de europeiska tillsynsmyndigheterna. De finansiella enheterna bör lämna in inledande rapporter, delrapporter och slutrapporter och informera sina användare och kunder om incidenten har påverkat eller kan påverka deras ekonomiska intressen. De behöriga myndigheterna bör lämna relevanta uppgifter om incidenterna till andra institut eller myndigheter: till de europeiska tillsynsmyndigheterna, ECB och de gemensamma kontaktpunkter som har utsetts enligt direktiv (EU) 2016/1148.

För att inleda en dialog mellan finansiella enheter och behöriga myndigheter som skulle bidra till att minimera effekterna och identifiera lämpliga åtgärder bör rapporteringen av större IKT-relaterade incidenter kompletteras med återkoppling och vägledning från tillsynsmyndigheterna.

Slutligen bör möjligheten till centralisering på unionsnivå av IKT-relaterad incidentrapportering undersökas ytterligare i en gemensam rapport från de europeiska tillsynsmyndigheterna, ECB och Enisa med en bedömning av möjligheten att inrätta en

gemensamt EU-knutpunkt för finansiella enheters rapportering av större IKT-relaterade incidenter.

Testning av digital operativ motståndskraft (artiklarna 21–24)

Den kapacitet och de funktioner som ingår i IKT-riskhanteringsramen måste regelbundet testas med avseende på beredskap och identifiering av svagheter, brister eller luckor samt ett snabbt genomförande av korrigerande åtgärder. Denna förordning möjliggör en proportionell tillämpning av testkraven för digital operativ motståndskraft beroende på de finansiella enheternas storlek, affärsverksamhet och riskprofiler: alla enheter bör visserligen testa IKT-verktyg och IKT-system, men endast de som har identifierats som betydande och cybermogna av behöriga myndigheter (på grundval av kriterier i denna förordning och vidareutvecklade av de europeiska tillsynsmyndigheterna) bör åläggas att utföra avancerad testning som bygger på hotstyrda penetrationstester. I denna förordning fastställs också krav på testare och erkännande av resultat av hotstyrda penetrationstester i hela unionen för finansiella enheter som är verksamma i flera medlemsstater.

IKT-tredjepartsrisker (artiklarna 25–39)

Förordningen är utformad för att säkerställa en sund övervakning av IKT-tredjepartsrisker. Detta mål ska i första hand att uppnås genom att man respekterar de principbaserade regler som gäller för finansiella enheters övervakning av risker som uppstår genom tredjepartsleverantörer av IKT-tjänster. För det andra innebär förordningen en harmonisering av de viktigaste delarna i tjänster från och förhållandet till IKT-tredjepartsleverantörer. I dessa delar ingår minimiaspekter som anses avgörande för att den finansiella enheten ska kunna övervaka IKT-tredjepartsrisk i samband med slutande, fullgörande och uppsägning av avtal och även efter det att avtalet har upphört att gälla.

Framför allt kommer det att krävas att de avtal som reglerar detta förhållande ska innehålla en heltäckande beskrivning av tjänsterna, angivande av var uppgifterna ska behandlas, beskrivningar av fullständig servicenivå åtföljda av kvantitativa och kvalitativa prestationsmål, relevanta bestämmelser om åtkomstmöjlighet, tillgänglighet, integritet, säkerhet och skydd av personuppgifter samt garantier för åtkomst, återställning och återlämnande vid fel hos tredjepartsleverantörer av IKT-tjänster, uppsägningsperioder och rapporteringsskyldigheter för tredjepartsleverantörer av IKT-tjänster, rätt till åtkomst, kontroll och revision av den finansiella enheten eller en utsedd tredjepart, tydliga uppsägningsrätter och tydliga uppsägningsförfaranden. Eftersom vissa av dessa avtalskomponenter kan standardiseras förordas i förordningen dessutom frivillig användning av standardavtalsklausuler som kommissionen ska utarbeta för användning i molntjänster.

Slutligen syftar förordningen till att främja konvergens när det gäller tillsynsstrategier för IKT-tredjepartsrisker i finanssektorn genom att kritiska tredjepartsleverantörer av IKT-tjänster omfattas av unionens tillsynsram. Genom en ny harmoniserad rättslig ram får den europeiska tillsynsmyndighet som har utsetts som ledande tillsynsmyndighet för varje sådan kritisk tredjepartsleverantör av IKT-tjänster befogenheter att se till att leverantörer av tekniska tjänster som har avgörande betydelse för den finansiella sektorns funktion övervakas på ett adekvat sätt på europeisk nivå. Den tillsynsram som föreskrivs i denna förordning bygger på den befintliga institutionella strukturen på området finansiella tjänster, där de europeiska tillsynsmyndigheternas gemensamma kommitté säkerställer sektorsövergripande samordning i alla frågor som rör IKT-risker, i enlighet med sina uppgifter i fråga om cybersäkerhet, med stöd av den relevanta underkommitté (tillsynsforum) som utför förberedande arbete inför enskilda beslut och kollektiva rekommendationer till kritiska tredjepartsleverantörer.

Informationsutbyte (artikel 40)

För att öka medvetenheten om IKT-risker, minimera deras spridning, stödja finansiella enheters försvarsförmåga och metoder för att upptäcka hot, kommer förordningen att göra det möjligt för finansiella enheter att göra överenskommelser om att utbyta information och underrättelser om it-hot med varandra.

2020/0266 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska centralbankens yttrande,[25]

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[26],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) I den digitala tidsåldern stöder informations- och kommunikationstekniken (IKT) komplexa system som används för dagliga samhällsaktiviteter. Den får våra ekonomier att fungera inom viktiga sektorer, däribland finanssektorn, och förbättrar den inre marknadens funktion. Ökad digitalisering och sammanlänkning ökar också IKT-riskerna och gör samhället som helhet – och i synnerhet det finansiella systemet – mer sårbart för cyberhot eller IKT-avbrott. Även om den allmänt utbredda användningen av IKT-system och hög digitalisering och konnektivitet i dag är centrala inslag i all verksamhet som bedrivs av unionens finansiella enheter är den digitala motståndskraften ännu inte tillräckligt inbyggd i deras operativa ramar.

(2) Användningen av IKT har under de senaste årtiondena fått en avgörande roll inom finanssektorn och är idag kritisk för driften av alla finansiella enheters vanliga dagliga funktioner. Digitaliseringen omfattar t.ex. betalningar, som i allt högre grad har gått från kontanter och pappersbaserade metoder till användning av digitala lösningar, liksom clearing och avveckling av värdepapper, elektronisk och algoritmisk handel, utlåning och finansiering, peer-to-peer-finansiering, kreditvärdering, försäkringsgarantiverksamhet, skadereglering och back-office-verksamhet. Finanssektorn har inte bara blivit till stor del digital i hela sektorn, utan digitaliseringen har också fördjupat sammanlänkningar och beroenden inom finanssektorn och med tredjepartsinfrastruktur och tredjepartstjänsteleverantörer.

---

25 [*lägg till hänvisning*] EUT C , , s. .

26 [*lägg till hänvisning*] EUT C , , s. .

(3) Europeiska systemrisknämnden (ESRB) har i en rapport från 2020 om systemrisker på cyberområdet[27] bekräftat att den nuvarande höga graden av sammanlänkning mellan finansiella enheter, finansmarknader och finansmarknadsinfrastrukturer, och särskilt det ömsesidiga beroendet mellan deras IKT-system, potentiellt kan utgöra en systemsårbarhet, eftersom lokala cyberincidenter snabbt kan spridas från någon av de cirka 22 000 finansiella enheterna i unionen[28] till hela det finansiella systemet, utan hinder av geografiska gränser. Allvarliga IKT-överträdelser inom finanssektorn påverkar inte bara finansiella enheter var för sig. De underlättar också spridning av lokala sårbarheter i de finansiella överföringskanalerna och kan få negativa konsekvenser för stabiliteten i unionens finansiella system, generera likviditetsrusningar och generellt leda till ett minskat förtroende för finansmarknaderna.

(4) På senare år har IKT-risker uppmärksammats av nationella, europeiska och internationella beslutsfattare, tillsynsmyndigheter och standardiseringsorgan i ett försök att öka motståndskraften, fastställa standarder och samordna reglerings- och tillsynsarbetet. På internationell nivå har Baselkommittén för banktillsyn, kommittén för betalnings- och marknadsinfrastruktur, rådet för finansiell stabilitet, *Financial Stability Institute* samt G7- och G20-länderna som mål att förse behöriga myndigheter och marknadsoperatörer inom olika jurisdiktioner med verktyg för att stärka motståndskraften hos deras finansiella system.

(5) Trots nationella och europeiska riktade politiska initiativ och lagstiftningsinitiativ fortsätter IKT-riskerna att utgöra en utmaning för den operativa motståndskraften, prestandan och stabiliteten i unionens finansiella system. Den reform som följde på finanskrisen 2008 stärkte i första hand den finansiella motståndskraften hos unionens finanssektor och syftade till att skydda unionens konkurrenskraft och stabilitet ur ekonomiska, tillsynsmässiga och marknadsmässiga perspektiv. Även om IKT-säkerhet och digital motståndskraft ingår i de operativa riskerna har de inte uppmärksammats lika mycket i lagstiftningsagendan efter krisen och har bara utvecklats inom vissa områden av unionens politik och regelverk för finansiella tjänster, eller endast i ett fåtal medlemsstater.

(6) I kommissionens handlingsplan för fintech från 2018[29] betonades att det är ytterst viktigt att göra unionens finanssektor mer motståndskraftig även ur ett operativt perspektiv för att säkerställa dess tekniska säkerhet och goda funktion, och dess snabba återställning efter IKT-överträdelser och IKT-incidenter, så att finansiella tjänster i förlängningen kan tillhandahållas på ett effektivt och smidigt sätt i hela

---

27 ESRB:s rapport *Systemic Cyber Risk* från 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Enligt den konsekvensbedömning som åtföljer översynen av de europeiska tillsynsmyndigheterna (SWD(2017) 308) finns det omkring 5 665 kreditinstitut, 5 934 värdepappersföretag, 2 666 försäkringsföretag, 1 573 tjänstepensionsinstitut, 2 500 portföljförvaltningsbolag, 350 marknadsinfrastrukturer (t.ex. centrala motparter, fondbörser, systemviktiga internhandlare, transaktionsregister och MTF-plattformar), 45 kreditvärderingsinstitut och 2 500 auktoriserade betalningsinstitut och institut för elektroniska pengar. Sammantaget blir detta cirka 21 233 enheter, vilket inte omfattar gräsrotsfinansieringsföretag, lagstadgade revisorer och revisionsföretag, leverantörer av kryptotillgångstjänster och referensvärdesadministratörer.

29 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska centralbanken, Europeiska ekonomiska och sociala kommittén och Regionkommittén, *Handlingsplanen för fintech – ett viktigt steg mot en mer konkurrenskraftig europeisk finanssektor*, COM(2018)0109 final, https://eur-lex.europa.eu/legal-content/SV/TXT/?from=EN&uri=CELEX%3A52018DC0109.

unionen, även under stressituationer, samtidigt som konsumenternas och marknadens förtroende bevaras.

(7) I april 2019 utfärdade Europeiska bankmyndigheten (EBA), Europeiska värdepappers- och marknadsmyndigheten (Esma) och Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) (gemensamt kallade *de europeiska tillsynsmyndigheterna*) tillsammans två tekniska råd där man efterlyste en enhetlig strategi för IKT-risker inom finanssektorn och rekommenderade att den digitala operativa motståndskraften inom sektorn för finansiella tjänster skulle stärkas på ett proportionellt sätt genom ett sektorsspecifikt unionsinitiativ.

(8) Unionens finansiella sektor regleras genom ett harmoniserat enhetligt regelverk och styrs av ett europeiskt system för finansiell tillsyn. Icke desto mindre är bestämmelserna om digital operativ motståndskraft och IKT-säkerhet ännu inte fullständigt eller konsekvent harmoniserade, trots att den digitala operativa motståndskraften är avgörande för att säkerställa finansiell stabilitet och marknadsintegritet i den digitala tidsåldern, och inte mindre viktiga än t.ex. gemensamma standarder för tillsyn eller marknadsbeteenden. Det enhetliga regelverket och tillsynssystemet bör därför utvecklas så att de även omfattar denna del, genom att mandaten utökas för de finansiella tillsynsmyndigheter som har i uppdrag att övervaka och skydda den finansiella stabiliteten och marknadsintegriteten.

(9) Skillnader i lagstiftning och olika nationella reglerings- eller tillsynsstrategier för IKT-risker skapar hinder för den inre marknaden för finansiella tjänster och hindrar ett smidigt utövande av etableringsfriheten och tillhandahållandet av tjänster för finansiella enheter med gränsöverskridande närvaro. Konkurrensen mellan samma typ av finansiella enheter med verksamhet i olika medlemsstater kan också snedvridas. Särskilt på områden där unionens harmonisering har varit mycket begränsad – såsom testning av den digitala operativa motståndskraften – eller saknas – såsom övervakning av tredjepartsrisker inom IKT – kan skillnader som härrör från den planerade utvecklingen på nationell nivå skapa ytterligare hinder för den inre marknadens funktion, till skada för marknadsaktörerna och den finansiella stabiliteten.

(10) Den hittills fragmenterade behandlingen på EU-nivå av bestämmelser i fråga om IKT-risker uppvisar luckor eller överlappningar på viktiga områden, t.ex. när det gäller IKT-relaterad incidentrapportering och testning av digital operativ motståndskraft, vilket leder till bristande konsekvens när skiljaktiga nationella regler utformas eller överlappande regler tillämpas på ett icke kostnadseffektivt sätt. Detta är särskilt skadligt för IKT-intensiva användare som finanssektorn, eftersom teknikrisker inte stannar vid nationsgränser och finanssektorn använder sina tjänster på bred gränsöverskridande basis inom och utanför unionen.

Enskilda finansiella enheter som bedriver gränsöverskridande verksamhet eller som innehar flera tillstånd (en finansiell enhet kan t.ex. ha tillstånd som bank, värdepappersföretag och betalningsinstitut, där varje tillstånd har utfärdats av olika behöriga myndigheter i en eller flera medlemsstater) ställs inför operativa utmaningar när det gäller att på egen hand hantera IKT-risker och mildra IKT-incidenters negativa effekter på ett samstämmigt och kostnadseffektivt sätt.

(11) Eftersom det enhetliga regelverket inte har åtföljts av en heltäckande IKT-ram eller ram för operativa risker krävs ytterligare harmonisering av viktiga krav på digital operativ motståndskraft för alla finansiella enheter. Den kapacitet och övergripande motståndskraft som finansiella enheter skulle utveckla på grundval av sådana viktiga krav för att stå emot driftstörningar skulle bidra till att bevara stabiliteten och

integriteten på unionens finansmarknader och därmed bidra till att säkerställa en hög skyddsnivå för investerare och konsumenter i unionen. Eftersom syftet med denna förordning är att bidra till att den inre marknaden fungerar friktionsfritt bör den baseras på artikel 114 i EUF-fördraget, så som artikeln tolkats i EU-domstolens fasta rättspraxis.

(12) Denna förordning syftar först och främst till att konsolidera och uppgradera de IKT-riskkrav som hittills har behandlats separat i olika förordningar och direktiv. Även om dessa unionsrättsakter omfattade de huvudsakliga kategorierna av finansiell risk (t.ex. kreditrisk, marknadsrisk, motpartsrisk och likviditetsrisk, marknadsbeteenderisker), kunde inte alla komponenter i den operativa motståndskraften behandlas på ett heltäckande sätt när dessa akter antogs. När kraven på operativ risk utformades i dessa unionsrättsakter föredrogs ofta en traditionell kvantitativ strategi för riskhantering (dvs. fastställande av ett kapitalkrav för att täcka IKT-risker) i stället för riktade kvalitativa krav för att öka kapaciteten genom krav som var inriktade på skydd, upptäckt, begränsning, återställning och avhjälpande av IKT-relaterade incidenter eller genom fastställande av rapporteringskapacitet och digital testkapacitet. Dessa direktiv och förordningar var i första hand avsedda att omfatta grundläggande regler om tillsyn, marknadsintegritet eller marknadsbeteende.

Genom den här förordningen, där reglerna för IKT-risker konsolideras och uppdateras, skulle alla bestämmelser om digitala risker inom finanssektorn för första gången samlas på ett enhetligt sätt i en enda rättsakt. Detta initiativ bör därför täppa till luckorna eller avhjälpa bristen på konsekvens i vissa av de berörda rättsakterna, även i fråga om den terminologi som används i dem, och bör uttryckligen hänvisa till IKT-risker genom riktade regler om IKT-riskhanteringsförmåga, rapportering och testning och övervakning av tredjepartsrisk.

(13) Finansiella enheter bör följa samma tillvägagångssätt och samma principbaserade regler i sin hantering av IKT-risker. Enhetlighet bidrar till att öka förtroendet för det finansiella systemet och bevara dess stabilitet, särskilt i tider av överanvändning av IKT-system, IKT-plattformar och IKT-infrastrukturer, vilket medför ökad digital risk.

Respekten för grundläggande it-hygien bör också leda till att det går att undvika höga kostnader för ekonomin, genom att effekterna av och kostnaderna för IKT-avbrott minimeras.

(14) Användningen av en förordning bidrar till att minska lagstiftningens komplexitet, främja konvergens i tillsynen och öka rättssäkerheten, samtidigt som den bidrar till att begränsa efterlevnadskostnaderna, särskilt för finansiella enheter som bedriver gränsöverskridande verksamhet, och till att minska snedvridningen av konkurrensen. Valet av en förordning för inrättandet av en gemensam ram för finansiella enheters digitala operativa motståndskraft förefaller därför vara det lämpligaste sättet att garantera en enhetlig och samstämmig tillämpning av alla delar av IKT-riskhanteringen inom unionens finanssektorer.

(15) Utöver lagstiftningen om finansiella tjänster bildar Europaparlamentets och rådets direktiv (EU) 2016/1148[30] den nuvarande allmänna ramen för cybersäkerhet på unionsnivå. Av de sju kritiska sektorerna är det direktivet också tillämpligt på tre typer

[30] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

av finansiella enheter, nämligen kreditinstitut, handelsplatser och centrala motparter. Eftersom det i direktiv (EU) 2016/1148 fastställs en mekanism för identifiering på nationell nivå av leverantörer av samhällsviktiga tjänster, är det endast vissa kreditinstitut, handelsplatser och centrala motparter som identifieras av medlemsstaterna och som i praktiken omfattas av direktivets tillämpningsområde och därmed är skyldiga att uppfylla de rapporteringskrav i fråga om IKT-säkerhet och IKT-incidenter som fastställs i direktivet.

(16) Eftersom denna förordning leder till en ökad harmonisering av komponenter för digital motståndskraft genom att det införs strängare krav på IKT-riskhantering och IKT-relaterad incidentrapportering än de som fastställs i unionens nuvarande lagstiftning om finansiella tjänster, innebär detta en ökad harmonisering även jämfört med kraven i direktiv (EU) 2016/1148. Denna förordning utgör följaktligen lex specialis i förhållande till direktiv (EU) 2016/1148.

Det är mycket viktigt att upprätthålla en stark koppling mellan finanssektorn och unionens övergripande ram för cybersäkerhet, vilket skulle säkerställa överensstämmelse med de strategier för cybersäkerhet som redan har antagits av medlemsstaterna och göra det möjligt för finansiella tillsynsmyndigheter att få kännedom om cyberincidenter som påverkar andra sektorer som omfattas av direktiv (EU) 2016/1148.

(17) För att möjliggöra en sektorsövergripande inlärningsprocess och effektivt ta vara på erfarenheter från andra sektorer när det gäller att hantera cyberhot bör de finansiella enheter som avses i direktiv (EU) 2016/1148 fortsätta att ingå i ”ekosystemet” i det direktivet (t.ex. samarbetsgruppen för säkerhet i nätverks- och informationssystem och enheter för hantering av it-säkerhetsincidenter (*Computer Security Incident Response Teams*, nedan kallade *CSIRT-enheter*)).

De europeiska tillsynsmyndigheterna och de nationella behöriga myndigheterna bör kunna delta i de strategiska politiska diskussionerna och det tekniska arbetet i samarbetsgruppen för säkerhet i nätverks- och informationssystem, utbyta information och samarbeta ytterligare med de gemensamma kontaktpunkter som har utsetts enligt direktiv (EU) 2016/1148. De behöriga myndigheterna enligt denna förordning bör också samråda och samarbeta med de nationella CSIRT-enheter som har utsetts i enlighet med artikel 9 i direktiv (EU) 2016/1148.

(18) Det är också viktigt att säkerställa överensstämmelse med direktivet om europeisk kritisk infrastruktur, som för närvarande ses över för att förbättra skyddet av och motståndskraften hos kritisk infrastruktur mot icke cyberrelaterade hot, vilket kan få konsekvenser för finanssektorn. [31]

(19) Leverantörer av molntjänster är en kategori av leverantörer av digitala tjänster som omfattas av direktiv (EU) 2016/1148. Som sådana omfattas de av efterhandstillsyn som utförs av de nationella myndigheter som har utsetts i enlighet med det direktivet. Denna tillsyn är begränsad till de krav på IKT-säkerhets- och incidentrapportering som fastställs i den rättsakten. Eftersom den tillsynsram som inrättas genom denna förordning är tillämplig på alla kritiska tredjepartsleverantörer av IKT-tjänster, inbegripet leverantörer av molntjänster, när de tillhandahåller IKT-tjänster till

[31] Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EUT L 345, 23.12.2008, s. 75).

finansiella enheter, bör den betraktas som ett komplement till den tillsyn som utförs enligt direktiv (EU) 2016/1148. Den tillsynsram som inrättas genom denna förordning bör dessutom omfatta leverantörer av molntjänster i avsaknad av en EU-omfattande sektorsövergripande ram för inrättande av en digital tillsynsmyndighet.

(20) För att de finansiella enheterna ska kunna behålla full kontroll över IKT-risker måste de ha övergripande kapacitet som möjliggör en kraftfull och effektiv IKT-riskhantering, tillsammans med särskilda mekanismer och riktlinjer för IKT-relaterad incidentrapportering, testning av IKT-system, IKT-kontroller och IKT-processer samt för hantering av IKT-tredjepartsrisker. Den digitala operativa motståndskraften för det finansiella systemet bör stärkas samtidigt som man möjliggör en proportionerlig tillämpning av kraven på finansiella enheter som är mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG[32].

(21) Tröskelvärden och taxonomier för rapportering av IKT-relaterade incidenter varierar avsevärt på nationell nivå. Även om en samsyn kan uppnås genom relevant arbete som utförs av Europeiska unionens cybersäkerhetsbyrå (Enisa)[33] och samarbetsgruppen för säkerhet i nätverks- och informationssystem för finansiella enheter enligt direktiv (EU) 2016/1148, kan det fortfarande förekomma eller växa fram olika strategier för tröskelvärden och taxonomier för de andra finansiella enheterna. Detta medför flera krav som finansiella enheter måste uppfylla, särskilt när de är verksamma inom flera av unionens jurisdiktioner och när de ingår i en finansiell koncern. Dessa skillnader kan dessutom hindra inrättandet av ytterligare enhetliga eller centraliserade mekanismer på unionsnivå för att påskynda rapporteringsprocessen och underlätta ett snabbt och smidigt informationsutbyte mellan behöriga myndigheter, vilket är avgörande för att hantera IKT-risker vid storskaliga attacker med eventuella konsekvenser för det finansiella systemet.

(22) För att de behöriga myndigheterna ska kunna fullgöra sina tillsynsuppgifter genom att skaffa sig en fullständig överblick över IKT-relaterade incidenters art, frekvens, betydelse och inverkan och för att förbättra informationsutbytet mellan berörda offentliga myndigheter, inbegripet brottsbekämpande myndigheter och resolutionsmyndigheter, är det nödvändigt att fastställa regler för att komplettera IKT-systemet för incidentrapportering med de krav som för närvarande saknas i lagstiftningen för finansiella delsektorer och undanröja eventuella överlappningar och dubbleringar för att minska kostnaderna. Det är därför viktigt att harmonisera IKT-systemet för incidentrapportering genom att kräva att alla finansiella enheter endast ska rapportera till sina behöriga myndigheter. Dessutom bör de europeiska tillsynsmyndigheterna ges befogenhet att närmare specificera IKT-relaterade delar i incidentrapporteringen, såsom taxonomi, tidsramar, datamängder, mallar och tillämpliga tröskelvärden.

(23) Krav på testning av digital operativ motståndskraft har utarbetats för vissa finansiella delsektorer inom flera, icke samordnade nationella ramar där samma frågor behandlas på olika sätt. Detta leder till dubbla kostnader för gränsöverskridande finansiella

---

32 Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

33 Enisa, *Reference Incident Classification Taxonomy*, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

enheter och försvårar det ömsesidiga erkännandet av resultat. Icke samordnade tester kan därför leda till att den inre marknaden fragmenteras.

(24) I de fall där det inte krävs någon testning förblir dessutom sårbarheter oupptäckta, vilket innebär en högre risk för den finansiella enheten och i förlängningen för den finansiella sektorns stabilitet och integritet. Utan unionsåtgärder skulle testningen av digital operativ motståndskraft fortsätta att vara ojämn och det skulle inte finnas något ömsesidigt erkännande av testresultat i olika jurisdiktioner. Eftersom det är osannolikt att andra finansiella delsektorer skulle anta sådana system i en meningsfull omfattning skulle de också gå miste om de potentiella fördelarna, t.ex. att avslöja sårbarheter och risker, testa försvarskapacitet och driftskontinuitet och öka kundernas, leverantörernas och affärspartnernas förtroende. För att åtgärda sådana överlappningar, skillnader och luckor är det nödvändigt att fastställa regler som syftar till samordnad testning av finansiella enheter och behöriga myndigheter, för att på så sätt underlätta ömsesidigt erkännande av avancerade tester för betydande finansiella enheter.

(25) Finansinstitutens beroende av IKT-tjänster beror delvis på deras behov av att anpassa sig till en framväxande konkurrenskraftig digital global ekonomi, effektivisera sin verksamhet och tillgodose konsumenternas efterfrågan. Karaktären på och omfattningen av ett sådant beroende har utvecklats kontinuerligt under de senaste åren, vilket har drivit fram kostnadsminskningar inom finansiell förmedling, möjliggjort företagsexpansion och skalbarhet vid införandet av finansiell verksamhet och samtidigt gett tillgång till ett brett spektrum av IKT-verktyg för att hantera komplexa interna processer.

(26) Denna omfattande användning av IKT-tjänster framgår av komplexa avtalsarrangemang, där finansiella enheter ofta stöter på svårigheter med att förhandla om avtalsvillkor som är anpassade till de tillsynsstandarder eller andra lagstadgade krav som de omfattas av, eller på annat sätt hävda särskilda rättigheter, såsom åtkomsträtt eller revisionsrätt, när dessa är inskrivna i avtalen. Många sådana avtal innehåller dessutom inte tillräckliga skyddsåtgärder som möjliggör en fullständig övervakning av utkontrakteringsprocesser, vilket gör att den finansiella enheten inte har möjlighet att bedöma dessa risker. Eftersom tredjepartsleverantörer av IKT-tjänster ofta tillhandahåller standardiserade tjänster till olika typer av kunder kan det dessutom hända att sådana avtal inte alltid tillgodoser finansbranschaktörernas individuella eller särskilda behov.

(27) Trots vissa allmänna regler om utkontraktering i några av unionens rättsakter om finansiella tjänster är övervakningen av avtalsdimensionen inte helt förankrad i unionslagstiftningen. I avsaknad av tydliga och skräddarsydda unionsstandarder som är tillämpliga på de avtalsarrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster behandlas inte den externa IKT-riskkällan på ett heltäckande sätt. Det är därför nödvändigt att fastställa vissa nyckelprinciper för att vägleda finansiella enheters hantering av IKT-tredjepartsrisker, tillsammans med en uppsättning grundläggande avtalsenliga rättigheter i samband med flera aspekter av fullgörandet och avslutandet av avtal i syfte att införa vissa minimiskyddsåtgärder och stärka finansiella enheters förmåga att effektivt övervaka alla IKT-risker som uppstår på tredjepartsnivå.

(28) Det råder brist på homogenitet och konvergens när det gäller IKT-tredjepartsrisk och beroende av IKT-tredjeparter. Trots vissa ansträngningar för att ta itu specifikt med

utkontrakteringsområdet, t.ex. 2017 års rekommendationer om utkontraktering till molntjänstleverantörer,[34] behandlas frågan om systemrisker som kan utlösas av finanssektorns exponering mot ett begränsat antal kritiska tredjepartsleverantörer av IKT-tjänster nästan inte alls i unionslagstiftningen. Denna brist på unionsnivå förvärras av att det inte finns några särskilda mandat och verktyg som gör det möjligt för nationella tillsynsmyndigheter att skaffa sig en god bild av beroendet av IKT-tredjeparter och på lämpligt sätt övervaka risker som uppstår till följd av koncentration av sådana beroenden av IKT-tredjeparter.

(29) Med hänsyn till de potentiella systemrisker som den ökade utkontrakteringen och koncentrationen av IKT-tredjeparter medför, och till de nationella mekanismer som gör det möjligt för finansiella tillsynsmyndigheter att kvantitativt och kvalitativt fastställa och åtgärda konsekvenserna av IKT-risker som uppstår hos kritiska tredjepartsleverantörer av IKT-tjänster, är det nödvändigt att inrätta en lämplig unionsram för tillsyn som möjliggör en kontinuerlig övervakning av verksamheten hos tredjepartsleverantörer av IKT-tjänster som är kritiska leverantörer till finansiella enheter.

(30) I och med att IKT-hoten blir mer komplexa och sofistikerade kommer effektiva upptäcktsåtgärder och förebyggande åtgärder att i hög grad vara beroende av regelbundet utbyte av underrättelser om hot och sårbarhet mellan finansiella enheter. Informationsutbyte bidrar till ökad medvetenhet om cyberhot, vilket i sin tur ökar de finansiella enheternas förmåga att förhindra att hot materialiseras till verkliga incidenter och gör det möjligt för de finansiella enheterna att bättre begränsa effekterna av IKT-relaterade incidenter och återhämta sig mer effektivt. I avsaknad av vägledning på unionsnivå verkar flera faktorer ha hindrat sådant utbyte av underrättelser, framför allt osäkerhet om förenligheten med dataskyddsreglerna, antitrustreglerna och ansvarsbestämmelserna.

(31) Dessutom leder tveksamheter om vilken typ av information som kan delas med andra marknadsaktörer, eller med myndigheter som inte är tillsynsmyndigheter (t.ex. Enisa, för analytiskt underlag eller Europol, för brottsbekämpande ändamål) till att användbar information inte lämnas ut. Omfattningen av och kvaliteten på informationsutbytet är fortfarande begränsad och fragmenterad. Relevanta utbyten görs oftast lokalt (via nationella initiativ) och det saknas enhetliga EU-omfattande arrangemang för informationsutbyte som är anpassade till behoven i en integrerad finanssektor.

(32) Finansiella enheter bör därför uppmuntras att kollektivt utnyttja sina individuella kunskaper och praktiska erfarenheter på strategisk, taktisk och operativ nivå i syfte att förbättra sin förmåga att på lämpligt sätt bedöma, övervaka, försvara och reagera på cyberhot. Det är därför nödvändigt att på unionsnivå möjliggöra framväxten av mekanismer för frivilligt informationsutbyte som, när de genomförs i betrodda miljöer, skulle hjälpa finanssektorn att förebygga och kollektivt reagera på hot genom att snabbt begränsa spridningen av IKT-risker och hindra potentiella spridningseffekter genom de finansiella kanalerna. Dessa mekanismer bör genomföras i full överensstämmelse med unionens tillämpliga konkurrensregler[35] och på ett sätt som garanterar full respekt för unionens dataskyddsregler, främst Europaparlamentets och

---

34 Rekommendationer om utkontraktering till molntjänstleverantörer (EBA/REC/2017/03), som nu har upphävts genom EBA:s riktlinjer för utkontraktering (EBA/GL/2019/02).

35 Meddelande från kommissionen – *Riktlinjer för tillämpningen av artikel 101 i fördraget om Europeiska unionens funktionssätt på horisontella samarbetsavtal*, 2011/C 11/01.

rådets förordning (EU) 2016/679,[36] särskilt i samband med sådan behandling av personuppgifter som är nödvändig för ändamål som rör den registeransvariges eller en tredjeparts berättigade intresse, i enlighet med artikel 6.1 f i den förordningen.

(33) Trots den breda täckning som föreskrivs i denna förordning bör man vid tillämpningen av reglerna om digital operativ motståndskraft beakta betydande skillnader mellan finansiella enheter i fråga om storlek, affärsprofiler eller exponering för digital risk. Som en allmän princip bör finansiella enheter, när de fördelar resurser och kapacitet till genomförandet av IKT-riskhanteringsramen, på lämpligt sätt väga sina IKT-relaterade behov mot sin storlek och affärsprofil, medan de behöriga myndigheterna bör fortsätta att bedöma och se över tillvägagångssättet för en sådan fördelning.

(34) Eftersom större finansiella enheter kan ha mer omfattande resurser och snabbt skulle kunna använda medel för att utveckla styrningsstrukturer och inrätta olika företagsstrategier, bör endast finansiella enheter som inte är mikroföretag i den mening som avses i denna förordning vara skyldiga att inrätta mer komplexa styrformer. Framför allt är sådana enheter bättre rustade att inrätta särskilda ledningsfunktioner för att övervaka arrangemang med tredjepartsleverantörer av IKT-tjänster eller för att sköta krishantering, organisera sin IKT-riskhantering enligt modellen med tre försvarslinjer eller anta ett personaldokument som på ett heltäckande sätt förklarar riktlinjerna för åtkomsträttigheter.

På samma sätt bör endast sådana finansiella enheter uppmanas att göra djupgående bedömningar efter större förändringar i infrastrukturen och processerna för nätverks- och informationssystem, regelbundet genomföra riskanalyser av befintliga IKT-system eller utöka testningen av driftskontinuitet och åtgärds- och återställningsplaner för att fånga upp överflyttningsscenarier mellan primär IKT-infrastruktur och reservanläggningar.

(35) Eftersom endast de finansiella enheter som har identifierats som betydande vid tillämpning av avancerade testning av digital motståndskraft bör vara skyldiga att utföra hotstyrda penetrationstester, bör dessutom de administrativa processer och finansiella kostnader som genomförandet av sådana tester medför överföras till en liten andel av de finansiella enheterna. För att minska regelbördan bör slutligen endast andra finansiella enheter än mikroföretag uppmanas att regelbundet rapportera till de behöriga myndigheterna om alla kostnader och förluster som orsakas av IKT-avbrott och om resultatet av översyner efter betydande IKT-avbrott.

(36) För att säkerställa fullständig anpassning och övergripande konsekvens mellan finansiella enheters affärsstrategier, å ena sidan, och genomförandet av IKT-riskhantering, å andra sidan, bör ledningsorganet vara skyldigt att ha en central och aktiv roll i styrningen och anpassningen av IKT-riskhanteringsramen och den övergripande strategin för digital motståndskraft. Ledningsorganets strategi bör inte enbart vara inriktad på hur IKT-systemens motståndskraft säkerställs, utan även omfatta människor och processer genom en uppsättning strategier som, på varje företagsnivå och för all personal, främjar en stark känsla av medvetenhet om it-risker och ett åtagande att tillämpa en strikt it-hygien på alla nivåer.

---

[36] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

Ledningsorganet yttersta ansvar för att hantera en finansiell enhets IKT-risker bör utgöra en övergripande princip för den heltäckande strategin och omsättas i ett fortlöpande engagemang hos ledningen för att kontrollera övervakningen av IKT-riskhanteringen.

(37) Dessutom går ledningsorganets fullständiga ansvarsskyldighet hand i hand med uppgiften att säkerställa att IKT-investeringarna och den övergripande budgeten är tillräckliga för att den finansiella enheten ska kunna uppnå sin referensnivå för digital operativ motståndskraft.

(38) Med inspiration från relevanta internationella, nationella och branschspecifika standarder, riktlinjer, rekommendationer eller strategier för hantering av it-risker,[37] förordas i denna förordning en uppsättning funktioner som underlättar den övergripande struktureringen av IKT-riskhanteringen. Så länge som de finansiella enheternas huvudsakliga kapacitet uppfyller behoven enligt de mål som anges i denna förordning (identifiering, skydd och förebyggande, upptäckt, åtgärd och återställning, lärande och utveckling samt kommunikation) står det finansiella enheter fritt att använda IKT-riskhanteringsmodeller som utformas eller kategoriseras på olika sätt.

(39) För att hålla jämna steg med det föränderliga cyberhotlandskapet bör finansiella enheter upprätthålla uppdaterade IKT-system som är tillförlitliga och har tillräcklig kapacitet, inte bara för att garantera behandlingen av data eftersom det är nödvändigt för att de ska kunna utföra sina tjänster, utan också för att säkerställa teknisk motståndskraft som gör det möjligt för finansiella enheter att på ett adekvat sätt hantera ytterligare behandlingsbehov som stressade marknadsförhållanden eller andra ogynnsamma situationer kan ge upphov till. Även om denna förordning inte medför någon standardisering av specifika IKT-system, IKT-verktyg eller IKT-tekniker, är den beroende av att de finansiella enheterna använder europeiska och internationellt erkända tekniska standarder (t.ex. ISO) eller branschens bästa praxis på lämpligt sätt, i den mån den användningen är helt förenlig med särskilda tillsynsinstruktioner om användning och införlivande av internationella standarder.

(40) Effektiva kontinuitets- och återställningsplaner krävs för att finansiella enheter snabbt ska kunna åtgärda IKT-relaterade incidenter, särskilt it-attacker, genom att begränsa skador och prioritera återupptagande av verksamhet och återställningsåtgärder. Behandlingen i säkerhetskopieringssystem bör påbörjas så snart som möjligt, men detta får inte på något sätt äventyra integriteten och säkerheten i nätverks- och informationssystem eller uppgifternas konfidentialitet.

(41) Även om denna förordning innebär att finansiella enheter kan fastställa mål för återställningstiden på ett flexibelt sätt och därvid fullt ut ta hänsyn till den berörda funktionens egenskaper och kritiska betydelse och till eventuella särskilda verksamhetsbehov, bör det också krävas en bedömning av den eventuella övergripande inverkan på marknadseffektiviteten när sådana mål fastställs.

(42) De betydande konsekvenserna av it-attacker förstärks när de sker inom finanssektorn, ett område som löper mycket större risk att bli måltavla för skadliga spridare som vill

---

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf G7 *Fundamental Elements of Cybersecurity for the Financial Sector,* https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf, NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, FSB *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

göra ekonomisk vinning direkt vid källan. För att minska sådana risker och förhindra att IKT-system förlorar integritet eller blir otillgängliga och att det sker intrång i konfidentiella uppgifter eller att fysisk IKT-infrastruktur skadas, bör de finansiella enheternas rapportering av större IKT-relaterade incidenter förbättras avsevärt.

IKT-relaterad incidentrapportering bör harmoniseras för alla finansiella enheter genom att de åläggs att endast rapportera till sina behöriga myndigheter. Alla finansiella enheter skulle omfattas av denna rapportering, men alla bör inte påverkas på samma sätt, eftersom relevanta väsentlighetströsklar och tidsramar bör kalibreras så att de endast fångar upp större IKT-relaterade incidenter. Direkt rapportering skulle göra det möjligt för finansiella tillsynsmyndigheter att få tillgång till information om IKT-relaterade incidenter. De finansiella tillsynsmyndigheterna bör dock vidarebefordra denna information till icke-finansiella offentliga myndigheter (behöriga myndigheter för säkerhet i nätverks- och informationssystem, nationella dataskyddsmyndigheter och brottsbekämpande myndigheter för incidenter som är av brottslig art). Information om IKT-relaterade incidenter bör förmedlas ömsesidigt: de finansiella tillsynsmyndigheterna bör ge all nödvändig återkoppling eller vägledning till den finansiella enheten, medan de europeiska tillsynsmyndigheterna bör dela anonymiserade uppgifter om hot och sårbarheter i samband med en händelse till stöd för ett bredare kollektivt försvar.

(43) Det bör övervägas ytterligare diskussioner om en eventuell centralisering av IKT-relaterade incidentrapporter genom en enda gemensam EU-knutpunkt som antingen direkt tar emot relevanta rapporter och automatiskt underrättar nationella behöriga myndigheter, eller som enbart tar emot rapporter från de nationella behöriga myndigheterna och fyller en samordnande funktion. De europeiska tillsynsmyndigheterna bör åläggas att senast vid ett visst datum i samråd med ECB och Enisa utarbeta en gemensam rapport om möjligheten att inrätta en sådan gemensam EU-knutpunkt.

(44) För att uppnå en stabil digital operativ motståndskraft, och i linje med internationella standarder (t.ex. G7-gruppens *Fundamental Elements for Threat-Led Penetration Testing*), bör finansiella enheter regelbundet testa sina IKT-system och sin personal med avseende på hur effektiv deras kapacitet för förebyggande, upptäckt, åtgärd och återställning är, för att upptäcka och åtgärda potentiella IKT-sårbarheter. För att ta hänsyn till skillnader mellan och inom de finansiella undersektorerna när det gäller de finansiella enheternas cybersäkerhetsberedskap bör testerna omfatta ett brett spektrum av verktyg och åtgärder, alltifrån en bedömning av grundläggande krav (t.ex. sårbarhetsbedömningar och skanningar, analyser av öppen källkod, nätverkssäkerhetsbedömningar, bristanalyser, fysiska säkerhetsgranskningar, frågeformulär och programvarulösningar, källkodsgranskningar där så är möjligt, scenariobaserade tester, kompatibilitetstester, resultatprovning eller end-to-end-tester) till mer avancerade tester (t.ex. hotstyrda penetrationstester för de finansiella enheter som är tillräckligt mogna ur ett IKT-perspektiv). Testningen av den digitala operativa motståndskraften bör därför vara mer krävande för betydande finansiella enheter (t.ex. stora kreditinstitut, fondbörser, värdepapperscentraler, centrala motparter osv.). Samtidigt bör testning av digital operativ motståndskraft också vara mer relevant för vissa delsektorer som har en central betydelse för systemet (t.ex. betalningar, bankverksamhet, clearing och avveckling) och mindre relevant för andra delsektorer (t.ex. kapitalförvaltare, kreditvärderingsinstitut osv.). Gränsöverskridande finansiella enheter som utövar sin etableringsfrihet eller frihet att tillhandahålla tjänster inom unionen bör uppfylla en enda uppsättning avancerade testkrav (t.ex. hotstyrda

penetrationstester) i sin hemmedlemsstat, och detta test bör omfatta IKT-infrastrukturerna i alla jurisdiktioner i unionen där den gränsöverskridande koncernen bedriver verksamhet, vilket innebär att testningskostnader uppstår i endast en jurisdiktion för gränsöverskridande koncerner.

(45) För att säkerställa en sund övervakning av IKT-tredjepartsrisk är det nödvändigt att fastställa en uppsättning principbaserade regler för att vägleda finansiella enheters övervakning av risker som uppstår i samband med funktioner som har utkontrakterats till tredjepartsleverantörer av IKT-tjänster och, mer allmänt, inom ramen för beroenden av IKT-tredjeparter.

(46) En finansiell enhet bör alltid ha det fulla ansvaret för att uppfylla skyldigheterna enligt denna förordning. En proportionell övervakning av de risker som uppstår hos tredjepartsleverantören av IKT-tjänster bör utformas genom att vederbörlig hänsyn tas till omfattningen av, komplexiteten hos och betydelsen av IKT-relaterade beroenden, kritikaliteten hos eller betydelsen av de tjänster, processer eller funktioner som omfattas av avtalsarrangemangen och, i förlängningen, på grundval av en noggrann bedömning av eventuella effekter på kontinuiteten och kvaliteten hos finansiella tjänster på individuell nivå och gruppnivå, beroende på vad som är lämpligt.

(47) Denna övervakning bör följa ett strategiskt tillvägagångssätt för IKT-tredjepartsrisker som inrättas formellt genom att den finansiella enhetens ledningsorgan antar en särskild strategi som bygger på en kontinuerlig granskning av alla sådana beroenden av IKT-tredjeparter. För att öka tillsynsmyndigheternas medvetenhet om beroenden av IKT-tredjeparter och ytterligare stödja den tillsynsram som inrättas genom denna förordning, bör finansiella tillsynsmyndigheter regelbundet få viktig information från registren och bör kunna begära utdrag ur registren på ad hoc-basis.

(48) En grundlig förhandsanalys bör ligga till grund för och utföras innan formella avtalsarrangemang ingås, medan uppsägning av avtal bör föranledas av åtminstone en rad omständigheter som visar på brister hos tredjepartsleverantören av IKT-tjänster.

(49) För att hantera systemeffekterna av koncentrationsrisken för IKT-tredjeparter bör en balanserad lösning främjas genom en flexibel och gradvis strategi, eftersom strikta tak eller strikta begränsningar kan hindra företagens affärsverksamhet och avtalsfrihet. Finansiella enheter bör göra en grundlig bedömning av avtalsarrangemangen för att fastställa sannolikheten för att en sådan risk uppstår, bland annat genom djupgående analyser av underentreprenadavtal, särskilt när de ingås med tredjepartsleverantörer av IKT-tjänster som är etablerade i ett tredjeland. I detta skede, och i syfte att uppnå en rimlig balans mellan kravet på att bevara avtalsfriheten och kravet på att garantera finansiell stabilitet, anses det inte lämpligt att fastställa strikta tak och gränser för exponeringar mot IKT-tredjeparter. Den europeiska tillsynsmyndighet som har utsetts för att utöva tillsyn över varje kritisk tredjepartsleverantör av IKT-tjänster (nedan kallad *den ledande tillsynsmyndigheten*) bör vid fullgörandet av sina tillsynsuppgifter ägna särskild uppmärksamhet åt att fullt ut förstå omfattningen av ömsesidiga beroenden och upptäcka specifika fall där en hög koncentration av kritiska tredjepartsleverantörer av IKT-tjänster i unionen sannolikt kommer att sätta press på stabiliteten och integriteten i unionens finansiella system och upprätthålla en dialog med kritiska tredjepartsleverantörer av IKT-tjänster där denna risk har identifierats.[38]

[38] Om det dessutom skulle uppstå en risk för missbruk av en tredjepartsleverantör av IKT-tjänster som anses dominerande bör de finansiella enheterna också ha möjlighet att lämna in ett formellt eller

(50) För att kunna utvärdera och regelbundet övervaka förmågan hos tredjepartsleverantören av IKT-tjänster att på ett säkert sätt tillhandahålla tjänster till den finansiella enheten utan negativa effekter på den senares motståndskraft, bör det finnas en harmonisering av centrala avtalsdelar under hela fullgörandet av avtal med IKT-tredjepartsleverantörer. Dessa delar omfattar endast minimiaspekter av avtalet som anses avgörande för att den finansiella enheten ska kunna bedriva en fullständig övervakning i syfte att säkerställa den digitala motståndskraft som är beroende av IKT-tjänstens stabilitet och säkerhet.

(51) Avtalsarrangemangen bör särskilt innehålla en specifikation med heltäckande beskrivningar av funktioner och tjänster, platser där sådana funktioner tillhandahålls och där uppgifter behandlas, samt en uppgift om beskrivningar av fullständig servicenivå tillsammans med kvantitativa och kvalitativa prestationsmål inom överenskomna servicenivåer för att möjliggöra en effektiv övervakning från den finansiella enhetens sida. På samma sätt bör bestämmelser om åtkomst, tillgänglighet, integritet, säkerhet och skydd av personuppgifter samt garantier för åtkomst, återvinning och återlämnande vid insolvens, resolution eller nedläggning av affärsverksamheten hos tredjepartsleverantören av IKT-tjänster också betraktas som väsentliga delar för att en finansiell enhet ska kunna säkerställa övervakningen av tredjepartsrisken.

(52) För att säkerställa att finansiella enheter fortfarande har full kontroll över all utveckling som kan försämra deras IKT-säkerhet bör tidsfrister för anmälan och rapporteringsskyldigheter för tredjepartsleverantören av IKT-tjänster fastställas för händelser som kan ha en väsentlig inverkan på tredjepartsleverantörens förmåga att effektivt utföra kritiska eller viktiga funktioner, inbegripet tillhandahållande av bistånd från tredjepartsleverantören i händelse av en IKT-relaterad incident utan extra kostnad eller till en kostnad som fastställs på förhand.

(53) Den finansiella enhetens eller en utsedd tredjeparts rätt till åtkomst, kontroll och revision är avgörande verktyg i de finansiella enheternas fortlöpande övervakning av IKT-tredjepartsleverantörens prestanda, i kombination med att den sistnämnda samarbetar fullt ut under kontrollerna. På samma sätt bör den finansiella enhetens behöriga myndighet ha dessa rättigheter för att, på grundval av anmälningar, kontrollera och granska tredjepartsleverantören av IKT-tjänster, med förbehåll för sekretesskrav.

(54) Avtalsarrangemangen bör innehålla tydliga uppsägningsrättigheter och tillhörande minimimeddelanden samt särskilda exitstrategier som i synnerhet möjliggör obligatoriska övergångsperioder under vilka tredjepartsleverantörer av IKT-tjänster bör fortsätta att tillhandahålla relevanta funktioner för att minska risken för avbrott på finansiell enhetsnivå eller göra det möjligt för den finansiella enheten att på ett effektivt sätt byta till andra tredjepartsleverantörer av IKT-tjänster, eller använda sig av lösningar på plats som är förenliga med den tillhandahållna tjänstens komplexitet.

(55) Dessutom kan frivillig användning av standardavtalsklausuler kommissionen har utvecklat för molntjänster underlätta ytterligare för de finansiella enheterna och deras IKT-tredjepartsleverantörer genom att öka rättssäkerheten när det gäller den finansiella sektorns användning av molntjänster, i fullständig överensstämmelse med de krav och förväntningar som fastställs i förordningen om finansiella tjänster. Detta arbete bygger

---

informellt klagomål till Europeiska kommissionen eller till de nationella konkurrensrättsliga myndigheterna.

på åtgärder som planerades redan i 2018 års handlingsplan för fintech, där kommissionen tillkännagav sin avsikt att uppmuntra och underlätta utarbetandet av standardavtalsbestämmelser för finansinstituts utkontraktering till molntjänster, genom att bygga på de branschöverskridande ansträngningar från molntjänstintressenternas sida som kommissionen redan har bidragit till med den finansiella sektorns medverkan.

(56) I syfte att främja konvergens och effektivitet när det gäller tillsynsstrategier för tredjepartsrisker inom IKT-sektorn, stärka den digitala operativa motståndskraften hos finansiella enheter som är beroende av kritiska tredjepartsleverantörer av IKT-tjänster för att utföra operativa funktioner, och därmed bidra till att bevara stabiliteten i unionens finansiella system, bör integriteten på den inre marknaden för finansiella tjänster omfattas av en unionstillsynsram.

(57) Eftersom det endast är motiverat med en särskild behandling av kritiska tredjepartsleverantörer bör en urvalsmekanism för tillämpningen av unionens tillsynsram inrättas för att ta hänsyn till omfattningen och arten av den finansiella sektorns beroende av sådana tredjepartsleverantörer av IKT-tjänster genom en uppsättning kvantitativa och kvalitativa kriterier för att fastställa kritikalitetsparametrar som grund för att inkludera leverantörerna i tillsynen. Kritiska tredjepartsleverantörer av IKT-tjänster som inte automatiskt utses genom tillämpning av dessa kriterier bör ha möjlighet att delta frivilligt i tillsynsramen, medan de tredjepartsleverantörer på IKT-området som redan omfattas av tillsynsmekanismer som har inrättats inom ramen för Eurosystemet till stöd för de uppgifter som avses i artikel 127.2 i fördraget om Europeiska unionens funktionssätt bör undantas.

(58) Kravet på att tredjepartsleverantörer av IKT-tjänster som har klassificerats som kritiska ska vara rättsligt erkända i unionen innebär inte datalokalisering, eftersom denna förordning inte medför några ytterligare krav på lagring eller behandling av data i unionen.

(59) Denna ram bör inte påverka medlemsstaternas behörighet att utföra egna tillsynsuppdrag avseende tredjepartsleverantörer av IKT-tjänster som inte är kritiska enligt denna förordning men som kan anses vara viktiga på nationell nivå.

(60) För att utnyttja den nuvarande flerskiktade institutionella strukturen på området finansiella tjänster bör de europeiska tillsynsmyndigheternas gemensamma kommitté fortsätta att säkerställa den övergripande sektorsövergripande samordningen i alla frågor som rör IKT-risker, i enlighet med sina uppgifter i fråga om cybersäkerhet, med stöd av en ny underkommitté (tillsynsforum) som utför förberedande arbete för både enskilda beslut riktade till kritiska tredjepartsleverantörer av IKT-tjänster och kollektiva rekommendationer, särskilt när det gäller riktmärkning av tillsynsprogram för kritiska tredjepartsleverantörer av IKT-tjänster, och fastställande av bästa praxis för hantering av IKT-koncentrationsrisker.

(61) För att säkerställa att tredjepartsleverantörer av IKT-tjänster som spelar en avgörande roll för den finansiella sektorns funktion övervakas på motsvarande sätt på unionsnivå bör en av de europeiska tillsynsmyndigheterna utses till ledande tillsynsmyndighet för varje kritisk tredjepartsleverantör av IKT-tjänster.

(62) De ledande tillsynsmyndigheterna bör ha de befogenheter som krävs för att genomföra utredningar, kontroller på plats och på annan plats hos kritiska tredjepartsleverantörer av IKT-tjänster, få tillträde till alla relevanta lokaler och platser och få fullständig och uppdaterad information så att de kan få verklig inblick i typen, omfattningen och

effekten av den IKT-tredjepartsrisk som de finansiella enheterna och i förlängningen unionens finansiella system utsätts för.

Att de europeiska tillsynsmyndigheterna anförtros den ledande tillsynen är en förutsättning för att man ska kunna få grepp om och ta itu med den systemrelaterade dimensionen av IKT-risker inom finanssektorn. Det fotavtryck som kritiska tredjepartsleverantörer av IKT-tjänster har i unionen och de potentiella problemen med IKT-koncentrationsrisker i samband med detta kräver en gemensam strategi på unionsnivå. Att ett stort antal revisioner utförs och åtkomsträttigheter utnyttjas separat av en mängd behöriga myndigheter med liten eller ingen samordning, skulle inte ge någon fullständig överblick över IKT-tredjepartsriskerna och skulle samtidigt innebära onödig redundans, börda och komplexitet för kritiska IKT-tredjepartsleverantörer som skulle ställas inför en mängd förfrågningar.

(63) Dessutom bör de ledande tillsynsmyndigheterna kunna lämna rekommendationer om IKT-riskfrågor och lämpliga åtgärder, vilket även kan innebära att de motsätter sig vissa avtalsarrangemang som i förlängningen påverkar stabiliteten i den finansiella enheten eller det finansiella systemet. Efterlevnaden av sådana materiella rekommendationer från de ledande tillsynsmyndigheterna bör beaktas av de nationella behöriga myndigheterna inom ramen för deras uppdrag i samband med tillsynen över finansiella enheter.

(64) Tillsynsramen ska inte ersätta eller på något sätt eller i någon del användas i stället för de finansiella enheternas hantering av den risk som är förknippad med användningen av tredjepartsleverantörer av IKT-tjänster, inklusive skyldigheten att fortlöpande övervaka sina avtal med kritiska tredjepartsleverantörer av IKT-tjänster. Den ska inte heller påverka de finansiella enheternas fulla ansvar för att efterleva och uppfylla alla krav enligt denna förordning och relevant lagstiftning om finansiella tjänster. För att undvika dubbelarbete och överlappningar bör de behöriga myndigheterna avstå från att vidta åtgärder som syftar till att övervaka riskerna i samband med den kritiska tredjepartsleverantören av IKT-tjänster. Alla sådana åtgärder bör i förväg samordnas och överenskommas inom tillsynsramen.

(65) För att främja konvergens på internationell nivå när det gäller bästa praxis som ska användas vid granskningen av tredjepartsleverantörers digitala riskhantering bör de europeiska tillsynsmyndigheterna uppmuntras att ingå samarbetsavtal med relevanta behöriga tillsynsmyndigheter och reglerande myndigheter i tredjeländer för att underlätta utvecklingen av bästa praxis för hantering av IKT-tredjepartsrisker.

(66) För att dra nytta av den tekniska expertisen hos de behöriga myndigheternas experter på operativ riskhantering och IKT-riskhantering bör de ledande tillsynsmyndigheterna ta vara på nationell tillsynserfarenhet och inrätta särskilda granskningsgrupper för varje enskild kritisk tredjepartsleverantör av IKT-tjänster, för att samla sektorsövergripande grupper som kan stödja förberedelserna och det faktiska genomförandet av tillsynsverksamhet, inbegripet kontroller på plats av kritiska tredjepartsleverantörer av IKT-tjänster, samt nödvändig uppföljning av dem.

(67) De behöriga myndigheterna bör ha alla nödvändiga tillsyns-, utrednings- och sanktionsbefogenheter för att säkerställa tillämpningen av denna förordning. Administrativa sanktioner bör i princip offentliggöras. Eftersom finansiella enheter och tredjepartsleverantörer av IKT-tjänster kan vara etablerade i olika medlemsstater och övervakas av olika behöriga sektorsmyndigheter, bör ett nära samarbete mellan de

relevanta behöriga myndigheterna, inbegripet ECB när det gäller särskilda uppgifter som den tilldelas genom rådets förordning (EU) nr 1024/2013[39], och samråd med de europeiska tillsynsmyndigheterna säkerställas genom ömsesidigt informationsutbyte och bistånd inom ramen för tillsynsverksamheten.

(68) För att ytterligare kvantitativt och kvalitativt fastställa klassificeringskriterierna för kritiska tredjepartsleverantörer av IKT-tjänster och harmonisera tillsynsavgifterna bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt delegeras till kommissionen med avseende på följande: Närmare specificering av den systempåverkan som ett fel hos en tredjepartsleverantör av IKT-tjänster skulle kunna ha på de finansiella enheter som den levererar tjänster till, antalet globala systemviktiga institut eller andra systemviktiga institut som är beroende av respektive tredjepartsleverantör av IKT-tjänster, antalet tredjepartsleverantörer av IKT-tjänster som är verksamma på en viss marknad, kostnaderna för att migrera till en annan tredjepartsleverantör av IKT-tjänster, antalet medlemsstater där den berörda tredjepartsleverantören av IKT-tjänster tillhandahåller tjänster och där finansiella enheter som använder den berörda tredjepartsbetaltjänstleverantören bedriver verksamhet samt tillsynsavgifternas storlek och hur de ska betalas.

Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016.[40] För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(69) Eftersom denna förordning, tillsammans med Europaparlamentets och rådets direktiv (EU) 20xx/xx,[41] innebär en konsolidering av IKT-riskhanteringsbestämmelser som omfattar flera förordningar och direktiv i unionens regelverk om finansiella tjänster, inbegripet förordningarna (EG) nr 1060/2009, (EU) nr 600/2014 och (EU) nr 909/2014, bör dessa förordningar ändras för att säkerställa fullständig enhetlighet och klargöra att de relevanta bestämmelserna om IKT-risker fastställs i den här förordningen.

Tekniska standarder bör säkerställa en konsekvent harmonisering av kraven i denna förordning. Eftersom de europeiska tillsynsmyndigheterna har högspecialiserad expertis på området bör de få i uppdrag att utarbeta förslag till tekniska standarder för tillsyn som inte inbegriper några politiska val, och som ska läggas fram för kommissionen. Tekniska standarder för tillsyn bör utarbetas inom områdena IKT-riskhantering, rapportering, testning och nyckelkrav för en sund övervakning av IKT-tredjepartsrisker.

(70) Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. Kommissionen och de europeiska tillsynsmyndigheterna bör se till att dessa standarder och krav kan tillämpas av alla

---

39 Rådets förordning (EU) nr 1024/2013 av den 15 oktober 2013 om tilldelning av särskilda uppgifter till Europeiska centralbanken i fråga om politiken för tillsyn över kreditinstitut (EUT L 287, 29.10.2013, s. 63).

40 EUT L 123, 12.5.2016, s. 1.

41 [*Lägg in fullständig hänvisning*]

finansiella enheter på ett sätt som står i proportion till dessa enheter och deras verksamheter i fråga om deras art, omfattning och komplexitet.

(71) För att göra det lättare att jämföra viktiga IKT-relaterade incidentrapporter och säkerställa insyn i avtalsarrangemang för användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster, bör de europeiska tillsynsmyndigheterna ges i uppdrag att utarbeta förslag till tekniska standarder för genomförande där det fastställs standardiserade mallar, formulär och förfaranden för finansiella enheter för rapportering av en större IKT-relaterad incident, samt standardiserade mallar för registrering av information. När de europeiska tillsynsmyndigheterna utarbetar dessa standarder bör de ta hänsyn till de finansiella enheternas storlek och komplexitet samt arten av och risknivån för deras verksamhet. Kommissionen bör ges befogenhet att anta tekniska standarder för tillsyn genom delegerade akter i enlighet med artikel 291 i EUF-fördraget och i enlighet med artikel 15 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 respektive (EU) nr 1095/2010. Eftersom ytterligare krav redan har specificerats genom delegerade akter och genomförandeakter baserade på tekniska standarder för tillsyn och genomförande i förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 respektive (EU) nr 909/2014 är det lämpligt att ge de europeiska tillsynsmyndigheterna i uppdrag att, antingen enskilt eller gemensamt genom den gemensamma kommittén, överlämna tekniska standarder för tillsyn och genomförande till kommissionen för antagande av delegerade akter och genomförandeakter för att överföra och uppdatera befintliga IKT-riskhanteringsregler.

(72) Detta arbete kommer att medföra efterföljande ändringar av befintliga delegerade akter och genomförandeakter som har antagits inom olika områden av lagstiftningen om finansiella tjänster. Tillämpningsområdet för de artiklar om operativ risk för vilka delegerade akter och genomförandeakter ska antas enligt befogenheterna i de förordningarna bör ändras så att alla bestämmelser som omfattar digital operativ motståndskraft och som i dag ingår i de förordningarna överförs till den här förordningen.

(73) Eftersom målen för denna förordning, dvs. att uppnå en hög nivå av digital operativ motståndskraft som är tillämplig på alla finansiella enheter, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna eftersom de kräver harmonisering av en mängd olika regler som för närvarande finns i vissa unionsakter eller i de olika medlemsstaternas rättssystem, och de därför, på grund av åtgärdernas omfattning och effekt, bättre kan uppnås på unionsnivå, får unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

1. I denna förordning fastställs följande enhetliga krav avseende säkerhet i nätverks- och informationssystem som stöder finansiella enheters affärsprocesser, vilka behövs för att uppnå en hög gemensam nivå av digital operativ motståndskraft:

   (a) Krav som är tillämpliga på finansiella enheter i fråga om

   – riskhantering inom informations- och kommunikationsteknik (IKT),

   – rapportering av större IKT-relaterade incidenter till de behöriga myndigheterna,

   – testning av digital operativ motståndskraft,

   – utbyte av information och underrättelser i samband med cyberhot och sårbarheter,

   – åtgärder för att finansiella enheter ska kunna hantera tredjepartsrelaterade IKT-risker på ett sunt sätt.

   (b) Krav i samband med de avtalsarrangemang som har ingåtts mellan tredjepartsleverantörer av IKT-tjänster och finansiella enheter.

   (c) En ram för tillsyn av kritiska tredjepartsleverantörer av IKT-tjänster när de tillhandahåller tjänster till finansiella enheter.

   (d) Regler om samarbete mellan behöriga myndigheter och regler om behöriga myndigheters tillsyn och kontroll av efterlevnaden i alla frågor som omfattas av denna förordning.

2. När det gäller finansiella enheter som har identifierats som leverantörer av samhällsviktiga tjänster enligt nationella bestämmelser som införlivar artikel 5 i direktiv (EU) 2016/1148 ska denna förordning betraktas som en sektorsspecifik unionsrättsakt vid tillämpningen av artikel 1.7 i det direktivet.

Artikel 2

Tillämpningsområde med avseende på personer

1. Denna förordning är tillämplig på följande enheter:

   (a) Kreditinstitut.

   (b) Betalningsinstitut.

   (c) Institut för elektroniska pengar.

   (d) Värdepappersföretag.

   (e) Leverantörer av kryptotillgångstjänster, emittenter av kryptotillgångar, emittenter av tillgångsanknutna token och emittenter av betydande tillgångsanknutna token.

(f) Värdepapperscentraler.

(g) Centrala motparter.

(h) Handelsplatser.

(i) Transaktionsregister.

(j) Förvaltare av alternativa investeringsfonder.

(k) Förvaltningsbolag.

(l) Leverantörer av datarapporteringstjänster.

(m) Försäkrings- och återförsäkringsföretag.

(n) Försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet.

(o) Tjänstepensionsinstitut.

(p) Kreditvärderingsinstitut.

(q) Lagstadgade revisorer och revisionsföretag.

(r) Administratörer av kritiska referensvärden.

(s) Leverantörer av gräsrotsfinansieringstjänster.

(t) Värdepapperiseringsregister.

(u) Tredjepartsleverantörer av IKT-tjänster.

2. Vid tillämpningen av denna förordning ska de enheter som avses i leden a–t tillsammans benämnas *finansiella enheter*.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

(1) *digital operativ motståndskraft*: en finansiell enhets förmåga att bygga upp, säkerställa och se över sin operativa integritet ur ett tekniskt perspektiv genom att, direkt eller indirekt, med användning av tjänster från IKT-tredjepartsleverantörer, säkerställa hela skalan av IKT-relaterad kapacitet som behövs för att hantera säkerheten i de nätverks- och informationssystem som en finansiell enhet använder och som stöder ett fortlöpande tillhandahållande av finansiella tjänster och deras kvalitet.

(2) *nätverks- och informationssystem*: nätverks- och informationssystem enligt definitionen i artikel 4.1 i direktiv (EU) 2016/1148.

(3) *säkerhet i nätverks- och informationssystem*: säkerhet i nätverks- och informationssystem enligt definitionen i artikel 4.2 i direktiv (EU) 2016/1148.

(4) *IKT-risk*: varje rimligen identifierbar omständighet i samband med användningen av nätverks- och informationssystem – inbegripet funktionsfel, kapacitetsöverskridande, fel, avbrott, försämring, missbruk, förlust eller annan typ av skadlig eller icke skadlig händelse – som, om de inträffar, kan äventyra säkerheten i nätverks- och informationssystem, verktyg eller processer som är beroende av teknik, funktioner hos eller drift av processer, eller tillhandahållandet av tjänster, och som därigenom äventyrar integriteten eller tillgängligheten hos data, programvara eller andra

komponenter i IKT-tjänster och IKT-infrastruktur eller orsakar en sekretessöverträdelse, skada på fysisk IKT-infrastruktur eller andra negativa effekter.

(5) *informationstillgång*: en samling materiell eller immateriell skyddsvärd information.

(6) *IKT-relaterad incident*: en oförutsedd identifierad händelse i nätverks- och informationssystemen, till följd av skadlig eller icke-skadlig verksamhet, som äventyrar säkerheten i nätverks- och informationssystem, i den information som behandlas, lagras eller överförs i sådana system, eller som har negativa effekter på tillgängligheten, konfidentialiteten, kontinuiteten eller autenticiteten hos de finansiella tjänster som tillhandahålls av den finansiella enheten.

(7) *större IKT-relaterad incident*: IKT-relaterad incident med potentiellt stor negativ inverkan på nätverks- och informationssystem som stöder den finansiella enhetens kritiska funktioner.

(8) *cyberhot*: cyberhot enligt definitionen i artikel 2.8 i Europaparlamentets och rådets förordning (EU) nr 2019/881[42].

(9) *it-attack*: en uppsåtlig IKT-relaterad incident i form av ett försök att förstöra, exponera, ändra, deaktivera, stjäla eller få obehörig åtkomst till eller obehörigt utnyttja en tillgång som utförs av en fientlig aktör.

(10) *underrättelser om hot*: information som har sammanställts, omvandlats, analyserats, tolkats eller berikats för att skapa det sammanhang som krävs för beslutsfattande och som ger relevant och tillräcklig förståelse för att mildra effekterna av en IKT-relaterad incident eller ett cyberhot, inbegripet de tekniska detaljerna om en it-attack, de ansvariga för attacken och deras tillvägagångssätt och motiv.

(11) *djupförsvar*: en IKT-relaterad strategi som innefattar människor, processer och teknik för att upprätta en rad olika hinder i enhetens olika skikt och dimensioner.

(12) *sårbarhet*: en svaghet, mottaglighet eller brist hos en tillgång, ett system, en process eller en kontroll som kan utnyttjas av ett hot.

(13) *hotstyrd penetrationstestning*: en ram som efterliknar den taktik, teknik och de förfaranden som används av verkliga fientliga aktörer, som uppfattas som ett genuint cyberhot och som ger ett kontrollerat, skräddarsytt, underrättelsestyrt (”red team/rött lag”) test av de kritiska produktionssystem som är i drift hos enheten.

(14) *IKT-tredjepartsrisk*: IKT-risk som kan uppstå för en finansiell enhet i samband med dess användning av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster eller av underleverantörer till sådana leverantörer.

(15) *tredjepartsleverantör av IKT-tjänster*: ett företag som tillhandahåller digitala tjänster och datatjänster, inbegripet leverantörer av molntjänster, programvara, dataanalystjänster, datacentraler, men med undantag av leverantörer av maskinvarukomponenter och företag som har auktoriserats enligt unionsrätten och

[42] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

som tillhandahåller elektroniska kommunikationstjänster enligt definitionen i artikel 2.4 i Europaparlamentets och rådets direktiv 2018/1972/EU[43].

(16) *IKT-tjänster*: digitala tjänster och datatjänster som tillhandahålls genom IKT-system till en eller flera interna eller externa användare, inbegripet tillhandahållande av data, datainmatning, datalagring, databehandling och rapportering, dataövervakning samt databaserade affärs- och beslutsstödtjänster.

(17) *kritisk eller viktig funktion*: en funktion vars upphörande, brister eller misslyckande väsentligt skulle försämra en finansiell enhets fortsatta efterlevnad av villkoren och skyldigheterna i auktorisationen eller av dess övriga skyldigheter enligt tillämplig lagstiftning om finansiella tjänster, eller dess finansiella resultat eller sundheten eller kontinuiteten i dess tjänster och verksamhet.

(18) *kritisk tredjepartsleverantör av IKT-tjänster*: en tredjepartsleverantör av IKT-tjänster som har utsetts i enlighet med artikel 29 och som omfattas av den tillsynsram som avses i artiklarna 30–37.

(19) *tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland*: en tredjepartsleverantör av IKT-tjänster som är en juridisk person som är etablerad i ett tredjeland, som inte har etablerat verksamhet/närvaro i unionen och som har ingått ett avtal med en finansiell enhet om tillhandahållande av IKT-tjänster.

(20) *IKT-underleverantör etablerad i ett tredjeland*: IKT-underleverantör som är en juridisk person som är etablerad i ett tredjeland, som inte har etablerat verksamhet/närvaro i unionen och som har ingått ett avtal antingen med en tredjepartsleverantör av IKT-tjänster eller med en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland.

(21) *IKT-koncentrationsrisk*: exponering mot enskilda eller flera närstående kritiska tredjepartsleverantörer av IKT-tjänster som skapar ett visst beroende av sådana leverantörer, så att otillgänglighet, fel eller annan typ av brist hos dessa kan äventyra förmågan hos en finansiell enhet och i förlängningen hos unionens finansiella system som helhet att tillhandahålla kritiska funktioner eller leda till andra typer av negativa effekter, inbegripet stora förluster.

(22) *ledningsorgan*: ett ledningsorgan enligt definitionen i artikel 4.1.36 i direktiv 2014/65/EU, artikel 3.1.7 i direktiv 2013/36/EU, artikel 2.1 s i direktiv 2009/65/EG, artikel 2.1.45 i förordning (EU) nr 909/2014, artikel 3.1.20 i Europaparlamentets och rådets förordning (EU) 2016/1011[44] och artikel 3.1 u i Europaparlamentets och rådets förordning (EU) 20xx/xx[45] [förordning om marknader för kryptotillgångar], eller motsvarande personer som i praktiken leder enheten eller har nyckelfunktioner i enlighet med relevant unionslagstiftning eller nationell lagstiftning.

---

43 Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning) (EUT L 321, 17.12.2018, s. 36).

44 Europaparlamentets och rådets förordning (EU) 2016/1011 av den 8 juni 2016 om index som används som referensvärden för finansiella instrument och finansiella avtal eller för att mäta investeringsfonders resultat, och om ändring av direktiven 2008/48/EG och 2014/17/EU och förordning (EU) nr 596/2014 (EUT L 171, 29.6.2016, s. 1).

45 [*Infoga fullständig titel och EUT-uppgifter*]

(23) *kreditinstitut*: ett kreditinstitut enligt definitionen i artikel 4.1.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013[46],

(24) *värdepappersföretag*: ett värdepappersföretag enligt definitionen i artikel 4.1.1 i direktiv 2014/65/EU.

(25) *betalningsinstitut*: ett betalningsinstitut enligt definitionen i artikel 1.1. d i direktiv (EU) 2015/2366.

(26) *institut för elektroniska pengar*: institut för elektroniska pengar enligt definitionen i artikel 2.1 i Europaparlamentets och rådets direktiv 2009/110/EG[47].

(27) *central motpart*: central motpart enligt definitionen i artikel 2.1 förordning (EU) nr 648/2012.

(28) *transaktionsregister*: transaktionsregister enligt definitionen i artikel 2.2 i förordning (EU) nr 648/2012.

(29) *värdepapperscentral*: värdepapperscentral enligt definitionen i artikel 2.1.1 i förordning 909/2014.

(30) *handelsplats*: en handelsplats enligt definitionen i artikel 4.1.24 i direktiv 2014/65/EU.

(31) *förvaltare av alternativa investeringsfonder*: förvaltare av alternativa investeringsfonder enligt definitionen i artikel 4.1. b i direktiv 2011/61/EU.

(32) *förvaltningsbolag*: förvaltningsbolag enligt definitionen i artikel 2.1 b i direktiv 2009/65/EG.

(33) *leverantör av datarapporteringstjänster*: en leverantör av datarapporteringstjänster enligt definitionen i artikel 4.1.63 i direktiv 2014/65/EG.

(34) *försäkringsföretag*: försäkringsföretag enligt definitionen i artikel 13.1 i direktiv 2009/138/EG.

(35) *återförsäkringsföretag*: återförsäkringsföretag enligt definitionen i artikel 13.4 i direktiv 2009/138/EG.

(36) *försäkringsförmedlare*: försäkringsförmedlare enligt definitionen i artikel 2.3 i direktiv (EU) 2016/97.

(37) *försäkringsförmedlare som bedriver förmedling som sidoverksamhet*: försäkringsförmedlare som bedriver förmedling som sidoverksamhet enligt definitionen i artikel 2.4 i direktiv (EU) 2016/97.

(38) *återförsäkringsförmedlare*: återförsäkringsförmedlare enligt definitionen i artikel 2.5 i direktiv (EU) 2016/97.

(39) *tjänstepensionsinstitut*: tjänstepensionsinstitut enligt definitionen i artikel 1.6 i direktiv 2016/2341.

---

46 Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).

47 Europaparlamentets och rådets direktiv 2009/110/EG av den 16 september 2009 om rätten att starta och driva affärsverksamhet i institut för elektroniska pengar samt om tillsyn av sådan verksamhet, om ändring av direktiven 2005/60/EG och 2006/48/EG och om upphävande av direktiv 2000/46/EG (EUT L 267, 10.10.2009, s. 7).

(40) *kreditvärderingsinstitut*: ett kreditvärderingsinstitut enligt definitionen i artikel 3.1. a i förordning (EG) nr 1060/2009.

(41) *lagstadgad revisor*: lagstadgad revisor enligt definitionen i artikel 2 2 i direktiv 2006/43/EG.

(42) *revisionsföretag*: ett revisionsföretag enligt definitionen i artikel 2.3 i direktiv 2006/43/EG.

(43) leverantör av kryptotillgångstjänster: leverantör av kryptotillgångstjänster enligt definitionen i artikel 3.1 n i förordning (EU) 202x/xx [Publikationsbyrån: infoga hänvisning till förordningen om marknader för kryptotillgångar].

(44) emittent av kryptotillgångar: emittent av kryptotillgångar enligt definitionen i artikel 3.1 h i [EUT: infoga hänvisning till förordningen om marknader för kryptotillgångar].

(45) emittent av tillgångsanknutna token: emittent av tillgångsanknutna token enligt definitionen i artikel 3.1 i) i [EUT: infoga hänvisning till förordningen om marknader för kryptotillgångar].

(46) emittent av betydande tillgångsanknutna token: emittent av betydande tillgångsanknutna token enligt definitionen i artikel 3.1 j i [EUT: infoga hänvisning till förordningen om marknader för kryptotillgångar].

(47) *administratör av kritiska referensvärden*: administratör av kritiska referensvärden enligt definitionen i artikel x.x i förordning (EU) nr xx/202x [*EUT: infoga hänvisning till förordningen om referensvärden*].

(48) leverantör av gräsrotsfinansieringstjänster: leverantör av gräsrotsfinansieringstjänster enligt definitionen i artikel x.x i förordning (EU) 202x/xx [Publikationsbyrån: infoga hänvisning till förordningen om gräsrotsfinansiering].

(49) *värdepapperiseringsregister*: värdepapperiseringsregister enligt definitionen i artikel 2.23 i förordning (EU) 2017/2402.

(50) *mikroföretag*: mikroföretag enligt definitionen i artikel 2.3 i bilagan till rekommendation 2003/361/EG.

KAPITEL II

IKT-RISKHANTERING

AVSNITT I

Artikel 4

Styrning och organisation

1. Finansiella enheter ska ha interna styrnings- och kontrollramar som säkerställer en effektiv och ansvarsfull hantering av alla IKT-risker.

2. Den finansiella enhetens ledningsorgan ska fastställa, godkänna, övervaka och ansvara för genomförandet av alla arrangemang som rör den IKT-riskhanteringsram som avses i artikel 5.1:

   Vid tillämpning av det första stycket ska ledningsorganet

(a) ha det slutliga ansvaret för att hantera den finansiella enhetens IKT-risker,

(b) fastställa tydliga roller och ansvarsområden för alla IKT-relaterade funktioner,

(c) fastställa en lämplig risktoleransnivå för IKT-risk för den finansiella enheten, enligt vad som avses i artikel 5.9 b,

(d) godkänna, övervaka och regelbundet se över genomförandet av den IKT-kontinuitetsplan och den IKT-katastrofplan för den finansiella enheten som avses i artikel 10.1 respektive 10.3,

(e) godkänna och regelbundet se över IKT-revisionsplaner, IKT-revisioner och väsentliga ändringar av dessa,

(f) anslå och regelbundet se över lämplig budget för att uppfylla den finansiella enhetens behov av digital operativ motståndskraft när det gäller alla typer av resurser, inbegripet utbildning om IKT-risker och IKT-färdigheter för all berörd personal,

(g) godkänna och regelbundet se över den finansiella enhetens riktlinjer för arrangemang vad gäller användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster,

(h) vederbörligen informeras om de arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster, om alla relevanta planerade väsentliga ändringar som rör tredjepartsleverantörerna av IKT-tjänster och om den potentiella effekten av sådana ändringar på de kritiska eller viktiga funktioner som omfattas av dessa arrangemang, inbegripet att få en sammanfattning av riskanalysen för att bedöma effekterna av dessa ändringar,

(i) vederbörligen informeras om IKT-relaterade incidenter och deras inverkan samt om åtgärder, återställande och korrigerande åtgärder.

3. Andra finansiella enheter än mikroföretag ska inrätta en funktion för att övervaka de arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster, eller utse en medlem av den verkställande ledningen som ansvarig för att övervaka den åtföljande riskexponeringen och relevant dokumentation.

4. Medlemmarna i ledningsorganet ska regelbundet genomgå särskild utbildning för att skaffa sig tillräckliga och aktuella kunskaper och färdigheter för att förstå och bedöma IKT-risker och deras inverkan på den finansiella enhetens verksamhet.

AVSNITT II

Artikel 5

IKT-riskhanteringsram

1. Finansiella enheter ska ha en sund, heltäckande och väldokumenterad IKT-riskhanteringsram som gör det möjligt för dem att snabbt, effektivt och heltäckande hantera IKT-risker och säkerställa en hög nivå av digital operativ motståndskraft som motsvarar deras affärsbehov, storlek och komplexitet.

2. Den IKT-riskhanteringsram som avses i punkt 1 ska omfatta de strategier, riktlinjer, förfaranden, IKT-protokoll och IKT-verktyg som är nödvändiga för att på ett korrekt och effektivt sätt skydda alla relevanta fysiska komponenter och infrastrukturer,

inbegripet datormaskinvara, servrar och alla relevanta lokaler, datacentraler och känsliga angivna områden, för att säkerställa att alla dessa fysiska element är tillräckligt skyddade mot risker, inbegripet skada och obehörig åtkomst eller användning.

3. De finansiella enheterna ska minimera effekterna av IKT-risker genom att införa lämpliga strategier, riktlinjer, förfaranden, protokoll och verktyg i enlighet med IKT-riskhanteringsramen. De ska tillhandahålla fullständig och uppdaterad information om IKT-risker i enlighet med de behöriga myndigheternas krav.

4. Som en del av den IKT-riskhanteringsram som avses i punkt 1 ska andra finansiella enheter än mikroföretag införa ett system för hantering av informationssäkerhet som bygger på erkända internationella standarder och i enlighet med tillsynsriktlinjer och regelbundet se över detta system.

5. Andra finansiella enheter än mikroföretag ska säkerställa lämplig åtskillnad mellan IKT-förvaltningsfunktioner, kontrollfunktioner och interna revisionsfunktioner, i enlighet med modellen med tre försvarslinjer eller en intern riskhanterings- och kontrollmodell.

6. Den IKT-riskhanteringsram som avses i punkt 1 ska dokumenteras och ses över minst en gång per år, liksom vid uppkomsten av större IKT-relaterade incidenter, och i enlighet med tillsynsinstruktioner eller slutsatser från relevanta testnings- eller revisionsprocesser för digital operativ motståndskraft. Ramen ska förbättras fortlöpande på grundval av erfarenheterna från genomförande och övervakning.

7. Den IKT-riskhanteringsram som avses i punkt 1 ska regelbundet granskas av IKT-revisorer som har tillräckliga kunskaper, färdigheter och expertkunskaper om IKT-risker. IKT-revisionernas frekvens och inriktning ska stå i proportion till den finansiella enhetens IKT-risker.

8. En formell uppföljningsprocess ska fastställas, inklusive regler för snabb kontroll och snabbt åtgärdande av kritiska resultat från IKT-revision, med beaktande av slutsatserna från granskningen, samtidigt som vederbörlig hänsyn tas till arten, omfattningen och komplexiteten hos de finansiella enheternas tjänster och verksamhet.

9. Den IKT-riskhanteringsram som avses i punkt 1 ska omfatta en strategi för digital motståndskraft där det anges hur ramen genomförs. För detta ändamål ska strategin innefatta metoderna för att hantera IKT-risker och uppnå specifika IKT-mål på följande sätt:

   (a) Förklara hur IKT-riskhanteringsramen stöder den finansiella enhetens affärsstrategi och mål.

   (b) Fastställa ristoleransknivån för IKT-risk i enlighet med den finansiella enhetens riskbenägenhet och analysera toleransen mot effekterna av IKT-avbrott.

   (c) Fastställa tydliga informationssäkerhetsmål.

   (d) Förklara IKT-referensarkitekturen och eventuella förändringar som krävs för att uppnå specifika verksamhetsmål.

   (e) Beskriva de olika mekanismer som har införts för att upptäcka, skydda och förebygga effekterna av IKT-relaterade incidenter.

(f) Lägga fram bevis för antalet rapporterade större IKT-relaterade incidenter och de förebyggande åtgärdernas effektivitet.

(g) Utforma en holistisk strategi med flera olika leverantörer av IKT-tjänster på enhetsnivå som visar de viktigaste beroendena av tredjepartsleverantörer av IKT-tjänster och förklarar logiken bakom upphandlingsmixen av tredjepartsleverantörer av IKT-tjänster

(h) Genomföra tester av den digitala operativa motståndskraften.

(i) Beskriva en kommunikationsstrategi vid IKT-relaterade incidenter.

10. Efter godkännande av behöriga myndigheter får de finansiella enheterna delegera uppgiften att kontrollera efterlevnaden av IKT-riskhanteringskraven till koncerninterna eller externa företag.

Artikel 6

IKT-system, IKT-protokoll och IKT-verktyg

1. De finansiella enheterna ska använda och upprätthålla uppdaterade IKT-system, IKT-protokoll och IKT-verktyg som uppfyller följande villkor:

(a) Systemen och verktygen är lämpliga med hänsyn till arten, variationen, komplexiteten och omfattningen hos de transaktioner som ligger till grund för deras verksamhet.

(b) De är tillförlitliga.

(c) De har tillräcklig kapacitet för att korrekt behandla de uppgifter som krävs för att bedriva verksamheten och tillhandahålla tjänster i tid, och vid behov hantera toppar i order-, meddelande- eller transaktionsvolymer, även vid införande av ny teknik.

(d) De är tekniskt motståndskraftiga för att på lämpligt sätt hantera ytterligare informationsbehandlingsbehov när detta krävs under stressade marknadsförhållanden eller andra ogynnsamma situationer.

2. Om de finansiella enheterna använder internationellt erkända tekniska standarder och branschledande metoder för informationssäkerhet och intern IKT-kontroll ska de använda dessa standarder och rutiner i linje med eventuella relevanta tillsynsrekommendationer om deras införlivande.

Artikel 7

Identifiering

1. Som en del av den IKT-riskhanteringsram som avses i artikel 5.1 ska de finansiella enheterna identifiera, klassificera och på lämpligt sätt dokumentera alla IKT-relaterade affärsfunktioner, de informationstillgångar som stöder dessa funktioner och IKT-systemets konfigurationer och kopplingar till interna och externa IKT-system. De finansiella enheterna ska vid behov, och minst en gång per år, granska lämpligheten i klassificeringen av informationstillgångarna och av all relevant dokumentation.

2. De finansiella enheterna ska fortlöpande identifiera alla källor till IKT-risker, särskilt riskexponeringen mot och från andra finansiella enheter, och bedöma cyberhot och

IKT-sårbarheter som är relevanta för deras IKT-relaterade affärsfunktioner och informationstillgångar. De finansiella enheterna ska regelbundet och minst en gång per år se över de riskscenarier som påverkar dem.

3. Andra finansiella enheter än mikroföretag ska göra en riskbedömning av varje större förändring av nätverks- och informationssystemets infrastruktur, av de processer eller förfaranden som påverkar deras funktioner, stödprocesser eller informationstillgångar.

4. De finansiella enheterna ska identifiera alla konton för IKT-system, inbegripet konton på fjärrplatser, nätresurser och maskinvaruutrustning, och kartlägga fysisk utrustning som anses vara kritisk. De ska kartlägga IKT-tillgångarnas konfiguration samt kopplingarna och det ömsesidiga beroendet mellan de olika IKT-tillgångarna.

5. De finansiella enheterna ska identifiera och dokumentera alla processer som är beroende av tredjepartsleverantörer av IKT-tjänster och identifiera kopplingar till tredjepartsleverantörer av IKT-tjänster.

6. Vid tillämpning av punkterna 1, 4 och 5 ska de finansiella enheterna upprätthålla och regelbundet uppdatera relevanta inventeringar.

7. Andra finansiella enheter än mikroföretag ska regelbundet, och minst en gång per år, genomföra en särskild IKT-riskbedömning av alla befintliga IKT-system, särskilt före och efter sammanlänkning av gamla och nya tekniker, tillämpningar eller system.

Artikel 8

Skydd och förebyggande

1. För att skydda IKT-systemen på lämpligt sätt och organisera motåtgärder ska de finansiella enheterna kontinuerligt övervaka och kontrollera IKT-systemens och IKT-verktygens funktion och ska minimera effekterna av sådana risker genom att införa lämpliga verktyg, riktlinjer och förfaranden för IKT-säkerhet.

2. De finansiella enheterna ska utforma, upphandla och genomföra IKT-relaterade säkerhetsstrategier, riktlinjer, förfaranden, protokoll och verktyg som i synnerhet syftar till att säkerställa IKT-systemens motståndskraft, kontinuitet och tillgänglighet, och upprätthålla höga standarder för säkerhet, konfidentialitet och integritet hos data, oberoende av om de är i vila, i bruk eller under överföring.

3. För att uppnå de mål som avses i punkt 2 ska de finansiella enheterna använda den senaste IKT-teknik och de senaste IKT-processer som

   (a) garanterar skyddet vid informationsöverföring,

   (b) minimerar risken för förvanskning eller förlust av uppgifter, obehörig åtkomst och tekniska brister som kan hindra affärsverksamheten,

   (c) förhindrar informationsläckage,

   (d) säkerställer att uppgifterna skyddas mot bristfällig förvaltning eller processrelaterade risker, inbegripet otillräcklig dokumentation.

4. Som en del av den IKT-riskhanteringsram som avses i artikel 5.1 ska de finansiella enheterna

(a) utarbeta och dokumentera riktlinjer för informationssäkerhet där det fastställs regler för att skydda konfidentialiteten, integriteten och tillgängligheten i deras respektive kunders IKT-resurser-, data- och informationstillgångar,

(b) enligt en riskbaserad strategi upprätta en sund förvaltning av nätverk och infrastruktur med hjälp av lämpliga tekniker, metoder och protokoll, inbegripet införande av automatiserade mekanismer för att isolera berörda informationstillgångar vid it-attacker,

(c) genomföra riktlinjer för att begränsa den fysiska och virtuella åtkomsten till IKT-systemets resurser och data till vad som krävs för legitima och godkända funktioner och verksamheter, och för detta ändamål fastställa en uppsättning riktlinjer, förfaranden och kontroller för åtkomsträttigheter och en sund förvaltning av dessa,

(d) genomföra riktlinjer och protokoll för starka autentiseringsmekanismer, baserade på relevanta standarder och särskilda kontrollsystem för att förhindra åtkomst till kryptografiska nycklar där data krypteras på grundval av resultat från godkända processer för klassificering och riskbedömning,

(e) genomföra riktlinjer, förfaranden och kontroller för hantering av IKT-förändringar, inbegripet ändringar av programvara, maskinvara, fasta programvarukomponenter, system eller säkerhetsändringar, som bygger på en riskbedömningsmetod och är en integrerad del av den finansiella enhetens övergripande förändringshanteringsprocess, för att säkerställa att alla ändringar av IKT-system registreras, testas, bedöms, godkänns, genomförs och verifieras på ett kontrollerat sätt,

(f) ha lämpliga och heltäckande strategier för programfixar och uppdateringar.

Vid tillämpning av led b ska de finansiella enheterna utforma infrastrukturen för nätanslutning på ett sätt som gör att den omedelbart kan avskiljas och ska säkerställa att den är uppdelad och segmenterad i syfte att minimera och förhindra spridning, särskilt för sammanlänkade finansiella processer.

Vid tillämpning av led e ska processen för hantering av IKT-förändringar godkännas av lämpliga ledningsnivåer och ska ha särskilda protokoll som möjliggör akuta ändringar.

Artikel 9

Upptäckt

1. De finansiella enheterna ska ha mekanismer för att snabbt upptäcka onormal verksamhet i enlighet med artikel 15, inbegripet frågor som rör IKT-nätverkens prestanda och IKT-relaterade incidenter, och för att identifiera alla potentiella väsentliga felkritiska systemdelar (*single points of failure*).

   Alla upptäcktsmekanismer som avses i första stycket ska testas regelbundet i enlighet med artikel 22.

2. De upptäcktsmekanismer som avses i punkt 1 ska möjliggöra flera kontrollnivåer, innehålla fastställda varningströskelvärden och varningskriterier för att utlösa processer för upptäckt av IKT-relaterade incidenter och för hantering av IKT-relaterade incidenter samt automatiska varningsmekanismer för relevant personal med ansvar för hantering av IKT-relaterade incidenter.

3. De finansiella enheterna ska avsätta tillräckligt med resurser och kapacitet, med hänsyn till deras storlek, affärs- och riskprofiler, för att övervaka användarnas verksamhet, förekomsten av IKT-avvikelser och IKT-relaterade incidenter, särskilt it-attacker.

4. De finansiella enheter som avses i artikel 2.1 ska dessutom ha system som på ett effektivt sätt gör det möjligt att kontrollera handelsrapporters fullständighet, hitta fall av utelämnad information och uppenbara fel och begära omsändning av alla sådana felaktiga rapporter.

Artikel 10

Åtgärder och återställande

1. Som en del av den IKT-riskhanteringsram som avses i artikel 5.1 och på grundval av identifieringskraven i artikel 7 ska finansiella enheter införa en särskild och heltäckande IKT-kontinuitetsplan som en integrerad del av den finansiella enhetens operativa kontinuitetsplan.

2. De finansiella enheterna ska genomföra den IKT-kontinuitetsplan som avses i punkt 1 genom särskilda, lämpliga och dokumenterade arrangemang, planer, förfaranden och mekanismer som syftar till att

   (a) registrera alla IKT-relaterade incidenter,

   (b) säkerställa kontinuiteten i den finansiella enhetens kritiska funktioner,

   (c) snabbt, lämpligt och effektivt reagera på och lösa alla IKT-relaterade incidenter, särskilt men inte begränsat till it-attacker, på ett sätt som begränsar skador och prioriterar återupptagande av verksamhet och återställningsåtgärder,

   (d) utan dröjsmål aktivera särskilda planer som möjliggör begränsningsåtgärder, processer och teknik som är anpassade till varje typ av IKT-relaterad incident och som förhindrar ytterligare skador, samt skräddarsydda åtgärds- och återställningsförfaranden som har fastställts i enlighet med artikel 11,

   (e) beräkna preliminära effekter, skador och förluster,

   (f) fastställa kommunikations- och krishanteringsinsatser som säkerställer att uppdaterad information överförs till all berörd intern personal och alla externa berörda parter i enlighet med artikel 13 och rapporteras till behöriga myndigheter i enlighet med artikel 17.

3. Som en del av den IKT-riskhanteringsram som avses i artikel 5.1 ska de finansiella enheterna genomföra en åtföljande IKT-katastrofplan som, när det gäller andra finansiella enheter än mikroföretag, ska bli föremål för oberoende granskningar.

4. De finansiella enheterna ska införa, upprätthålla och regelbundet testa lämpliga IKT-kontinuitetsplaner, särskilt när det gäller kritiska eller viktiga funktioner som har utkontrakterats eller kontrakterats genom avtal med tredjepartsleverantörer av IKT-tjänster.

5. Som en del av sin övergripande IKT-riskhantering ska de finansiella enheterna

   (a) testa IKT-kontinuitetsplanen och IKT-katastrofplanen minst en gång per år och efter omfattande ändringar av IKT-systemen,

   (b) testa de kriskommunikationsplaner som har upprättats i enlighet med artikel 13.

Vid tillämpning av led a ska andra finansiella enheter än mikroföretag i testplanerna inkludera scenarier för it-attacker och byten mellan den primära IKT-infrastrukturen och den reservkapacitet, de säkerhetskopior och reservanläggningar som krävs för att uppfylla de skyldigheter som anges i artikel 11.

De finansiella enheterna ska regelbundet se över sin IKT-kontinuitetsplan och IKT-katastrofplan med hänsyn till resultatet av tester som har utförts i enlighet med första stycket och rekommendationer från revisionskontroller eller tillsynsgranskningar.

6. Andra finansiella enheter än mikroföretag ska ha en krishanteringsfunktion som, om deras IKT-kontinuitetsplan eller IKT-katastrofplan aktiveras, ska innehålla tydliga förfaranden för hantering av intern och extern kriskommunikation i enlighet med artikel 13.

7. De finansiella enheterna ska dokumentera den verksamhet som pågår före och under avbrott när IKT-kontinuitetsplanen eller IKT-katastrofplanen aktiveras. Sådana register ska vara lättillgängliga.

8. De finansiella enheter som avses i artikel 2.1 f ska förse de behöriga myndigheterna med kopior av resultatet av de IKT-kontinuitetstester eller liknande tester som har genomförts under den granskade perioden.

9. Andra finansiella enheter än mikroföretag ska rapportera alla kostnader och förluster som orsakas av IKT-avbrott och IKT-relaterade incidenter till de behöriga myndigheterna.

Artikel 11

Säkerhetskopieringsstrategier och återställningsmetoder

1. För att säkerställa att IKT-system kan återställas med minsta möjliga driftstopp och begränsade avbrott ska finansiella enheter som en del i sin IKT-riskhanteringsram utarbeta

   (a) riktlinjer för säkerhetskopiering där de anger omfattningen av de data ska säkerhetskopieras och minimifrekvensen för säkerhetskopieringen, baserat på informationens kritikalitet eller uppgifternas känslighet,

   (b) återställningsmetoder.

2. Behandlingen i säkerhetskopieringssystem bör påbörjas så snart som möjligt, förutsatt att detta inte äventyrar säkerheten i nätverks- och informationssystemen eller uppgifternas integritet eller konfidentialitet.

3. När de finansiella enheterna återställer säkerhetskopierade data med hjälp av egna system ska de använda IKT-system som har en annan operativ miljö än huvudsystemet, som inte är direkt kopplad till huvudsystemet och som har ett säkert skydd mot obehörig åtkomst eller IKT-förvanskning.

   För de finansiella enheter som avses i artikel 2.1 g ska återställningsplanerna göra det möjligt att återställa alla transaktioner så som de var vid tidpunkten för avbrottet, så att den centrala motpartens verksamhet är fortsatt säker och avvecklingen kan fullföljas vid fastställd tidpunkt.

4. De finansiella enheterna ska upprätthålla IKT-reservkapacitet med resurser och funktioner som är tillräckliga och ändamålsenliga för att tillgodose verksamhetens behov.

5. De finansiella enheter som avses i artikel 2.1 f ska ha eller säkerställa att deras IKT-tredjepartsleverantörer har minst ett sekundärt driftsställe med tillfredsställande resurser, kapacitet, funktioner och lämpliga personalarrangemang som räcker för verksamhetens behov.

   Det sekundära driftsstället ska

   (a) vara beläget på ett geografiskt avstånd från det primära driftsstället som gör det möjligt för det sekundära driftsstället att ha en distinkt riskprofil och hindrar det från att påverkas av den händelse som påverkar det primära driftsstället,

   (b) kunna säkra kontinuiteten i kritiska tjänster som är identiska med det primära driftsstället eller tillhandahålla den servicenivå som är nödvändig för att säkerställa att den finansiella enheten kan bedriva sin kritiska verksamhet inom ramen för återställningsmålen,

   (c) vara omedelbart tillgängligt för den finansiella enhetens personal i syfte att säkra driftskontinuitet i dess kritiska tjänster om det primära driftsstället inte är tillgängligt.

6. När de finansiella enheterna fastställer återställningstid och punktmål för varje funktion ska de ta hänsyn till den eventuella övergripande inverkan på marknadseffektiviteten. Tidsmålen ska säkerställa att de överenskomna servicenivåerna uppnås i extrema scenarier.

7. När finansiella enheter återställer verksamheten efter en IKT-relaterad incident ska de göra flera kontroller, inbegripet avstämningar, för att säkerställa att dataintegriteten håller högsta nivå. Dessa kontroller ska också utföras när data från externa berörda parter rekonstrueras för att säkerställa att alla data stämmer överens mellan systemen.

Artikel 12

Lärande och utveckling

1. De finansiella enheterna ska ha lämplig kapacitet och personal i förhållande till sin storlek, verksamhets- och riskprofil för att samla in information om sårbarheter och cyberhot, IKT-relaterade incidenter, särskilt it-attacker, och analysera deras sannolika inverkan på den digitala operativa motståndskraften.

2. De finansiella enheterna ska införa efterhandsöversyner av IKT-relaterade incidenter efter betydande IKT-avbrott i sin kärnverksamhet för att analysera orsakerna till avbrotten och identifiera nödvändiga förbättringar av IKT-verksamheten eller i den IKT-kontinuitetsplan som avses i artikel 10.

   När ändringar genomförs ska andra finansiella enheter än mikroföretag underrätta de behöriga myndigheterna om dessa ändringar.

   De efterhandsöversyner av IKT-relaterade incidenter som avses i första stycket ska fastställa om de fastställda förfarandena följdes och om de åtgärder som vidtogs var effektiva, bl.a. när det gäller

   (a) svarstiden för att reagera på säkerhetsvarningar och fastställa konsekvenserna av IKT-relaterade incidenter och deras allvarlighetsgrad,

   (b) kvalitet och snabbhet i utförandet av kriminaltekniska analyser,

   (c) incidenteskaleringens effektivitet inom den finansiella enheten,

(d) effektiviteten i intern och extern kommunikation.

3. Lärdomar av den testning av digital operativ motståndskraft som har utförts i enlighet med artiklarna 23 och 24 och av verkliga IKT-relaterade incidenter, särskilt it-attacker, samt utmaningar i samband med aktivering av kontinuitetsplaner eller återställningsplaner och relevant information som har utväxlats med motparter och bedömts under tillsynsgranskningar, ska införlivas fortlöpande i IKT-riskbedömningsprocessen. Dessa resultat ska omsättas i lämpliga översyner av relevanta delar i den IKT-riskhanteringsram som avses i artikel 5.1.

4. De finansiella enheterna ska övervaka effektiviteten i genomförandet av den strategi för digital motståndskraft som anges i artikel 5.9. De ska kartlägga IKT-riskernas utveckling över tid, analysera IKT-incidenters frekvens, typ, omfattning och utveckling, särskilt it-attacker och deras mönster, i syfte att förstå graden av IKT-riskexponering och öka den finansiella enhetens cybermognad och beredskap.

5. Högre IKT-personal ska minst en gång per år rapportera till ledningsorganet om de resultat som avses i punkt 3 och lägga fram rekommendationer.

6. De finansiella enheterna ska utarbeta program för medvetenhet om IKT-säkerhet och utbildning om digital operativ motståndskraft som obligatoriska moduler i sina personalutbildningsprogram. Dessa ska gälla för alla anställda och personer i ledande ställning.

   De finansiella enheterna ska kontinuerligt övervaka relevant teknisk utveckling, även i syfte att förstå vilka konsekvenser införandet av sådan ny teknik kan få för IKT-säkerhetskraven och den digitala operativa motståndskraften. De ska hålla sig uppdaterade om de senaste IKT-riskhanteringsprocesserna för att effektivt motverka nuvarande eller nya former av it-attacker.

Artikel 13

Kommunikation

1. Som en del av den IKT-riskhanteringsram som avses i artikel 5.1 ska finansiella enheter ha kommunikationsplaner som gör det möjligt att på ett ansvarsfullt sätt informera kunder och motparter samt allmänheten om IKT-relaterade incidenter eller större sårbarheter, beroende på vad som är lämpligt.

2. Som en del av den IKT-riskhanteringsram som avses i artikel 5.1 ska finansiella enheter genomföra kommunikationsstrategier för personal och externa berörda parter. I sina kommunikationsstrategier för personalen ska hänsyn tas till behovet av att skilja mellan personal som deltar i IKT-riskhantering, framför allt i åtgärder och återställande, och personal som behöver information.

3. Minst en person i enheten ska ha i uppgift att genomföra kommunikationsstrategin för IKT-relaterade incidenter och fungera som talesperson gentemot allmänheten och medierna i detta syfte.

Artikel 14

Ytterligare harmonisering av verktyg, metoder, processer och riktlinjer för IKT-riskhantering

Europeiska bankmyndigheten (EBA), Europeiska värdepappers- och marknadsmyndigheten (Esma) och Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) ska, i samråd

med Europeiska unionens cybersäkerhetsbyrå (Enisa), utarbeta förslag till tekniska standarder för tillsyn i följande syften:

(a) Närmare specificera delar som ska ingå i de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 8.2 i syfte att säkerställa säkerheten i nätverk, möjliggöra lämpliga skyddsåtgärder mot intrång och missbruk av uppgifter, bevara uppgifternas autenticitet och integritet, inbegripet krypteringsmetoder, och garantera en korrekt och snabb dataöverföring utan större avbrott.

(b) Föreskriva hur de riktlinjer, förfaranden och verktyg för IKT-säkerhet som avses i artikel 8.2 ska innefatta säkerhetskontroller i systemen från början (inbyggd säkerhet), möjliggöra anpassningar till det föränderliga hotlandskapet och möjliggöra användning av teknik för djupförsvar.

(c) Närmare specificera de lämpliga tekniker, metoder och protokoll som avses i artikel 8.4 b.

(d) Utveckla ytterligare komponenter i den hantering av kontroll av åtkomsträttigheter som avses i artikel 8.4 c och tillhörande personalpolitik där det specificeras åtkomsträttigheter, förfaranden för beviljande och återkallande av rättigheter, övervakning av onormalt beteende i förhållande till IKT-risker genom lämpliga indikatorer, inbegripet mönster för nätanvändning, tidpunkter, it-verksamhet och okänd utrustning.

(e) Vidareutveckla de delar som anges i artikel 9.1 för att möjliggöra en snabb upptäckt av onormal verksamhet och de kriterier som avses i artikel 9.2 som utlöser processer för upptäckt och hantering av IKT-relaterade incidenter.

(f) Närmare specificera komponenterna i den IKT-kontinuitetsplan som avses i artikel 10.1.

(g) Närmare specificera de tester av IKT-kontinuitetsplaner som avses i artikel 10.5 för att säkerställa att tillräckligt stor hänsyn tas till scenarier där kvaliteten på tillhandahållandet av en kritisk eller viktig funktion försämras till en oacceptabel nivå eller tillhandahållandet avbryts, och till de potentiella konsekvenserna av insolvens eller andra fel hos en relevant tredjepartsleverantör av IKT-tjänster och, i förekommande fall, de politiska riskerna i respektive leverantörers jurisdiktioner.

(h) Närmare specificera komponenterna i den IKT-katastrofplan som avses i artikel 10.3.

EBA, Esma och Eiopa ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den [*EUT: infoga datum ett år efter dagen för ikraftträdandet*].

Kommissionen ges befogenhet att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

KAPITEL III

IKT-RELATERADE INCIDENTER

HANTERING, KLASSIFICERING och RAPPORTERING

Artikel 15

Process för hantering av IKT-relaterade incidenter

1. De finansiella enheterna ska inrätta och genomföra en process för hantering av IKT-relaterade incidenter för att upptäcka, hantera och meddela IKT-relaterade incidenter samt även införa indikatorer för tidig varning som larm.

2. Finansiella enheter ska inrätta lämpliga förfaranden för att säkerställa en konsekvent och integrerad övervakning, hantering och uppföljning av IKT-relaterade incidenter, så att grundorsakerna identifieras och undanröjs i syfte att förhindra att sådana incidenter inträffar.

3. Den process för hantering av IKT-relaterade incidenter som avses i punkt 1 ska

   (a) innehålla fastställda förfaranden för att identifiera, spåra, logga, kategorisera och klassificera IKT-relaterade incidenter i enlighet med deras prioritetsordning och de berörda tjänsternas allvar och kritikalitet i enlighet med de kriterier som avses i artikel 16.1,

   (b) innehålla en fördelning av roller och ansvarsområden som behöver aktiveras för olika IKT-relaterade incidenttyper och scenarier,

   (c) innehålla planer för kommunikation till personal, externa berörda parter och medier i enlighet med artikel 13 och för anmälan till kunder, interna eskaleringsförfaranden, inbegripet IKT-relaterade kundklagomål, samt för tillhandahållande av information till finansiella enheter som fungerar som motparter, beroende på vad som är lämpligt,

   (d) säkerställa att större IKT-relaterade incidenter rapporteras till relevant högre ledning och att ledningsorganet informeras om större IKT-relaterade incidenter, med en förklaring av effekter, åtgärder och ytterligare kontroller som ska fastställas till följd av IKT-relaterade incidenter,

   (e) innehålla fastställda förfaranden för åtgärder vid IKT-relaterade incidenter för att mildra effekterna och säkerställa att tjänsterna snabbt kan tas i drift och är säkra.

Artikel 16

Klassificering av IKT-relaterade incidenter

1. Finansiella enheter ska klassificera IKT-relaterade incidenter och fastställa deras inverkan på grundval av följande kriterier:

   (a) Antalet användare eller finansiella motparter som påverkas av det avbrott som har orsakats av den IKT-relaterade incidenten, och om anseendet har påverkats av den IKT-relaterade incidenten.

   (b) Den IKT-relaterade incidentens varaktighet, inklusive driftstopp.

(c) Den geografiska spridningen med avseende på de områden som påverkas av den IKT-relaterade incidenten, särskilt om den påverkar fler än två medlemsstater.

(d) De dataförluster som den IKT-relaterade incidenten medför, t.ex. integritetsförlust, förlust av konfidentialitet eller förlust av tillgänglighet.

(e) Hur allvarlig den IKT-relaterade incidentens inverkan är på den finansiella enhetens IKT-system.

(f) De berörda tjänsternas kritikalitet, inbegripet den finansiella enhetens transaktioner och verksamhet.

(g) De ekonomiska effekterna av den IKT-relaterade incidenten i absoluta och relativa tal.

2. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén för de europeiska tillsynsmyndigheterna (nedan kallad *den gemensamma kommittén*) och efter samråd med Europeiska centralbanken (ECB) och Enisa, utarbeta gemensamma förslag till tekniska standarder för tillsyn som ytterligare specificerar följande:

(a) De kriterier som anges i punkt 1, inbegripet väsentlighetströsklar för att fastställa större IKT-relaterade incidenter som omfattas av rapporteringsskyldigheten i artikel 17.1.

(b) De kriterier som de behöriga myndigheterna ska tillämpa för att bedöma större IKT-relaterade incidenters relevans för andra medlemsstaters jurisdiktioner och de detaljer i rapporter om IKT-relaterade incidenter som ska delas med andra behöriga myndigheter i enlighet med artikel 17.5 och 17.6.

3. När de europeiska tillsynsmyndigheterna utarbetar de gemensamma förslag till tekniska standarder för tillsyn som avses i punkt 2 ska de ta hänsyn internationella standarder och specifikationer som har utarbetats och offentliggjorts av Enisa, inbegripet, när så är lämpligt, specifikationer för andra ekonomiska sektorer.

De europeiska tillsynsmyndigheterna ska överlämna dessa gemensamma förslag till tekniska standarder för tillsyn till kommissionen senast den [*Publikationsbyrån: infoga datum ett år efter dagen för ikraftträdandet*].

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i punkt 2 i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 17

Rapportering av större IKT-relaterade incidenter

1. De finansiella enheterna ska rapportera större IKT-relaterade incidenter till den relevanta behöriga myndighet som avses i artikel 41 inom de tidsfrister som anges i punkt 3.

Vid tillämpning av första stycket ska de finansiella enheterna, efter att ha samlat in och analyserat all relevant information, utarbeta en incidentrapport med hjälp av den mall som avses i artikel 18 och överlämna den till den behöriga myndigheten.

Rapporten ska innehålla all information som är nödvändig för att den behöriga myndigheten ska kunna fastställa betydelsen av den större IKT-relaterade incidenten och bedöma eventuella gränsöverskridande konsekvenser.

2. Om en större IKT-relaterad incident har eller kan påverka tjänsteanvändares och kunders ekonomiska intressen ska de finansiella enheterna utan onödigt dröjsmål informera sina tjänsteanvändare och kunder om den större IKT-relaterade incidenten och så snart som möjligt informera dem om alla åtgärder som har vidtagits för att mildra de negativa effekterna av en sådan incident.

3. De finansiella enheterna ska till den behöriga myndighet som avses i artikel 41 överlämna följande:

   (a) En första anmälan, utan dröjsmål, men inte senare än handelsdagens slut, eller, i händelse av en större IKT-relaterad incident som ägde rum senare än två timmar före handelsdagens slut, senast fyra timmar från början av nästa handelsdag, eller, om rapporteringskanaler inte finns tillgängliga, så snart de blir tillgängliga.

   (b) En delrapport, senast en vecka efter den första anmälan som avses i led a, vid behov åtföljd av uppdaterade anmälningar varje gång en relevant statusuppdatering finns tillgänglig, samt på särskild begäran av den behöriga myndigheten.

   (c) En slutrapport, när analysen av grundorsakerna har slutförts, oavsett om begränsande åtgärder redan har vidtagits eller inte, och när de faktiska påverkanssiffrorna finns tillgängliga för att ersätta uppskattningar, dock senast en månad från det att den första rapporten sändes.

4. De finansiella enheterna får endast delegera rapporteringsskyldigheterna enligt denna artikel till en tredjepartsleverantör av tjänster efter godkännande av den relevanta behöriga myndighet som avses i artikel 41.

5. Efter mottagandet av den rapport som avses i punkt 1 ska den behöriga myndigheten utan onödigt dröjsmål lämna närmare uppgifter om incidenten till

   (a) EBA, Esma eller Eiopa, beroende på vad som är lämpligt,

   (b) ECB, när så är lämpligt, när det gäller de finansiella enheter som avses i artikel 2.1 a, b och c, och

   (c) den gemensamma kontaktpunkt som har utsetts enligt artikel 8 i direktiv (EU) 2016/1148.

6. EBA, Esma eller Eiopa och ECB ska bedöma den större IKT-relaterade incidentens relevans för andra berörda offentliga myndigheter och så snart som möjligt underrätta dem om detta. ECB ska underrätta medlemmarna i Europeiska centralbankssystemet om frågor som är relevanta för betalningssystemet. På grundval av denna underrättelse ska de behöriga myndigheterna vid behov vidta alla nödvändiga åtgärder för att skydda det finansiella systemets omedelbara stabilitet.

Artikel 18

Harmonisering av rapporteringsinnehåll och mallar

1. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och efter samråd med Enisa och ECB, utarbeta

   (a) gemensamma förslag till tekniska standarder för tillsyn för att

      (1) fastställa innehållet i rapporteringen av större IKT-relaterade incidenter,

(2) närmare angivelser av på vilka villkor finansiella enheter får delegera de rapporteringsskyldigheter som anges i detta kapitel till en tredjepartsleverantör, efter förhandsgodkännande från den behöriga myndigheten,

(b) gemensamma förslag till tekniska standarder för genomförande i syfte att fastställa standardformulär, mallar och förfaranden för finansiella enheter för rapportering av en större IKT-relaterad incident.

De europeiska tillsynsmyndigheterna ska överlämna de gemensamma förslag till tekniska standarder för tillsyn som avses i punkt 1 a och de gemensamma förslag till tekniska genomförandestandarder som avses i punkt 1 b till kommissionen senast den xx 202x *[Publikationsbyrån: infoga datum ett år efter dagen för ikraftträdandet*].

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de gemensamma tekniska standarder för tillsyn som avses i punkt 1 a i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1095/2010 och (EU) nr 1094/2010.

Kommissionen ges befogenhet att anta de tekniska standarder för genomförande som avses i punkt 1 b i enlighet med artikel 15 i förordningarna (EU) nr 1093/2010, (EU) nr 1095/2010 och (EU) nr 1094/2010.

Artikel 19

Centralisering av rapportering av större IKT-relaterade incidenter

1. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med ECB och Enisa, utarbeta en gemensam rapport med en bedömning av genomförbarheten av ytterligare centralisering av incidentrapporteringen genom inrättandet av en gemensam EU-knutpunkt för finansiella enheters rapportering av större IKT-relaterade incidenter. Rapporten ska innehålla en undersökning av olika sätt att underlätta flödet av IKT-relaterad incidentrapportering, minska de därmed sammanhängande kostnaderna och underbygga tematiska analyser i syfte att öka konvergensen i tillsynen.

2. Den rapport som avses i punkt 1 ska innehålla minst följande:

(a) Förutsättningar för att inrätta en sådan EU-knutpunkt.

(b) Fördelar, begränsningar och eventuella risker.

(c) Inslag i den operativa förvaltningen.

(d) Villkor för medlemskap.

(e) Villkor för att finansiella enheter och nationella behöriga myndigheter ska få tillgång till EU-knutpunkten.

(f) En preliminär bedömning av de finansiella kostnaderna för inrättandet av den operativa plattformen till stöd för EU-knutpunkten, inklusive den sakkunskap som krävs.

3. De europeiska tillsynsmyndigheterna ska överlämna den rapport som avses i punkt 1 till kommissionen, Europaparlamentet och rådet senast den xx 202x *[EUT: infoga datum tre år efter dagen för ikraftträdandet*].

Artikel 20

Återkoppling från tillsynsmyndigheterna

1. När den behöriga myndigheten har mottagit en rapport enligt artikel 17.1 ska den bekräfta mottagandet av anmälan och så snart som möjligt lämna all nödvändig återkoppling eller vägledning till den finansiella enheten, särskilt för att diskutera avhjälpande åtgärder på enhetsnivå eller sätt att minimera de negativa effekterna inom alla olika sektorer.

2. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén årligen lämna anonymiserade och aggregerade rapporter om anmälningar av IKT-relaterade incidenter som har mottagits från behöriga myndigheter, med angivande av åtminstone antalet IKT-relaterade större incidenter, deras art, inverkan på finansiella enheters eller kunders verksamhet, kostnader och avhjälpande åtgärder som har vidtagits.

   De europeiska tillsynsmyndigheterna ska utfärda varningar och ta fram statistik på hög nivå till stöd för IKT-hot- och sårbarhetsbedömningar.

KAPITEL IV

TESTNING AV DIGITAL OPERATIV MOTSTÅNDSKRAFT

Artikel 21

Allmänna krav för testning av digital operativ motståndskraft

1. För att bedöma beredskapen för IKT-relaterade incidenter, identifiera svagheter, brister eller luckor i den digitala operativa motståndskraften och snabbt genomföra korrigerande åtgärder ska finansiella enheter, med hänsyn till sin storlek, affärsprofil och riskprofil, inrätta, upprätthålla och se över ett sunt och heltäckande program för testning av digital operativ motståndskraft som en integrerad del av den IKT-riskhanteringsram som avses i artikel 5.

2. Programmet för testning av digital operativ motståndskraft ska omfatta en rad bedömningar, tester, metoder, praxis och verktyg som ska tillämpas i enlighet med bestämmelserna i artiklarna 22 och 23.

3. De finansiella enheterna ska följa en riskbaserad metod när de genomför det testprogram för digital operativ motståndskraft som avses i punkt 1, med hänsyn tagen till IKT-riskernas utveckling, eventuella specifika risker som den finansiella enheten är eller kan bli exponerad för, kritikaliteten hos informationstillgångar och tillhandahållna tjänster samt varje annan faktor som den finansiella enheten anser lämplig.

4. De finansiella enheterna ska se till att testerna utförs av oberoende parter, oavsett om de är interna eller externa.

5. De finansiella enheterna ska fastställa förfaranden och riktlinjer för prioritering, klassificering och åtgärdande av alla problem som framkommer under genomförandet av testerna och ska införa interna valideringsmetoder för att säkerställa att alla identifierade svagheter, brister eller luckor åtgärdas fullt ut.

6. De finansiella enheterna ska minst en gång per år testa alla kritiska IKT-system och IKT-tillämpningar.

Artikel 22

Testning av IKT-verktyg och IKT-system

1. Det program för testning av digital operativ motståndskraft som avses i artikel 21 ska innehålla bestämmelser om utförande av en fullständig uppsättning lämpliga tester, inbegripet sårbarhetsanalyser och skanningar, analyser av öppen källkod, nätverkssäkerhetsbedömningar, gapanalyser, fysiska säkerhetsgranskningar, frågeformulär och programvarulösningar för skanning, källkodsgranskningar när så är möjligt, scenariobaserade tester, kompatibilitetstester, prestandastester, tester ändpunkt till ändpunkt (*end-to-end*) och penetrationstester.

2. De finansiella enheter som avses i artikel 2.1 f och g ska utföra sårbarhetsbedömningar före eventuell användning eller omfördelning av nya eller befintliga tjänster som stöder den finansiella enhetens kritiska funktioner, tillämpningar och infrastrukturkomponenter.

Artikel 23

Avancerad testning av IKT-verktyg, IKT-system och IKT-processer baserade på hotstyrd penetrationstestning

1. De finansiella enheter som har identifierats i enlighet med punkt 4 ska minst vart tredje år genomföra avancerade tester med hjälp av hotstyrda penetrationstester.

2. De hotstyrda penetrationstesterna ska minst omfatta en finansiell enhets kritiska funktioner och tjänster och ska utföras på produktionssystem i drift som stöder sådana funktioner. Den exakta omfattningen av de hotstyrda penetrationstesterna ska fastställas av finansiella enheter och valideras av de behöriga myndigheterna på grundval av bedömningen av kritiska funktioner och tjänster.

   Vid tillämpning av första stycket ska de finansiella enheterna identifiera alla relevanta underliggande IKT-processer, IKT-system och IKT-tekniker som stöder kritiska funktioner och tjänster, inbegripet funktioner och tjänster som har utkontrakterats eller kontrakterats till tredjepartsleverantörer av IKT-tjänster.

   Om tredjepartsleverantörer av IKT-tjänster omfattas av den hotstyrda penetrationstestningen ska den finansiella enheten vidta nödvändiga åtgärder för att säkerställa att dessa leverantörer deltar.

   De finansiella enheterna ska tillämpa effektiva riskhanteringskontroller för att minska riskerna för möjliga effekter på data, skador på tillgångar och avbrott i kritiska tjänster eller transaktioner hos den finansiella enheten själv, dess motparter eller den finansiella sektorn.

   När testet har avslutats och efter det att rapporter och åtgärdsplaner har godkänts ska den finansiella enheten och de externa testarna förse den behöriga myndigheten med dokumentation som bekräftar att det hotstyrda penetrationstestet har utförts i enlighet med kraven. De behöriga myndigheterna ska validera dokumentationen och utfärda ett intyg.

3. De finansiella enheterna ska anlita testare i enlighet med artikel 24 i syfte att genomföra ett hotstyrt penetrationstest.

   De behöriga myndigheterna ska identifiera de finansiella enheter som ska genomföra hotstyrda penetrationstester på ett sätt som står i proportion till den finansiella

enhetens storlek, omfattning, verksamhet och övergripande riskprofil, på grundval av en bedömning av följande:

(a) Påverkansfaktorer, särskilt kritikaliteten hos de tjänster som tillhandahålls och den verksamhet som bedrivs av den finansiella enheten.

(b) Eventuella farhågor om den finansiella stabiliteten, inbegripet den finansiella enhetens betydelse för systemet som helhet på nationell nivå eller unionsnivå, beroende på vad som är lämpligt.

(c) Den berörda finansiella enhetens specifika IKT-riskprofil, IKT-mognadsgrad och tekniska funktioner.

4. EBA, Esma och Eiopa ska, efter samråd med ECB och med beaktande av relevanta ramar i unionen som är tillämpliga på underrättelsebaserade penetrationstester, utarbeta förslag till tekniska standarder för tillsyn för att närmare specificera

(a) de kriterier som används för tillämpningen av punkt 6 i denna artikel,

(b) kraven i fråga om

(a) omfattningen av den hotstyrda penetrationstestning som avses i punkt 2 i denna artikel,

(b) den testmetod och det tillvägagångssätt som ska följas för varje specifik fas i testprocessen,

(c) testningens resultat och avslutnings- och åtgärdsfaser,

(c) den typ av tillsynssamarbete som krävs för genomförandet av hotstyrd penetrationstestning när det gäller finansiella enheter som är verksamma i mer än en medlemsstat, för att det ska gå att införa lämplig nivå av tillsynsengagemang och ett flexibelt genomförande i syfte att ta hänsyn till särdragen hos finansiella delsektorer eller lokala finansmarknader.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den *[EUT: infoga datum två månader före dagen för ikraftträdandet*].

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i andra stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1095/2010 och (EU) nr 1094/2010.

Artikel 24

Krav för testare

1. De finansiella enheterna ska endast använda testare för att utföra hostyrda penetrationstester som

(a) är allra bäst lämpade och har högst anseende,

(b) har teknisk och organisatorisk kapacitet och uppvisar särskild sakkunskap om hotbildsunderrättelser, penetrationstester eller red-team-tester,

(c) har certifierats av ett ackrediteringsorgan i en medlemsstat eller följer formella uppförandekoder eller etiska ramar,

(d) om det rör sig om externa testare, lämnar en oberoende försäkran eller en revisionsberättelse om sund riskhantering i samband med genomförandet av

den hotstyrda penetrationstestningen, inbegripet korrekt skydd av den finansiella enhetens konfidentiella information och ersättning för den finansiella enhetens affärsrisker,

(e) om det rör sig om externa testare, har en relevant och heltäckande ansvarsförsäkring som omfattar risker för fel och försummelser i yrkesutövningen.

2. De finansiella enheterna ska se till att avtal som ingås med externa testare innehåller krav på en sund förvaltning av resultaten av de hotstyrda penetrationstesterna och att all behandling av dem, inbegripet generering, utkast, lagring, aggregering, rapportering, kommunikation eller förstörelse, inte skapar risker för den finansiella enheten.

KAPITEL V

HANTERING AV IKT-TREDJEPARTSRISKER

AVSNITT I

HUVUDPRINCIPER FÖR EN SUND HANTERING AV IKT-TREDJEPARTSRISKER

Artikel 25

Allmänna principer

De finansiella enheterna ska hantera IKT-tredjepartsrisker som en integrerad del av IKT-risken inom sin IKT-riskhanteringsram och i enlighet med följande principer:

1. De finansiella enheter som har ingått ett kontraktsmässigt arrangemang om användningen av IKT-tjänster för att bedriva sin affärsverksamhet ska alltid ha det fulla ansvaret för att uppfylla och fullgöra alla skyldigheter enligt denna förordning och tillämplig lagstiftning om finansiella tjänster.

2. De finansiella enheternas hantering av IKT-tredjepartsrisker ska genomföras med hänsyn till proportionalitetsprincipen, med beaktande av

(a) IKT-relaterade beroendens omfattning, komplexitet och betydelse,

(b) de risker som uppstår till följd av kontraktsmässiga arrangemang om användningen av IKT-tjänster som har ingåtts med tredjepartsleverantörer av IKT-tjänster, med hänsyn till den kritiska karaktären hos respektive tjänst, process eller funktion eller dess betydelse, och den potentiella inverkan på kontinuiteten och kvaliteten hos finansiella tjänster och verksamheter, på individuell nivå och på gruppnivå.

3. Som en del av sin IKT-riskhanteringsram ska de finansiella enheterna anta och regelbundet se över en strategi för IKT-tredjepartsrisker, med beaktande av den strategi för flera olika leverantörer som avses i artikel 5.9 g. Strategin ska omfatta riktlinjer för användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster och ska tillämpas individuellt och, i förekommande fall, på undergrupps- och gruppnivå. Ledningsorganet ska regelbundet se över de risker som har identifierats i samband med utkontraktering av kritiska eller viktiga funktioner.

4. Som en del av sin IKT-riskhanteringsram ska de finansiella enheterna upprätthålla och uppdatera ett register med information på enhetsnivå, undergrupps- och gruppnivå om alla kontraktsmässiga arrangemang som rör användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster.

   De kontraktsmässiga arrangemang som avses i första stycket ska dokumenteras på lämpligt sätt, varvid åtskillnad ska göras mellan de kontraktsmässiga arrangemang som omfattar kritiska eller viktiga funktioner och de som inte gör det.

   De finansiella enheterna ska minst en gång per år rapportera till de behöriga myndigheterna om antalet nya arrangemang för användningen av IKT-tjänster, kategorierna av tredjepartsleverantörer av IKT-tjänster, typen av kontraktsmässigt arrangemang och de tjänster och funktioner som tillhandahålls.

   De finansiella enheterna ska på begäran ge den behöriga myndigheten tillgång till det fullständiga registret eller angivna avsnitt av registret, tillsammans med all information som anses nödvändig för att möjliggöra en effektiv tillsyn av den finansiella enheten.

   De finansiella enheterna ska i god tid informera den behöriga myndigheten om planerad utkontraktering av kritiska eller viktiga funktioner och när en funktion har blivit kritisk eller viktig.

5. Innan de finansiella enheterna ingår ett kontraktsmässigt arrangemang om användning av IKT-tjänster ska de

   (a) bedöma om det kontraktsmässiga arrangemanget omfattar en kritisk eller viktig funktion,

   (b) bedöma om tillsynsvillkoren för utkontraktering är uppfyllda,

   (c) identifiera och bedöma alla relevanta risker i samband med det kontraktsmässiga arrangemanget, inbegripet möjligheten att sådana avtal kan bidra till att förstärka IKT-koncentrationsrisken,

   (d) genomföra all due diligence-granskning av potentiella tredjepartsleverantörer av IKT-tjänster och under urvals- och bedömningsprocesserna se till att tredjepartsleverantören av IKT-tjänster är lämplig,

   (e) identifiera och bedöma intressekonflikter som det kontraktsmässiga arrangemanget kan orsaka.

6. De finansiella enheterna får endast ingå avtal med tredjepartsleverantörer av IKT-tjänster som uppfyller höga, lämpliga och aktuella standarder för informationssäkerhet.

7. När de finansiella enheterna utövar åtkomst-, kontroll- och revisionsrättigheter gentemot IKT-tredjepartsleverantören av IKT-tjänster ska de på grundval av en riskbaserad metod på förhand fastställa frekvensen för revisioner och kontroller och de områden som ska granskas genom att följa allmänt accepterade revisionsstandarder i enlighet med eventuella tillsynsinstruktioner om användning och införlivande av sådana revisionsstandarder.

   När det gäller kontraktsmässiga arrangemang som medför en hög teknisk komplexitet ska den finansiella enheten kontrollera att revisorer, oavsett om de är interna, ingår i pooler av revisorer eller är externa, har lämpliga färdigheter och kunskaper för att effektivt kunna utföra relevanta revisioner och bedömningar.

8. De finansiella enheterna ska se till att kontraktsmässiga arrangemang om användning av IKT-tjänster avslutas under åtminstone följande omständigheter:

(a) Tredjepartsleverantören av IKT-tjänster bryter mot tillämpliga lagar, förordningar eller avtalsvillkor.

(b) Omständigheter har identifierats under övervakningen av IKT-tredjepartsrisker som bedöms kunna ändra prestandan hos de funktioner som tillhandahålls genom det kontraktsmässiga arrangemanget, inbegripet väsentliga förändringar som påverkar arrangemanget eller situationen för tredjepartsleverantören av IKT-tjänster.

(c) IKT-tredjepartsleverantörer har påvisade brister i sin övergripande IKT-riskhantering och i synnerhet det sätt på vilket den säkerställer säkerheten och integriteten för konfidentiella, personuppgifter eller på annat sätt känsliga uppgifter eller icke-personuppgifter.

(d) Omständigheter då den behöriga myndigheten inte längre effektivt kan utöva tillsyn över den finansiella enheten till följd av respektive kontraktsmässiga arrangemang.

9. De finansiella enheterna ska införa exitstrategier för att ta hänsyn till risker som kan uppstå hos tredjepartsleverantören av IKT-tjänster, i synnerhet eventuella fel hos denne, försämring av kvaliteten på de funktioner som tillhandahålls, eventuella avbrott i verksamheten på grund av olämpligt eller misslyckat tillhandahållande av tjänster eller väsentliga risker som uppstår i samband med en lämplig och kontinuerlig användning av funktionen.

De finansiella enheterna ska säkerställa att de kan säga upp kontraktsmässiga arrangemang utan

(a) avbrott i sin affärsverksamhet,

(b) begränsning av efterlevnaden av lagstadgade krav,

(c) skada på kontinuiteten och kvaliteten hos deras tillhandahållande av tjänster till kunder.

Exitplanerna ska vara heltäckande, dokumenterade och, när så är lämpligt, tillräckligt testade.

De finansiella enheterna ska identifiera alternativa lösningar och utarbeta övergångsplaner som gör det möjligt för dem att avlägsna de kontrakterade funktionerna och relevanta data från tredjepartsleverantören av IKT-tjänster och på ett säkert och fullständigt sätt överföra dem till alternativa leverantörer eller återintegrera dem internt.

De finansiella enheterna ska vidta lämpliga beredskapsåtgärder för att upprätthålla kontinuiteten i verksamheten under alla omständigheter som avses i första stycket.

10. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för genomförande för att fastställa standardmallar för det register över uppgifter som avses i punkt 4.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för genomförande till kommissionen senast den *[EUT: infoga datum ett år efter dagen för ikraftträdandet av den här förordningen*].

Kommissionen ges befogenhet att anta de tekniska standarder för genomförande som avses i första stycket i enlighet med artikel 15 i förordningarna (EU) nr 1093/2010, (EU) nr 1095/2010 och (EU) nr 1094/2010.

11. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till standarder för tillsyn

(a) för att närmare specificera det detaljerade innehållet i de riktlinjer som avses i punkt 3 i fråga om de kontraktsmässiga arrangemangen för användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster, med hänvisning till de viktigaste faserna i livscykeln för respektive arrangemang för användning av IKT-tjänster,

(b) i fråga om de typer av uppgifter ska ingå i det register över information som avses i punkt 4.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den *[EUT: infoga datum ett år efter dagen för ikraftträdandet*].

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i andra stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1095/2010 och (EU) nr 1094/2010.

Artikel 26

Preliminär bedömning av IKT-koncentrationsrisker och ytterligare arrangemang för underentreprenad

1. När de finansiella enheterna utför den identifiering och bedömning av IKT-koncentrationsrisk som avses i artikel 25.5 c ska de ta hänsyn till om ingåendet av ett kontraktsmässigt arrangemang avseende IKT-tjänsterna skulle leda till något av följande:

(a) Avtal med en tredjepartsleverantör av IKT-tjänster som inte är lätt utbytbar. .

(b) Flera kontraktsmässiga arrangemang om tillhandahållande av IKT-tjänster med samma tredjepartsleverantör av IKT-tjänster eller med nära anknutna tredjepartsleverantörer av IKT-tjänster.

De finansiella enheterna ska väga fördelarna och kostnaderna med alternativa lösningar, t.ex. användning av olika tredjepartsleverantörer av IKT-tjänster, med hänsyn till om och hur planerade lösningar motsvarar de affärsbehov och mål som anges i deras strategi för digital motståndskraft.

2. Om det kontraktsmässiga arrangemanget om användning av IKT-tjänster inbegriper möjligheten att en tredjepartsleverantör av IKT-tjänster lägger ut en kritisk eller viktig funktion på underentreprenad till andra tredjepartsleverantörer av IKT-tjänster, ska de finansiella enheterna väga de fördelar och risker som kan uppstå i samband med en sådan eventuell underentreprenad, särskilt när det gäller en IKT-underleverantör som är etablerad i ett tredjeland.

Om kontraktsmässiga arrangemang om användningen av IKT-tjänster ingås med en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland ska de finansiella enheterna beakta åtminstone följande faktorer:

(a) Respekt för uppgiftsskydd.

(b) Effektiv tillämpning av lagen.

(c) Insolvensrättsliga bestämmelser som skulle vara tillämpliga om IKT-tjänsteleverantören går i konkurs.

(d) Eventuella begränsningar som kan uppstå när det gäller skyndsam återställning av den finansiella enhetens data.

De finansiella enheterna ska bedöma om och hur potentiellt långa eller komplexa underentreprenadskedjor kan påverka deras förmåga att till fullo övervaka de avtalade funktionerna och den behöriga myndighetens förmåga att effektivt övervaka den finansiella enheten i detta avseende.

Artikel 27

Viktiga avtalsbestämmelser

1. Rättigheterna och skyldigheterna för den finansiella enheten och tredjepartsleverantören av IKT-tjänster ska vara tydligt fördelade och skriftligen angivna. Hela avtalet, vilket omfattar servicenivåavtalen, ska dokumenteras i ett skriftligt dokument som parterna har tillgång till på papper eller i ett nedladdningsbart och tillgängligt format.

2. De kontraktsmässiga arrangemangen för användning av IKT-tjänster ska minst omfatta följande:

(a) En tydlig och fullständig beskrivning av alla funktioner och tjänster som ska tillhandahållas av tredjepartsleverantören av IKT-tjänster, med uppgift om huruvida underentreprenad av en kritisk eller viktig funktion eller väsentliga delar därav, är tillåten och, om så är fallet, de villkor som gäller för sådan underentreprenad.

(b) De platser där de funktioner och tjänster som har utkontrakterats eller lagts ut på underentreprenad ska tillhandahållas och var uppgifterna ska behandlas, inklusive lagringsplatsen, och ett krav på att tredjepartsleverantören av IKT-tjänster ska underrätta den finansiella enheten om den planerar att ändra sådana platser.

(c) Bestämmelser om åtkomstmöjlighet, tillgänglighet, integritet, säkerhet och skydd av personuppgifter och om säkerställande av åtkomst, återställande och återlämnande i ett lättillgängligt format av personuppgifter och andra uppgifter än personuppgifter som behandlas av den finansiella enheten i händelse av insolvens, resolution eller nedläggning av verksamheten för tredjepartsleverantören av IKT-tjänster.

(d) Beskrivningar av fullständig servicenivå, inklusive uppdateringar och revideringar av dessa, och exakta kvantitativa och kvalitativa prestationsmål inom de överenskomna servicenivåerna för att göra det möjligt för den finansiella enheten att effektivt övervaka och utan onödigt dröjsmål möjliggöra lämpliga korrigerande åtgärder när överenskomna servicenivåer inte uppnås.

(e) Anmälningsperioder och rapporteringsskyldigheter för tredjepartsleverantören av IKT-tjänster till den finansiella enheten, inbegripet underrättelse om varje händelse som kan ha en väsentlig inverkan på IKT-tredjepartsleverantörens förmåga att effektivt utföra kritiska eller viktiga funktioner i linje med överenskomna servicenivåer.

(f) Skyldighet för tredjepartsleverantören av IKT-tjänster att tillhandahålla assistans i händelse av en IKT-incident utan extra kostnad eller till en kostnad som fastställs på förhand.

(g) Krav på att tredjepartsleverantören av IKT-tjänster ska genomföra och testa beredskapsplaner för verksamheten och ha infört IKT-säkerhetsåtgärder, IKT-verktyg och IKT-strategier som på ett tillfredsställande sätt garanterar ett säkert tillhandahållande av tjänster från den finansiella enhetens sida i enlighet med dess regelverk.

(h) Rätt att fortlöpande övervaka tredjepartsleverantören av IKT-tjänster, vilket omfattar följande:

i) Rätt till tillgång till, kontroll och revision för den finansiella enheten eller en utsedd tredjepart, och rätt att ta kopior av relevant dokumentation, vars faktiska utövande inte hindras eller begränsas av andra kontraktsmässiga arrangemang eller riktlinjer för genomförande.

ii) Rätt att komma överens om alternativa garantinivåer om andra kunders rättigheter påverkas.

iii) Åtagande om att samarbeta fullt ut under de kontroller på plats som utförs av den finansiella enheten och närmare uppgifter om omfattningen, formerna och frekvensen för revisioner på distans.

(i) Skyldighet för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut med de behöriga myndigheterna och resolutionsmyndigheterna för den finansiella enheten, inbegripet personer som har utsetts av dem.

(j) Uppsägningsrätt och tillhörande minimiuppsägningstid för uppsägning av kontraktet, i enlighet med de behöriga myndigheternas förväntningar.

(k) Exitstrategier, särskilt inrättande av en obligatorisk lämplig övergångsperiod

(a) under vilken tredjepartsleverantören av IKT-tjänster kommer att fortsätta att tillhandahålla respektive funktioner eller tjänster i syfte att minska risken för avbrott hos den finansiella enheten,

(b) som gör det möjligt för den finansiella enheten att byta till en annan tredjepartsleverantör av IKT-tjänster eller byta till lösningar på plats som är förenliga med komplexiteten hos den tillhandahållna tjänsten.

3. När finansiella enheter och tredjepartsleverantörer av IKT-tjänster förhandlar om kontraktsmässiga arrangemang ska de överväga att använda standardavtalsklausuler som har utarbetats för specifika tjänster.

4. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för tillsyn för att närmare specificera de delar som en finansiell enhet måste fastställa och bedöma när den lägger ut kritiska eller viktiga funktioner på underentreprenad för att korrekt genomföra bestämmelserna i punkt 2 a.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den *[EUT: infoga datum ett år efter dagen för ikraftträdandet*].

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1095/2010 och (EU) nr 1094/2010.

AVSNITT II

TILLSYNSRAM FÖR KRITISKA TREDJEPARTSLEVERANTÖRER AV IKT-TJÄNSTER

Artikel 28

Utseende av kritiska tredjepartsleverantörer av IKT-tjänster

1. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och på rekommendation av det tillsynsforum som har inrättats i enlighet med artikel 29.1,

   (a) utse tredjepartsleverantörer av IKT-tjänster som är kritiska för finansiella enheter, med beaktande av de kriterier som anges i punkt 2,

   (b) utse EBA, Esma eller Eiopa till ledande tillsynsmyndighet för varje kritisk tredjepartsleverantör av IKT-tjänster, beroende på om det totala värdet av tillgångarna hos de finansiella enheter som utnyttjar den kritiska tredjepartsleverantörens IKT-tjänster och som omfattas av någon av förordningarna (EU) nr 1093/2010 (EU), (EU) nr 1094/2010 respektive (EU) nr 1095/2010 utgör mer än hälften av värdet av de totala tillgångarna hos alla finansiella enheter som utnyttjar tjänster från den kritiska tredjepartsleverantören av IKT-tjänster, i enlighet med vad som framgår av dessa finansiella enheters konsoliderade balansräkningar eller enskilda balansräkningar, om balansräkningarna inte är konsoliderade.

2. Det utseende som avses i punkt 1 a ska baseras på samtliga följande kriterier:

   (a) Systempåverkan på stabiliteten, kontinuiteten eller kvaliteten på tillhandahållandet av finansiella tjänster om den berörda tredjepartsleverantören av IKT-tjänster skulle drabbas av ett omfattande driftsavbrott i tillhandahållandet av tjänster, med tanke på antalet finansiella enheter som den berörda tredjepartsleverantören av IKT-tjänster tillhandahåller tjänster till.

   (b) Påverkan på eller betydelsen för systemet av de finansiella enheter som är beroende av den berörda tredjepartsleverantören av IKT-tjänster, bedömt enligt följande parametrar:

      i) Antalet globala systemviktiga institut eller andra systemviktiga institut som är beroende av respektive tredjepartsleverantör av IKT-tjänster.

      ii) Det ömsesidiga beroendet mellan de globala systemviktiga institut eller andra systemviktiga institut som avses i led i och andra finansiella enheter, inbegripet situationer där de globala systemviktiga instituten eller andra systemviktiga instituten tillhandahåller finansiella infrastrukturtjänster till andra finansiella enheter.

   (c) De finansiella enheternas beroende av de tjänster som tillhandahålls av den berörda tredjepartsleverantören av IKT-tjänster i förhållande till kritiska eller viktiga funktioner hos de finansiella enheter som i sista hand involverar samma tredjepartsleverantör av IKT-tjänster, oavsett om de finansiella enheterna direkt

eller indirekt är beroende av dessa tjänster, med hjälp av eller genom underleverantörsavtal.

(d) Graden av utbytbarhet hos tredjepartsleverantören av IKT-tjänster, med beaktande av följande parametrar:

i) Avsaknad av verkliga alternativ, även delvis, på grund av det begränsade antalet tredjepartsleverantörer av IKT-tjänster som är verksamma på en viss marknad, eller marknadsandelen för den berörda tredjepartsleverantören av IKT-tjänster, eller den tekniska komplexiteten eller avancerade karaktären, inbegripet i förhållande till eventuell proprietär teknik, eller särdragen hos IKT-tredjepartsleverantörens organisation eller verksamhet.

ii) Svårigheter att helt eller delvis överföra relevanta data och arbetsbelastningar från den berörda tredjepartsleverantören av IKT-tjänster till en annan, på grund av betydande finansiella kostnader, tidsåtgång eller andra typer av resurser som migrationsprocessen kan medföra, eller på grund av ökade IKT-risker eller andra operativa risker som den finansiella enheten kan utsättas för genom sådan migration.

(e) Antalet medlemsstater där den berörda tredjepartsleverantören av IKT-tjänster tillhandahåller tjänster.

(f) Antalet medlemsstater där de finansiella enheter som använder den berörda tredjepartsleverantören av IKT-tjänster är verksamma.

3. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 50 för att komplettera de kriterier som avses i punkt 2.

4. Den utseendemekanism som avses i punkt 1 a får inte användas förrän kommissionen har antagit en delegerad akt i enlighet med punkt 3.

5. Den utseendemekanism som avses i punkt 1 a ska inte tillämpas på tredjepartsleverantörer av IKT-tjänster som omfattas av tillsynsramar som har inrättats till stöd för de uppgifter som avses i artikel 127.2 i fördraget om Europeiska unionens funktionssätt.

6. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén upprätta, offentliggöra och årligen uppdatera förteckningen över kritiska tredjepartsleverantörer av IKT-tjänster på unionsnivå.

7. Vid tillämpning av punkt 1 a ska de behöriga myndigheterna årligen och i aggregerad form översända de rapporter som avses i artikel 25.4 till det tillsynsforum som har inrättats i enlighet med artikel 29. Tillsynsforumet ska bedöma de finansiella enheternas IKT-beroende gentemot tredjepart på grundval av den information som har mottagits från de behöriga myndigheterna.

8. Tredjepartsleverantörer av IKT-tjänster som inte ingår i den förteckning som avses i punkt 6 får begära att bli upptagna i den förteckningen.

Vid tillämpning av första stycket ska tredjepartsleverantören av IKT-tjänster lämna in en motiverad ansökan till EBA, Esma eller Eiopa, som genom den gemensamma kommittén ska besluta huruvida den tredjepartsleverantören av IKT-tjänster ska tas upp i den förteckningen i enlighet med punkt 1 a.

Det beslut som avses i andra stycket ska antas och meddelas tredjepartsleverantören av IKT-tjänster inom sex månader från mottagandet av ansökan.

9. De finansiella enheterna får inte använda sig av en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland och som skulle betecknas som kritisk enligt punkt 1 a om den var etablerad i unionen.

Artikel 29

Tillsynsramens struktur

1. Den gemensamma kommittén ska i enlighet med artikel 57 i förordning (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010, inrätta tillsynsforumet som en underkommitté för att stödja arbetet i den gemensamma kommittén och i den ledande tillsynsmyndighet som avses i artikel 28.1 b inom området för IKT-tredjepartsrisker i alla finansiella sektorer. Tillsynsforumet ska utarbeta utkast till gemensamma ståndpunkter och gemensamma akter från den gemensamma kommittén på detta område.

   Tillsynsforumet ska regelbundet diskutera relevant utveckling när det gäller IKT-risker och IKT-sårbarheter och främja en konsekvent strategi för övervakning av IKT-tredjepartsrisker på unionsnivå.

2. Tillsynsforumet ska årligen göra en gemensam bedömning av resultaten och slutsatserna av den tillsynsverksamhet som genomförts för alla kritiska IKT-tredjepartsleverantörer och främja samordningsåtgärder för att öka de finansiella enheternas digitala operativa motståndskraft, främja bästa praxis för hantering av IKT-koncentrationsrisker och undersöka riskreducerande åtgärder för sektorsövergripande risköverföring.

3. Tillsynsforumet ska lägga fram heltäckande referensvärden för kritiska tredjepartsleverantörer av IKT-tjänster som ska antas av den gemensamma kommittén i form av gemensamma ståndpunkter från de europeiska tillsynsmyndigheterna i enlighet med artikel 56.1 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

4. Tillsynsforumet ska bestå av ordförandena för de europeiska tillsynsmyndigheterna och en företrädare på hög nivå för den tjänstgörande personalen på den relevanta behöriga myndigheten i varje medlemsstat. De verkställande direktörerna för varje europeisk tillsynsmyndighet och en företrädare för Europeiska kommissionen, ESRB, ECB och Enisa ska delta i tillsynsforumet som observatörer.

5. I enlighet med artikel 16 i förordning (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 ska de europeiska tillsynsmyndigheterna vid tillämpningen av detta avsnitt utfärda riktlinjer för samarbetet mellan de europeiska tillsynsmyndigheterna och de behöriga myndigheterna i fråga om detaljerade förfaranden och villkor för utförandet av uppgifter mellan behöriga myndigheter och de europeiska tillsynsmyndigheterna och närmare uppgifter om det informationsutbyte som de behöriga myndigheterna behöver för att säkerställa uppföljningen av de rekommendationer som ledande tillsynsmyndigheter i enlighet med artikel 31.1 d riktar till kritiska IKT-tredjepartsleverantörer.

6. De krav som fastställs i detta avsnitt ska inte påverka tillämpningen av direktiv (EU) 2016/1148 och andra unionsbestämmelser om tillsyn som är tillämpliga på leverantörer av molntjänster.

7. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och på grundval av det förberedande arbete som utförs av tillsynsforumet, varje år lägga

fram en rapport för Europaparlamentet, rådet och kommissionen om tillämpningen av detta avsnitt.

Artikel 30

Den ledande tillsynsmyndighetens uppgifter

1. Den ledande tillsynsmyndigheten ska bedöma huruvida varje kritisk tredjepartsleverantör av IKT-tjänster har infört heltäckande, sunda och effektiva regler, förfaranden, mekanismer och arrangemang för att hantera de IKT-risker som den kan utgöra för finansiella enheter.

2. Den bedömning som avses i punkt 1 ska omfatta följande:

   (a) IKT-krav för att i synnerhet säkerställa säkerhet, tillgänglighet, kontinuitet, skalbarhet och kvalitet hos de tjänster som den kritiska tredjepartsleverantören av IKT-tjänster tillhandahåller finansiella enheter, samt förmåga att alltid upprätthålla höga standarder för säkerhet, konfidentialitet och dataintegritet.

   (b) Den fysiska säkerhet som bidrar till att säkerställa IKT-säkerheten, inbegripet säkerheten i lokaler, anläggningar och datacenter.

   (c) Riskhanteringsprocesser, inbegripet IKT-riskhanteringsstrategier, IKT-kontinuitetsplaner och IKT-katastrofplaner.

   (d) Styrformer, inbegripet en organisationsstruktur med tydliga, transparenta och konsekventa ansvarsregler som möjliggör en effektiv IKT-riskhantering.

   (e) Identifiering, övervakning och snabb rapportering av IKT-relaterade incidenter till de finansiella enheterna, hantering och avhjälpande av dessa incidenter, särskilt it-attacker.

   (f) Mekanismer för dataportabilitet, tillämpningsportabilitet och interoperabilitet, som säkerställer att de finansiella enheterna effektivt kan utöva sin uppsägningsrätt.

   (g) Testning av IKT-system, IKT-infrastruktur och IKT-kontroller.

   (h) IKT-revisioner.

   (i) Användning av relevanta nationella och internationella standarder som är tillämpliga på tillhandahållandet av leverantörens IKT-tjänster till de finansiella enheterna.

3. På grundval av den bedömning som avses i punkt 1 ska den ledande tillsynsmyndigheten anta en tydlig, detaljerad och motiverad tillsynsplan för varje kritisk tredjepartsleverantör av IKT-tjänster. Planen ska varje år meddelas den kritiska tredjepartsleverantören av IKT-tjänster.

4. När de årliga tillsynsplaner som avses i punkt 3 har godkänts och anmälts till de kritiska tredjepartsleverantörerna av IKT-tjänster får de behöriga myndigheterna endast vidta åtgärder avseende kritiska tredjepartsleverantörer av IKT-tjänster i samförstånd med den ledande tillsynsmyndigheten.

Artikel 31

Den ledande tillsynsmyndighetens befogenheter

1. För att fullgöra de uppgifter som anges i detta avsnitt ska den ledande tillsynsmyndigheten ha befogenhet att

   (a) begära all relevant information och dokumentation i enlighet med artikel 32,

   (b) genomföra allmänna utredningar och kontroller i enlighet med artiklarna 33 och 34,

   (c) begära rapporter efter det att tillsynsverksamheten har slutförts med angivande av de åtgärder som har vidtagits eller de avhjälpande åtgärder som har vidtagits av kritiska IKT-tredjepartsleverantörer i samband med de rekommendationer som avses i led d i denna punkt,

   (d) utarbeta rekommendationer på de områden som avses i artikel 30.2, särskilt

      i) om tillämpning av specifika IKT-säkerhets- och kvalitetskrav eller IKT-processer, särskilt i samband med införandet av programfixar, uppdateringar, kryptering och andra säkerhetsåtgärder som den ledande tillsynsmyndigheten anser vara relevanta för att säkerställa IKT-säkerheten för tjänster som tillhandahålls till finansiella enheter,

      ii) om användning av villkor, inbegripet deras tekniska genomförande, enligt vilka kritiska tredjepartsleverantörer av IKT-tjänster tillhandahåller tjänster till finansiella enheter, som den ledande tillsynsmyndighetens bedömer är relevanta för att förhindra uppkomsten av felkritiska systemdelar (*single points of failure*), eller för att förstärka dessa, eller för att minimera eventuella systemeffekter inom unionens finansiella sektor i händelse av IKT-koncentrationsrisk,

      iii) efter den granskning som har gjorts i enlighet med artiklarna 32 och 33 av underleverantörsavtal, inbegripet underentreprenadsavtal som de kritiska tredjepartsleverantörerna av IKT-tjänster planerar att ingå med andra tredjepartsleverantörer av IKT-tjänster eller med IKT-underleverantörer som är etablerade i ett tredjeland, om alla planerade underleverantörsavtal, inbegripet underentreprenad, om den ledande tillsynsmyndigheten bedömer att ytterligare underentreprenad kan utlösa risker för den finansiella enhetens tillhandahållande av tjänster eller risker för den finansiella stabiliteten,

      iv) om att avstå från att ingå ytterligare underleverantörsavtal, om följande kumulativa villkor är uppfyllda:

         – den planerade underleverantören är en tredjepartsleverantör av IKT-tjänster eller en IKT-underleverantör som är etablerad i ett tredjeland,

         – underentreprenaden avser en kritisk eller viktig funktion hos den finansiella enheten.

2. Den ledande tillsynsmyndigheten ska samråda med tillsynsforumet innan den utövar de befogenheter som avses i punkt 1.

3. Kritiska tredjepartsleverantörer av IKT-tjänster ska samarbeta lojalt med den ledande tillsynsmyndigheten och bistå den ledande tillsynsmyndigheten vid fullgörandet av dess uppgifter.

4. Den ledande tillsynsmyndigheten får besluta om vite för att tvinga den kritiska tredjepartsleverantören av IKT-tjänster att uppfylla kraven i punkt 1 a, b och c.

5. Det vite som avses i punkt 4 ska åläggas dagligen till dess att efterlevnad har uppnåtts och i högst sex månader efter anmälan till den kritiska tredjepartsleverantören av IKT-tjänster.

6. Vitesbeloppet, beräknat från det datum som anges i beslutet om föreläggande av vitet, ska vara 1 % av den genomsnittliga globala omsättningen per dag för den kritiska tredjepartsleverantören av IKT-tjänster under det föregående räkenskapsåret.

7. Vitet ska vara av administrativ karaktär och ska vara verkställbart. Verkställigheten ska följa de civilprocessrättsliga regler som gäller i den medlemsstat inom vars territorium kontrollerna och åtkomsten ska genomföras. Domstolarna i den berörda medlemsstaten ska vara behöriga att pröva klagomål som rör oegentligheter i verkställigheten. De belopp som åläggs i form av viten ska tillfalla Europeiska unionens allmänna budget.

8. De europeiska tillsynsmyndigheterna ska offentliggöra alla viten som har förelagts utom i de fall då offentliggörandet skulle skapa allvarlig oro på de finansiella marknaderna eller orsaka de berörda parterna oproportionerligt stor skada.

9. Innan ett vite åläggs enligt punkt 4 ska den ledande tillsynsmyndigheten ge företrädarna för den kritiska IKT-tredjepartsleverantör som är föremål för förfarandena möjlighet att höras om de omständigheter som tillsynsmyndigheterna har påtalat och ska grunda sina beslut endast på omständigheter som den kritiska IKT-tredjepartsleverantören som är föremål för förfarandet har haft möjlighet att yttra sig över. Rätten till försvar för personer som är föremål för förfarandena ska iakttas fullt ut under förfarandena. De ska ha rätt att få tillgång till ärendehandlingarna, med förbehåll för andra personers berättigade intresse av att deras affärshemligheter skyddas. Tillgången till ärendehandlingarna ska inte omfatta konfidentiella uppgifter eller ledande tillsynsmyndighetens interna förberedande handlingar.

Artikel 32

Begäran om information

1. Den ledande tillsynsmyndigheten får genom en enkel begäran eller genom ett beslut kräva att de kritiska tredjepartsleverantörerna av IKT-tjänster tillhandahåller all information som är nödvändig för att den ledande tillsynsmyndigheten ska kunna utföra sina uppgifter enligt denna förordning, inbegripet alla relevanta affärshandlingar eller operativa dokument, avtal, dokumentation av riktlinjer, rapporter från IKT-säkerhetsgranskningar, IKT-relaterade incidentrapporter samt all information som rör parter till vilka den kritiska tredjepartsleverantören av IKT-tjänster har utkontrakterat operativa funktioner eller verksamheter.

2. När den ledande tillsynsmyndigheten skickar en enkel begäran om information ska den

   (a) hänvisa till denna artikel som rättslig grund för begäran,

   (b) ange syftet med begäran,

(c) specificera vilka uppgifter som begärs,

(d) ange en tidsfrist inom vilken uppgifterna ska lämnas,

(e) underrätta företrädaren för den kritiska tredjepartsleverantör av IKT-tjänster av vilken uppgifterna begärs om att den inte är skyldig att lämna informationen, men att den information som lämnas vid ett frivilligt svar på begäran inte får vara oriktig eller vilseledande.

3. När den ledande tillsynsmyndigheten begär uppgifter enligt punkt 1 ska den

(a) hänvisa till denna artikel som rättslig grund för begäran,

(b) ange syftet med begäran,

(c) specificera vilka uppgifter som begärs,

(d) ange en tidsfrist inom vilken uppgifterna ska lämnas,

(e) ange de viten som föreskrivs i artikel 31.4 om den begärda informationen är ofullständig,

(f) informera om rätten att överklaga beslutet inför de europeiska tillsynsmyndigheternas överklagandenämnd och att få beslutet prövat av Europeiska unionens domstol (nedan kallad *domstolen*) i enlighet med artiklarna 60 och 61 i förordning (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

4. Företrädare för kritiska tredjepartsleverantörer av IKT-tjänster ska tillhandahålla den begärda informationen. I behörig ordning befullmäktigade advokater får lämna de begärda uppgifterna på sina huvudmäns vägnar. Den kritiska tredjepartsleverantören av IKT-tjänster förblir ansvarig fullt ut om de lämnade uppgifterna är ofullständiga, oriktiga eller vilseledande.

5. Den ledande tillsynsmyndigheten ska utan dröjsmål skicka en kopia av beslutet för att informera de behöriga myndigheterna om de finansiella enheter som använder de kritiska tredjepartsleverantörernas IKT-tjänster.

Artikel 33

Allmänna utredningar

1. För att fullgöra sina uppgifter enligt denna förordning får den ledande tillsynsmyndigheten, med bistånd av den undersökningsgrupp som avses i artikel 34.1, genomföra nödvändiga utredningar av tredjepartsleverantörer av IKT-tjänster.

2. Den ledande tillsynsmyndigheten ska ha befogenhet att

(a) granska handlingar, uppgifter, rutiner och allt annat material av relevans för utförandet av dess uppgifter oberoende av i vilken form de föreligger,

(b) ta eller erhålla bestyrkta kopior av, eller utdrag ur, sådana handlingar, uppgifter, rutiner och sådant annat material,

(c) kalla till sig företrädare för tredjepartsleverantören av IKT-tjänster och be dem om muntliga eller skriftliga förklaringar angående sakförhållanden eller dokument som rör föremålet för och syftet med utredningen samt nedteckna svaren,

(d) höra varje annan fysisk eller juridisk person som går med på att höras i syfte att samla in information om föremålet för utredningen,

(e) begära in uppgifter om tele- och datatrafik.

3. De tjänstemän och andra personer som av den ledande tillsynsmyndigheten har bemyndigats att genomföra sådana utredningar som avses i punkt 1 ska utöva sina befogenheter mot uppvisande av ett skriftligt tillstånd där utredningens föremål och syfte anges.

I tillståndet ska även anges de viten som föreskrivs i artikel 31.4 om den dokumentation, de uppgifter, förfaranden eller annat material som krävs eller svaren på frågor till företrädare för tredjepartsleverantören av IKT-tjänster inte tillhandahålls eller är ofullständiga.

4. Företrädarna för tredjepartsleverantörer av IKT-tjänster är skyldiga att underkasta sig utredningarna på grundval av ett beslut av den ledande tillsynsmyndigheten. Beslutet ska ange föremålet för och syftet med utredningen, de viten som föreskrivs i artikel 31.4, de rättsmedel som finns tillgängliga enligt förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 samt rätten att få beslutet prövat av domstolen.

5. Den ledande tillsynsmyndigheten ska i god tid före en utredning underrätta de behöriga myndigheterna för de finansiella enheter som använder tredjepartsleverantören av IKT-tjänster om utredningen och namnge de bemyndigade personerna.

Artikel 34

Kontroller på plats

1. För att utföra sina uppgifter enligt denna förordning får den ledande tillsynsmyndigheten, med bistånd av de undersökningsgrupper som avses i artikel 35.1, inleda och genomföra alla nödvändiga kontroller på plats i företagslokaler, på mark eller egendom som tillhör IKT-tredjepartsleverantörerna, såsom huvudkontor, driftscentrum, sekundära lokaler, samt för att utföra kontroller off-line.

2. Tjänstemän och andra personer som av den ledande tillsynsmyndigheten har bemyndigats att genomföra en kontroll på plats får bereda sig tillträde till företagslokaler, mark eller egendom och ska ha alla befogenheter att försegla företagslokaler och räkenskaper eller affärshandlingar under den tid och i den utsträckning som krävs för kontrollen.

De ska utöva sina befogenheter mot uppvisande av ett skriftligt tillstånd som anger kontrollens föremål och syften liksom de viten som föreskrivs i artikel 31.4 om företrädarna för de berörda tredjepartsleverantörerna av IKT-tjänster inte underkastar sig kontrollen.

3. Den ledande tillsynsmyndigheten ska i god tid före en kontroll informera de behöriga myndigheterna för de finansiella enheter som använder denna IKT-tredjepartsleverantör.

4. Kontrollerna ska omfatta alla relevanta IKT-system, nätverk, anordningar, information och data som används för eller bidrar till tillhandahållandet av tjänster till finansiella enheter.

5. Före ett planerat besök på plats ska de ledande tillsynsmyndigheterna i rimlig tid underrätta de kritiska tredjepartsleverantörerna av IKT-tjänster, såvida detta inte är omöjligt på grund av en nöd- eller krissituation, eller om det skulle leda till en situation där kontrollen eller revisionen inte längre skulle vara effektiv.

6. Den kritiska tredjepartsleverantören av IKT-tjänster ska underkasta sig kontroller på plats som har beordrats genom beslut av den ledande tillsynsmyndigheten. Beslutet ska ange föremålet för och syftet med kontrollen, fastställa den dag då den ska inledas och ange de viten som föreskrivs i artikel 31.4, de rättsmedel som finns tillgängliga enligt förordning (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 samt rätten att få beslutet prövat av domstolen.

7. Om de tjänstemän och andra personer som har bemyndigats av den ledande tillsynsmyndigheten finner att en kritisk tredjepartsleverantör av IKT-tjänster motsätter sig en kontroll som har beordrats i enlighet med denna artikel, ska den ledande tillsynsmyndigheten informera den kritiska IKT-leverantören om konsekvenserna av att de motsätter sig kontrollen, inbegripet möjligheten för de berörda finansiella enheternas behöriga myndigheter att säga upp de kontraktsmässiga arrangemang som har ingåtts med den kritiska tredjepartsleverantören av IKT-tjänster.

Artikel 35
Fortlöpande tillsyn

1. Vid allmänna utredningar eller kontroller på plats ska de ledande tillsynsmyndigheterna bistås av en undersökningsgrupp som har inrättats för varje kritisk tredjepartsleverantör av IKT-tjänster.

2. Den gemensamma undersökningsgrupp som avses i punkt 1 ska bestå av personal från den ledande tillsynsmyndigheten och från de relevanta behöriga myndigheter som utövar tillsyn över de finansiella enheter till vilka den kritiska tredjepartsleverantören av IKT-tjänster tillhandahåller tjänster, vilka kommer att delta i förberedelserna och genomförandet av tillsynsverksamheten, med högst tio medlemmar. Alla medlemmar i den gemensamma undersökningen ska ha sakkunskap om IKT och operativa risker. Den gemensamma undersökningsgruppen ska samordnas av en utsedd anställd vid en europeisk tillsynsmyndighet (nedan kallad *den ledande tillsynsmyndighetens samordnare*).

3. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta gemensamma förslag till tekniska standarder för tillsyn för att närmare specificera utseendet av de medlemmar i den gemensamma undersökningsgruppen som kommer från de relevanta behöriga myndigheterna samt undersökningsgruppens uppgifter och arbetsmetoder. De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den *[EUT: infoga datum ett år efter dagen för ikraftträdandet*].

   Kommissionen ges befogenhet att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

4. Inom tre månader efter slutförandet av en utredning eller kontroll på plats ska den ledande tillsynsmyndigheten, efter samråd med tillsynsforumet, anta rekommendationer som ska riktas till den kritiska tredjepartsleverantören av IKT-tjänster i enlighet med de befogenheter som avses i artikel 31.

5. De rekommendationer som avses i punkt 4 ska omedelbart meddelas den kritiska tredjepartsleverantören av IKT-tjänster och de behöriga myndigheterna för de finansiella enheter till vilka denne tillhandahåller tjänster.

För att genomföra tillsynsverksamheten får de ledande tillsynsmyndigheterna ta hänsyn till relevanta tredjepartscertifieringar och interna eller externa IKT-revisionsrapporter som den kritiska tredjepartsleverantören av IKT-tjänster har gjort tillgängliga.

Artikel 36

Harmonisering av villkoren för tillsyn

1. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för tillsyn för att specificera

(a) den information som ska tillhandahållas av en kritisk tredjepartsleverantör av IKT-tjänster i ansökan om frivilligt deltagande i enlighet med artikel 28.8,

(b) innehållet i och formatet för de rapporter som kan begäras i enlighet med artikel 31.1 c,

(c) presentationen av den information, inbegripet struktur, format och metoder, som en kritisk tredjepartsleverantör av IKT-tjänster ska vara skyldig att lämna in, offentliggöra eller rapportera i enlighet med artikel 31.1,

(d) närmare uppgifter om de behöriga myndigheternas bedömning av åtgärder som har vidtagits av kritiska tredjepartsleverantörer av IKT-tjänster på grundval av rekommendationerna från ledande tillsynsmyndigheter i enlighet med artikel 37.2.

2. De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 1 januari 20xx [*EUT: infoga datum ett år efter dagen för ikraftträdandet*].

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med det förfarande som fastställs i artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 37

Behöriga myndigheters uppföljning

1. Inom 30 kalenderdagar efter mottagandet av de rekommendationer som har utfärdats av de ledande tillsynsmyndigheterna i enlighet med artikel 31.1 d ska kritiska tredjepartsleverantörer av IKT-tjänster underrätta den ledande tillsynsmyndigheten om huruvida de avser att följa dessa rekommendationer. De ledande tillsynsmyndigheterna ska omedelbart vidarebefordra denna information till de behöriga myndigheterna.

2. De behöriga myndigheterna ska övervaka huruvida de finansiella enheterna tar hänsyn till de risker som har identifierats i de rekommendationer som den ledande tillsynsmyndigheten har riktat till kritiska IKT-tredjepartsleverantörer i enlighet med artikel 31.1 d.

3. De behöriga myndigheterna får i enlighet med artikel 44 kräva att de finansiella enheterna tillfälligt, helt eller delvis, avbryter användningen eller införandet av en tjänst som tillhandahålls av den kritiska IKT-tredjepartsleverantören till dess att de risker som identifieras i rekommendationerna till kritiska IKT-tredjepartsleverantörer har åtgärdats. Vid behov får de kräva att de finansiella enheterna helt eller delvis avslutar de relevanta avtal som har ingåtts med de kritiska tredjepartsleverantörerna av IKT-tjänster.

4. När de behöriga myndigheterna fattar de beslut som avses i punkt 3 ska de ta hänsyn till typen och omfattningen av den risk som inte hanteras av den kritiska tredjepartsleverantören av IKT-tjänster, samt hur allvarlig den bristande efterlevnaden är, med beaktande av följande kriterier:

   (a) Den bristande efterlevnadens allvarlighetsgrad och varaktighet.

   (b) Huruvida den bristande efterlevnaden har påvisat allvarliga brister i den kritiska tredjepartsleverantörens förfaranden, ledningssystem, riskhantering och interna kontroller.

   (c) Huruvida ekonomisk brottslighet har underlättats, orsakats eller på annat sätt kan tillskrivas den bristande efterlevnaden.

   (d) Huruvida den bristande efterlevnaden är uppsåtlig eller beror på oaktsamhet.

5. De behöriga myndigheterna ska regelbundet informera de ledande tillsynsmyndigheterna om de metoder och åtgärder som de har vidtagit i sina tillsynsuppgifter när det gäller finansiella enheter samt om de avtalsåtgärder som har vidtagits av dessa om en kritisk tredjepartsleverantör av IKT-tjänster inte helt eller delvis har godtagit rekommendationerna från de ledande tillsynsmyndigheterna.

Artikel 38
Tillsynsavgifter

1. De europeiska tillsynsmyndigheterna ska från de kritiska tredjepartsleverantörerna av IKT-tjänster ta ut avgifter som till fullo täcker de europeiska tillsynsmyndigheternas nödvändiga utgifter i samband med fullgörandet av tillsynsuppgifter enligt denna förordning, inbegripet ersättning för eventuella kostnader som kan uppstå till följd av arbete som utförs av behöriga myndigheter som deltar i tillsynsverksamheten i enlighet med artikel 35.

   Det avgiftsbelopp som tas ut av en kritisk tredjepartsleverantör av IKT-tjänster ska täcka alla administrativa kostnader och stå i proportion till leverantörens omsättning.

2. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 50 för att komplettera denna förordning genom att fastställa avgiftsbeloppen och hur de ska betalas.

Artikel 39
Internationellt samarbete

1. EBA, Esma och Eiopa får, i enlighet med artikel 33 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 respektive (EU) nr 1095/2010, ingå administrativa arrangemang med tredjeländers reglerings- och tillsynsmyndigheter för att främja internationellt samarbete om IKT-tredjepartsrisker inom olika finansiella sektorer, särskilt genom att utveckla bästa praxis för översyn av IKT-riskhanteringsmetoder och IKT-kontroller, begränsningsåtgärder och incidenthantering.

2. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén vart femte år lämna en gemensam konfidentiell rapport till Europaparlamentet, rådet och kommissionen med en sammanfattning av resultaten av de relevanta diskussioner som har förts med de myndigheter i tredjeländer som avses i punkt 1, med fokus på utvecklingen av IKT-tredjepartsrisker och konsekvenserna för den finansiella stabiliteten, marknadsintegriteten, investerarskyddet eller den inre marknadens funktion.

KAPITEL VI

ARRANGEMANG FÖR INFORMATIONSUTBYTE

Artikel 40

Arrangemang för utbyte av information och underrättelser om cyberhot

1. Finansiella enheter får sinsemellan utbyta information och underrättelser om cyberhot, inbegripet indikatorer på äventyrad säkerhet, taktiker, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg, i den mån sådant utbyte av information och underrättelser

   (a) syftar till att förbättra de finansiella enheternas digitala operativa motståndskraft, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra cyberhotens spridningsförmåga, stödja finansiella enheters försvarsförmåga, metoder för att upptäcka hot, begränsningsstrategier eller åtgärds- och återställningsfaser,

   (b) äger rum inom betrodda grupper av finansiella enheter,

   (c) genomförs genom arrangemang för informationsutbyte som skyddar den potentiellt känsliga karaktären hos den information som utbyts och som styrs av uppföranderegler med full respekt för affärshemligheter, skydd av personuppgifter[48] och riktlinjer för konkurrenspolitiken.[49]

2. Vid tillämpning av punkt 1 c ska arrangemangen för informationsutbyte innehålla fastställda villkor för deltagande och, när så är lämpligt, närmare uppgifter om offentliga myndigheters deltagande och den kapacitet i vilken dessa kan knytas till arrangemangen för informationsutbyte, samt om operativa delar, inbegripet användningen av särskilda it-plattformar.

3. De finansiella enheterna ska underrätta de behöriga myndigheterna om sitt deltagande i de arrangemang för informationsutbyte som avses i punkt 1, när deras medlemskap har godkänts eller, i tillämpliga fall, när medlemskapet upphör, så snart detta träder i kraft.

---

48 I enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

49 Meddelande från kommissionen – *Riktlinjer för tillämpningen av artikel 101 i fördraget om Europeiska unionens funktionssätt på horisontella samarbetsavtal*, 2011/C 11/01.

KAPITEL VII

BEHÖRIGA MYNDIGHETER

Artikel 41

Behöriga myndigheter

Utan att det påverkar tillämpningen av de bestämmelser om tillsynsramen för kritiska tredjepartsleverantörer av IKT-tjänster som avses i kapitel V avsnitt II i denna förordning ska efterlevnaden av de skyldigheter som fastställs i denna förordning säkerställas av följande behöriga myndigheter i enlighet med de befogenheter som tilldelats genom respektive rättsakt:

(a) För kreditinstitut: den behöriga myndighet som har utsetts i enlighet med artikel 4 i direktiv 2013/36/EU, utan att det påverkar de särskilda uppgifter som ECB tilldelas genom förordning (EU) nr 1024/2013.

(b) För betaltjänstleverantörer: den behöriga myndighet som har utsetts i enlighet med artikel 22 i direktiv (EU) 2015/2366.

(c) För institut för elektroniska betalningar: den behöriga myndighet som har utsetts i enlighet med artikel 37 i direktiv 2009/110/EG.

(d) För värdepappersföretag: den behöriga myndighet som har utsetts i enlighet med artikel 4 i direktiv (EU) 2019/2034.

(e) För leverantörer av kryptotillgångstjänster, emittenter av kryptotillgångar, emittenter av tillgångsanknutna token och emittenter av betydande tillgångsanknutna token: den behöriga myndighet som har utsetts i enlighet med artikel 3.1 ee första strecksatsen i [*förordning (EU) 20xx om marknader för kryptotillgångar*].

(f) För värdepapperscentraler: den behöriga myndighet som har utsetts i enlighet med artikel 11 i förordning (EU) nr 909/2014.

(g) För centrala motparter: den behöriga myndighet som har utsetts i enlighet med artikel 22 i förordning (EU) nr 648/2012.

(h) För handelsplatser och leverantörer av datarapporteringstjänster: den behöriga myndighet som har utsetts i enlighet med artikel 67 i direktiv 2014/65/EU.

(i) För transaktionsregister: den behöriga myndighet som har utsetts i enlighet med artikel 55 i förordning (EU) nr 648/2012.

(j) För förvaltare av alternativa investeringsfonder: den behöriga myndighet som har utsetts i enlighet med artikel 44 i direktiv 2011/61/EU.

(k) För förvaltningsbolag: den behöriga myndighet som har utsetts i enlighet med artikel 97 i direktiv 2009/65/EG.

(l) För försäkrings- och återförsäkringsföretag: den behöriga myndighet som har utsetts i enlighet med artikel 30 i direktiv 2009/138/EG.

(m) För försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet: den behöriga myndighet som har utsetts i enlighet med artikel 12 i direktiv (EU) 2016/97.

(n) För tjänstepensionsinstitut: den behöriga myndighet som har utsetts i enlighet med artikel 47 i direktiv 2016/2341.

(o) För kreditvärderingsinstitut: den behöriga myndighet som har utsetts i enlighet artikel 21 i förordning (EG) nr 1060/2009.

(p) För lagstadgade revisorer- och revisionsföretag: den behöriga myndighet som har utsetts i enlighet med artikel 3.2 och artikel 32 i direktiv 2006/43/EG.

(q) För administratörer av kritiska referensvärden: den behöriga myndighet som har utsetts i enlighet med artiklarna 40 och 41 i *förordning xx/202x*.

(r) För leverantörer av gräsrotsfinansieringstjänster: den behöriga myndighet som har utsetts i enlighet med *artikel x i förordning xx/202x*.

(s) För värdepapperiseringsregister: den behöriga myndighet som har utsetts i enlighet med artikel 10 och artikel 14.1 i förordning (EU) nr 2017/2402.

Artikel 42

Samarbete med strukturer och myndigheter som har inrättats genom direktiv (EU) 2016/1148

1. För att främja samarbete och möjliggöra tillsynsutbyten mellan de behöriga myndigheter som har utsetts enligt denna förordning och den samarbetsgrupp som har inrättats genom artikel 11 i direktiv (EU) 2016/1148 får de europeiska tillsynsmyndigheterna och de behöriga myndigheterna begära att bli inbjudna till samarbetsgruppens verksamhet.

2. De behöriga myndigheterna får vid behov samråda med den gemensamma kontaktpunkten och de nationella enheter för hantering av it-säkerhetsincidenter som avses i artiklarna 8 respektive 9 i direktiv (EU) 2016/1148.

Artikel 43

Övningar, kommunikation och samarbete mellan finansiella sektorer

1. De europeiska tillsynsmyndigheterna får, genom den gemensamma kommittén och i samarbete med behöriga myndigheter, ECB och ESRB, inrätta mekanismer för att möjliggöra utbyte av effektiv praxis mellan olika finansiella sektorer för att öka situationsmedvetenheten och identifiera gemensamma sårbarheter och risker på it-området.

   De får utveckla krishanterings- och beredskapsövningar som inbegriper it-attacker i syfte att utveckla kommunikationskanaler och gradvis möjliggöra en effektiv samordnad reaktion på EU-nivå i händelse av en större gränsöverskridande IKT-relaterad incident eller därmed sammanhängande hot som har en systempåverkan på unionens finansiella sektor som helhet.

   Dessa övningar kan när så är lämpligt även innefatta test av den finansiella sektorns beroendeförhållanden till andra ekonomiska sektorer.

2. Behöriga myndigheter, EBA, Esma eller Eiopa och ECB ska ha ett nära samarbete och utbyta information för att fullgöra sina uppgifter enligt artiklarna 42–48. De ska nära samordna sin tillsyn för att identifiera och åtgärda överträdelser av denna förordning, utveckla och främja bästa praxis, underlätta samarbete, främja en

konsekvent tolkning och tillhandahålla bedömningar över jurisdiktionsgränserna om det uppstår meningsskiljaktigheter.

Artikel 44

Administrativa sanktioner och avhjälpande åtgärder

1. De behöriga myndigheterna ska ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att de ska kunna fullgöra sina skyldigheter enligt denna förordning.

2. De befogenheter som avses i punkt 1 ska omfatta åtminstone befogenheter att

   (a) få tillgång till alla dokument eller uppgifter i vilken form som helst som enligt den behöriga myndigheten är relevanta för fullgörandet av dess uppgifter och få eller ta en kopia av dem,

   (b) utföra kontroller eller undersökningar på plats,

   (c) kräva korrigerande och avhjälpande åtgärder vid överträdelser av kraven i denna förordning.

3. Utan att det påverkar medlemsstaternas rätt att ålägga straffrättsliga påföljder enligt artikel 46 ska medlemsstaterna fastställa bestämmelser om lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av denna förordning och se till att de genomförs effektivt.

   Sådana sanktioner och åtgärder ska vara effektiva, proportionella och avskräckande.

4. Medlemsstaterna ska ge behöriga myndigheter befogenhet att tillämpa åtminstone följande administrativa sanktioner eller avhjälpande åtgärder vid överträdelser av denna förordning:

   (a) Utfärda ett föreläggande enligt vilken det krävs att den fysiska eller juridiska personen upphör med sitt agerande och inte upprepar detta agerande.

   (b) Kräva att varje praxis eller beteende som den behöriga myndigheten anser strider mot bestämmelserna i denna förordning tillfälligt eller permanent upphör och förhindra en upprepning av denna praxis eller detta beteende.

   (c) Vidta alla typer av åtgärder, även av ekonomisk art, för att säkerställa att finansiella enheter fortsätter att uppfylla rättsliga krav.

   (d) Kräva tillgång till, i den mån det är tillåtet enligt nationell rätt, befintliga uppgifter om datatrafik som innehas av en teleoperatör om det föreligger en rimlig misstanke om överträdelse av denna förordning och om dessa uppgifter kan vara relevanta för en utredning av överträdelser av denna förordning. .

   (e) Utfärda offentliga meddelanden, inklusive offentliga uttalanden, med uppgift om den fysiska eller juridiska personens identitet och överträdelsens art.

5. Om de bestämmelser som avses i punkt 2 c och punkt 4 är tillämpliga på juridiska personer ska medlemsstaterna ge de behöriga myndigheterna befogenhet att tillämpa administrativa sanktioner och avhjälpande åtgärder, med förbehåll för de villkor som föreskrivs i nationell rätt, på medlemmar i ledningsorganet och på andra personer som enligt nationell lagstiftning är ansvariga för överträdelsen.

6. Medlemsstaterna ska se till att alla beslut om att ålägga administrativa sanktioner eller avhjälpande åtgärder enligt punkt 2 c är vederbörligen motiverade och kan överklagas.

Artikel 45

Utövande av befogenheten att ålägga administrativa sanktioner och avhjälpande åtgärder

1. De behöriga myndigheterna ska utöva sina befogenheter att ålägga de administrativa sanktioner och avhjälpande åtgärder som avses i artikel 44 i enlighet med sina nationella rättsliga ramar, beroende på vad som är lämpligt

   (a) direkt,

   (b) i samarbete med andra myndigheter,

   (c) på eget ansvar genom delegering till andra myndigheter,

   (d) genom hänvändelse till de behöriga rättsliga myndigheterna.

2. De behöriga myndigheterna ska, när de fastställer typen av och nivån på en administrativ sanktion eller avhjälpande åtgärd som ska åläggas enligt artikel 44, ta hänsyn till i vilken utsträckning överträdelsen är avsiktlig eller beror på försummelse och alla andra relevanta omständigheter, bland annat följande, när så är lämpligt:

   (a) Överträdelsens väsentlighet, svårighetsgrad och varaktighet.

   (b) Graden av ansvar hos den fysiska eller juridiska person som gjort sig skyldig till överträdelsen.

   (c) Den finansiella ställningen för den fysiska eller juridiska person som gjort sig skyldig till överträdelsen.

   (d) Omfattningen av de vinster som erhållits eller av förluster som undvikits av den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen, i den mån de kan bestämmas.

   (e) Förluster för tredje parter orsakade av överträdelsen, i den mån de kan fastställas.

   (f) Viljan hos den ansvariga fysiska eller juridiska person att samarbeta med den behöriga myndigheten, utan att det påverkar behovet av att säkerställa återföring av den vinst som personen gjort eller de förluster som denne undvikit.

   (g) Tidigare överträdelser av den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen.

Artikel 46

Straffrättsliga påföljder

1. Medlemsstaterna får besluta att inte fastställa regler för administrativa sanktioner eller avhjälpande åtgärder för överträdelser som omfattas av straffrättsliga påföljder i deras nationella rätt.

2. Om medlemsstaterna har valt att fastställa straffrättsliga påföljder för överträdelser av denna förordning ska de säkerställa att lämpliga åtgärder har vidtagits så att de behöriga myndigheterna har alla nödvändiga befogenheter att samarbeta med rättsliga myndigheter, åklagarmyndigheter eller straffrättsliga myndigheter inom sin

jurisdiktion för att få specifik information om brottsutredningar eller straffrättsliga förfaranden som har inletts på grund av överträdelser av denna förordning, och att lämna samma information till andra behöriga myndigheter samt EBA, Esma eller Eiopa för att uppfylla sina skyldigheter att samarbeta enligt denna förordning.

Artikel 47

Underrättelseskyldigheter

Medlemsstaterna ska underrätta kommissionen, Esma, EBA och Eiopa om de lagar och andra författningar som genomför detta kapitel, inbegripet alla relevanta straffrättsliga bestämmelser senast *[EUT: infoga datum ett år efter dagen för ikraftträdandet*]. Medlemsstaterna ska utan onödigt dröjsmål underrätta kommissionen, Esma, EBA och Eiopa om eventuella ändringar av dessa.

Artikel 48

Offentliggörande av administrativa sanktioner

1. De behöriga myndigheterna ska utan onödigt dröjsmål på sina officiella webbplatser offentliggöra alla beslut om att ålägga en administrativ sanktion som inte kan överklagas efter det att sanktionens adressat har underrättats om beslutet.

2. Det offentliggörande som avses i punkt 1 ska innehålla information om överträdelsens typ och art, de ansvariga personernas identitet och ålagda sanktioner.

3. Om den behöriga myndigheten efter en bedömning av det enskilda fallet anser att ett offentliggörande av de juridiska personernas identitet eller av de fysiska personernas identitet eller personuppgifter är oproportionellt, kan hota stabiliteten på de finansiella marknaderna eller äventyra en pågående utredning eller, i den mån detta kan bestämmas, vålla den berörda personen oproportionerlig skada, ska den behöriga myndigheten vidta någon av följande åtgärder i fråga om beslutet om att pålägga en administrativ sanktion:

   (a) Skjuta upp offentliggörandet tills det inte längre finns någon anledning att inte offentliggöra det.

   (b) Offentliggöra beslutet på anonym grund på ett sätt som överensstämmer med nationell rätt. .

   (c) Avstå från att offentliggöra beslutet om de alternativ som anges i leden a och b inte anses vara tillräckliga för att säkerställa att det inte innebär något hot mot finansmarknadernas stabilitet eller säkerställa att offentliggörandet av ett sådant beslut är proportionellt när det gäller mindre stränga sanktioner.

4. Vid ett beslut om att offentliggöra en administrativ sanktion på anonym grund i enlighet med punkt 3 b får offentliggörandet av de relevanta uppgifterna skjutas upp.

5. Om en behörig myndighet offentliggör ett beslut om åläggande av en administrativ sanktion som överklagas till de relevanta rättsliga myndigheterna, ska de behöriga myndigheterna omedelbart på sin officiella webbplats lägga till denna information och i senare skeden all tillhörande information om resultatet av ett sådant överklagande. Varje rättsligt beslut om ogiltigförklaring av ett beslut om åläggande av en administrativ sanktion ska också offentliggöras.

6. De behöriga myndigheterna ska säkerställa att alla offentliggöranden som avses i punkterna 1–4 finns kvar på deras officiella webbplats i minst fem år efter

offentliggörandet. Personuppgifter i detta offentliggörande ska endast finnas på den behöriga myndighetens webbplats så länge detta krävs enligt gällande regler för uppgiftsskydd.

Artikel 49

Tystnadsplikt

1. All konfidentiell information som är föremål för mottagande, utbyte eller förmedling enligt denna förordning ska omfattas av de villkor för tystnadsplikt som föreskrivs i punkt 2.
2. Tystnadsplikten ska gälla alla personer som arbetar eller har arbetat för de behöriga myndigheter som omfattas av denna förordning, eller för en myndighet eller ett marknadsföretag eller en fysisk eller juridisk person som dessa behöriga myndigheter har delegerat sina befogenheter till, inbegripet revisorer och experter som arbetar på den behöriga myndighetens uppdrag.
3. Information som omfattas av tystnadsplikt får inte lämnas ut till någon annan person eller myndighet utom när detta föreskrivs i unionslagstiftningen eller nationell lagstiftning.
4. All information som utbyts mellan de behöriga myndigheterna enligt denna förordning och som avser affärs- eller driftsförhållanden och andra ekonomiska eller personliga förhållanden ska anses vara konfidentiell och omfattas av tystnadsplikt, utom när den behöriga myndigheten vid den tidpunkt då informationen lämnas anger att informationen får lämnas ut eller om det är nödvändigt att lämna ut informationen i samband med rättsliga förfaranden.

KAPITEL VIII

DELEGERADE AKTER

Artikel 50

Utövande av delegering

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
2. Den befogenhet att anta delegerade akter som avses i artiklarna 28.3 och 38.2 ska ges till kommissionen för en period på fem år från och med [PO: infoga datum fem år efter dagen för ikraftträdandet av den här förordningen].
3. Den delegering av befogenhet som avses i artiklarna 28.3 och 38.2 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning* eller vid ett senare, i beslutet angivet datum. Det påverkar inte giltigheten av de delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt, ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016.

5. Så snart kommissionen antar en delegerad akt, ska kommissionen samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artiklarna 28.3 och 38.2 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på begäran av Europaparlamentet eller rådet.

KAPITEL IX

ÖVERGÅNGS- OCH SLUTBESTÄMMELSER

AVSNITT I

Artikel 51

Översynsklausul

Senast den [*Publikationsbyrån: infoga datum fem år efter dagen för ikraftträdandet av den här förordningen]* ska kommissionen, efter samråd med EBA, Esma, Eiopa och ESRB, när så är lämpligt, genomföra en översyn och överlämna en rapport till Europaparlamentet och rådet, vid behov åtföljd av ett lagstiftningsförslag, om kriterierna för att utse kritiska tredjepartsleverantörer av IKT-tjänster i artikel 28.2.

AVSNITT II

ÄNDRINGAR

Artikel 52

Ändringar av förordning (EG) nr 1060/2009

I förordning (EG) nr 1060/2009 ska bilaga I avsnitt A punkt 4 första stycket ersättas med följande:

> ”Ett kreditvärderingsinstitut ska tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för internkontroll och effektiva riskbedömningsmetoder samt effektiva kontroll- och skyddssystem för förvaltningen av sina IKT-system i enlighet med Europaparlamentets och rådets förordning (EU) 2021/xx* [DORA].
>
> * Europaparlamentets och rådets förordning (EU) 2021/xx […] (EUT L XX, DD.MM.ÅÅÅÅ, s. X).”

Artikel 53

Ändringar av förordning (EU) nr 648/2012

Förordning (EU) nr 648/2012 ska ändras på följande sätt:

(1) Artikel 26 ska ändras på följande sätt:

(a) Punkt 3 ska ersättas med följande:

”3. En central motpart ska upprätthålla en organisationsstruktur som säkerställer en kontinuerlig och väl fungerande verksamhet och tillhandahållande av tjänster. Den ska använda lämpliga och proportionella system, resurser och förfaranden, inbegripet IKT-system som förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2021/xx * [DORA].

* Europaparlamentets och rådets förordning (EU) 2021/xx […] (EUT L XX, DD.MM.ÅÅÅÅ, s. X).”

(b) Punkt 6 ska utgå.

(2) Artikel 34 ska ändras på följande sätt:

(a) Punkt 1 ska ersättas med följande:

”1. En central motpart ska etablera, genomföra och upprätthålla lämpliga riktlinjer för kontinuerlig verksamhet och en lämplig katastrofplan, vilket ska innefatta IKT-kontinuitetsplaner och IKT-katastrofplaner som har upprättats i enlighet med förordning (EU) 2021/xx [DORA], för att trygga verksamheten, snabbt återuppta den och fullgöra den centrala motpartens skyldigheter.”

(b) I punkt 3 ska första stycket ersättas med följande:

”För att säkerställa en konsekvent tillämpning av denna artikel ska Esma, efter samråd med ECBS-medlemmarna, utarbeta förslag till tekniska standarder för tillsyn med närmare uppgifter om minimiinnehåll och krav avseende riktlinjerna för kontinuerlig verksamhet och katastrofplanen, exklusive IKT-kontinuitetsplanerna och IKT-katastrofplanerna.”

(3) I artikel 56 ska punkt 3 första stycket ersättas med följande:

”3. För att säkerställa en konsekvent tillämpning av denna artikel ska Esma utarbeta förslag till tekniska standarder för tillsyn med närmare uppgifter om den ansökan om registrering som avses i punkt 1, utom för krav som rör IKT-riskhantering.”

(4) I artikel 79 ska punkterna 1 och 2 ersättas med följande:

”1. Ett transaktionsregister ska kartlägga operativa riskkällor och minimera dem genom att utveckla lämpliga system, kontroller och förfaranden, inbegripet IKT-system som förvaltas i enlighet med förordning (EU) 2021/xx *[DORA]*.

2. Ett transaktionsregister ska utforma, tillämpa och upprätthålla tillräckliga riktlinjer för kontinuerlig verksamhet och en katastrofplan, inbegripet IKT-kontinuitetsplaner och IKT-katastrofplaner som har upprättats i enlighet med förordning (EU) 2021/xx*[DORA],* för att kunna upprätthålla verksamheten, snabbt kunna återuppta den och fullgöra

transaktionsregistrets skyldigheter.”

(5) I artikel 80 ska punkt 1 utgå.

Artikel 54

Ändringar av förordning (EU) nr 909/2014

Artikel 45 i förordning (EU) nr 909/2014 ska ändras på följande sätt:

(1) Punkt 1 ska ersättas med följande:

”1. En värdepapperscentral ska identifiera källor till operativ risk, såväl interna som externa, och minimera deras effekt genom att använda lämpliga IKT-verktyg, IKT-kontroller och IKT-förfaranden som har inrättats och förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2021/xx * *[DORA]*, samt andra relevanta lämpliga verktyg, kontroller och förfaranden för andra typer av operativa risker, inbegripet för samtliga avvecklingssystem för värdepapper som den driver.

* Europaparlamentets och rådets förordning (EU) 2021/xx […] (EUT L XX, DD.MM.ÅÅÅÅ, s. X).”

(2) Punkt 2 ska utgå.

(3) Punkterna 3 och 4 ska ersättas med följande:

”3. En värdepapperscentral ska för tjänster som den tillhandahåller samt för varje avvecklingssystem för värdepapper som den driver upprätta, genomföra och upprätthålla ändamålsenliga riktlinjer för driftskontinuitet och en plan för katastrofberedskap, inbegripet IKT-kontinuitetsplaner och IKT-katastrofplaner som har inrättats i enlighet med förordning (EU) 2021/xx [DORA], för att se till att dess tjänster kan upprätthållas, driften snabbt kan återupptas och värdepapperscentralens skyldigheter kan fullgöras vid händelser som medför en betydande risk för avbrott i verksamheten.

4. Den plan som avses i punkt 3 ska göra det möjligt att återupprätta alla transaktioner och deltagares positioner vid tidpunkten för avbrottet, så att värdepapperscentralens deltagare kan fortsätta sin verksamhet på ett säkert sätt och avvecklingen kan fullföljas på fastställd dag, inbegripet genom att säkerställa att driften av avgörande it-system kan återupptas från och med tidpunkten för avbrottet i enlighet med vad som anges i artikel 11.5 och 11.7 i förordning (EU) 2021/xx [DORA].”

(4) I punkt 6 ska första stycket ersättas med följande:

”En värdepapperscentral ska identifiera, övervaka och hantera de risker för verksamheten som de viktigaste deltagarna i det avvecklingssystem för värdepapper som den driver samt tjänsteleverantörer, andra värdepapperscentraler eller andra marknadsinfrastrukturer kan utgöra för dess verksamhet. Den ska på begäran tillhandahålla behöriga och relevanta myndigheter information om varje sådan risk som har identifierats. Den ska även utan dröjsmål informera den behöriga myndigheten och de relevanta myndigheterna om alla operativa incidenter till följd av sådana risker, med undantag för IKT-risker.”

(5) I punkt 7 ska första stycket ersättas med följande:

”Esma ska i nära samarbete med medlemmarna i ECBS utarbeta förslag till tekniska standarder för tillsyn i syfte att fastställa de andra operativa risker som avses i punkterna 1–6, med undantag för IKT-risker, och de metoder för att testa, hantera och minimera de riskerna, inbegripet de riktlinjer för driftskontinuitet och katastrofberedskap som avses i punkterna 3 och 4 samt metoderna för att bedöma dessa.”

Artikel 55

Ändringar av förordning (EU) nr 600/2014

Förordning (EU) nr 600/2014 ska ändras på följande sätt:

(1) Artikel 27g ska ändras på följande sätt:

(a) Punkt 4 ska utgå.

(b) Punkt 8 c ska ersättas med följande:

(c) ”c) De konkreta organisatoriska krav som avses i punkterna 3 och 5”.

(2) Artikel 27h ska ändras på följande sätt:

(a) Punkt 5 ska utgå.

(b) Punkt 8 e ska ersättas med följande:

”e) De konkreta organisatoriska krav som avses i punkt 4”.

(3) Artikel 27i ska ändras på följande sätt:

(a) Punkt 3 ska utgå.

(b) Punkt 5 b ska ersättas med följande:

”b) De konkreta organisatoriska krav som avses i punkterna 2 och 4”.

Artikel 56

Ikraftträdande och tillämpning

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den [*Publikationsbyrån: infoga datum – 12 månader efter dagen för ikraftträdande]*].

Artiklarna 23 och 24 ska dock tillämpas från och med [*Publikationsbyrån: infoga datum – 36 månader efter dagen för ikraftträdandet av denna förordning*].

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1,1. Förslagets eller initiativets titel

1,2. Berörda politikområden

1,3. Typ av förslag eller initiativ

1,4. Mål

1,5. Grunder för förslaget eller initiativet

1,6. Varaktighet för och budgetkonsekvenser av förslaget eller initiativet

1,7. Planerad metod för genomförandet

2. FÖRVALTNING

2,1. Bestämmelser om uppföljning och rapportering

2,2. Förvaltnings- och kontrollsystem

2,3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3,1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

3,2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

3.2.2. Beräknad inverkan på anslagen

3.2.3. Beräknad påverkan på personalbehov

3.2.4. Förenlighet med den gällande fleråriga budgetramen

3.2.5. Bidrag från tredje part

3,3. Beräknad inverkan på inkomsterna

Bilaga

Allmänna antaganden

Tillsynsbefogenheter

FINANSIERINGSÖVERSIKT FÖR BYRÅER

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets titel

Förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn.

1.2. Berörda politikområden

Politikområde: Finansiell stabilitet, finansiella tjänster och kapitalmarknadsunionen

Verksamhetsområde: Digital operativ motståndskraft

1.3. Förslaget avser

☑ **en ny åtgärd**

☐ **en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd**[50]

☐ **en förlängning av en befintlig åtgärd**

☐ **en sammanslagning av en eller flera åtgärder mot en annan/ny åtgärd**

1.4. Mål

1.4.1. Allmänt/allmänna mål:

Det allmänna målet för initiativet är att stärka den digitala operativa motståndskraften hos enheter i EU:s finansiella sektor genom att rationalisera och uppgradera befintliga regler och införa nya krav där det finns luckor. Detta skulle också stärka den digitala dimensionen av det enhetliga regelverket.

Det övergripande målet kan delas in i tre allmänna mål: 1) minska risken för finansiella störningar och instabilitet, 2) minska den administrativa bördan och öka tillsynens effektivitet och 3) öka skyddet för konsumenter och investerare.

1.4.2. Specifikt/specifika mål

Förslaget har följande specifika mål:

Ta itu med risker inom informations- och kommunikationsteknik (IKT) på ett mer övergripande sätt och stärka den finansiella sektorns digitala motståndskraft överlag.

Rationalisera IKT-relaterad incidentrapportering och ta itu med överlappande rapporteringskrav.

Ge de finansiella tillsynsmyndigheterna tillgång till information om IKT-relaterade incidenter.

Säkerställa att finansiella enheter som omfattas av detta förslag bedömer effektiviteten i sina förebyggande åtgärder och åtgärder för motståndskraft och identifierar IKT-relaterade sårbarheter.

Minska fragmenteringen av den inre marknaden och möjliggöra gränsöverskridande acceptans av testresultat.

[50] I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

Stärka de avtalsenliga skyddsåtgärderna för finansiella enheter när de använder IKT-tjänster, inbegripet regler för utkontraktering (som styr övervakningen av IKT-tredjepartsleverantörer). Möjliggöra tillsyn över verksamheten hos kritiska IKT-tredjepartsleverantörer. Uppmuntra utbyte av underrättelser om hot inom finanssektorn.

1.4.3. Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

En rättsakt om digital operativ motståndskraft för finanssektorn skulle säkerställa en övergripande ram som omfattar alla aspekter av den digitala operativa motståndskraften och skulle vara effektiv för att förbättra den finansiella sektorns övergripande operativa motståndskraft. Den skulle garantera tydlighet och konsekvens inom det enhetliga regelverket.

Rättsakten skulle också förtydliga och öka samstämmigheten i samspelet med direktivet om säkerhet i nätverks- och informationssystem och dess översyn. Den skulle skapa klarhet för finansiella enheter om de olika regler om digital operativ motståndskraft som de måste följa, särskilt för de finansiella enheter som innehar flera auktorisationer och är verksamma på olika marknader inom EU.

1.4.4. Prestationsindikatorer

Ange indikatorer för övervakning av framsteg och resultat.

Möjliga indikatorer:

Antal IKT-relaterade incidenter i EU:s finanssektor och deras inverkan.

Antal större IKT-relaterade incidenter som har rapporterats till tillsynsmyndigheter.

Antal finansiella enheter som skulle behöva utföra hotstyrda penetrationstester.

Antal finansiella enheter som använder standardavtalsklausuler för att ingå avtal med IKT-tredjepartsleverantörer.

Antal kritiska IKT-tredjepartsregleringar som övervakas av de europeiska tillsynsmyndigheterna/tillsynsmyndigheterna.

Antal finansiella enheter som deltar i lösningar för utbyte av hotbilder.

Antal myndigheter som ska ta emot rapporter om samma IKT-relaterade incident.

Antal gränsöverskridande hotstyrda penetrationstester.

1.5. Grunder för förslaget eller initiativet

1.5.1. Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

Finanssektorn förlitar sig i stor utsträckning på informations- och kommunikationsteknik (IKT). Trots de betydande framsteg som har gjorts genom nationella och europeiska riktade politiska initiativ och lagstiftningsinitiativ fortsätter IKT-riskerna att utgöra en utmaning för den operativa motståndskraften, prestandan och stabiliteten i EU:s finansiella system. Den reform som följde på finanskrisen 2008 stärkte i första hand den finansiella motståndskraften hos EU:s finanssektor och syftade till att skydda EU:s konkurrenskraft och stabilitet ur ekonomiska, tillsynsmässiga och marknadsmässiga perspektiv. IKT-säkerhet och övergripande digital operativ motståndskraft ingår i de operativa riskerna, men har inte uppmärksammats lika mycket i lagstiftningsagendan efter krisen och har bara utvecklats inom vissa områden av unionens politik och regelverk för finansmarknader, eller endast i ett fåtal medlemsstater. Detta innebär följande utmaningar som förslaget bör avhjälpa:

EU:s rättsliga ram för IKT-risker och operativ motståndskraft inom finanssektorn är fragmenterad och inte helt konsekvent.

Avsaknaden av enhetliga rapporteringskrav för IKT-relaterade incidenter leder till att tillsynsmyndigheterna har en ofullständig överblick över incidenternas art, frekvens, betydelse och inverkan.

Vissa finansiella enheter ställs inför komplexa, överlappande och potentiellt inkonsekventa rapporteringskrav för samma IKT-relaterade incident.

Otillräckligt informationsutbyte och otillräckligt samarbete om underrättelser om cyberhot på strategisk, taktisk och operativ nivå hindrar enskilda finansiella enheter från att på lämpligt sätt bedöma, övervaka, försvara sig mot och reagera på cyberhot.

I vissa finansiella delsektorer kan det finnas flera och icke samordnade ramar för penetreringstest och tester av motståndskraft, i kombination med att resultaten inte erkänns över gränserna, medan andra delsektorer saknar sådana testramar.

Tillsynsmyndigheternas brist på insyn i den del av de finansiella enheternas verksamhet som tillhandahålls av IKT-tredjepartsleverantörer utsätter de enskilda finansiella enheterna och det finansiella systemet som helhet för operativa risker.

De finansiella tillsynsmyndigheterna saknar tillräckliga mandat och verktyg för att övervaka och hantera koncentrations- och systemrisker som härrör från finansiella enheters beroende av IKT-tredjeparter.

1.5.2. Mervärdet av en åtgärd på unionsnivå (som kan bero på flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på unionsnivå” menas det värde en unionsinsats tillför som går utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

Skäl för åtgärder på europeisk nivå (på förhand):

Den digitala operativa motståndskraften är en fråga av gemensamt intresse för EU:s finansmarknader. Åtgärder på EU-nivå skulle medföra fler fördelar och större värde än åtgärder som vidtas separat på nationell nivå. Om dessa operativa bestämmelser om IKT-risker inte läggs till skulle det enhetliga regelverket tillhandahålla verktyg för att hantera alla andra typer av risker på europeisk nivå, men skulle utelämna de aspekter som rör digital operativ motståndskraft eller innebära att de hanteras genom för fragmenterade och osamordnade initiativ på nationell nivå. Förslaget skulle ge rättslig klarhet om huruvida och hur digitala operativa bestämmelser är tillämpliga, särskilt för gränsöverskridande finansiella enheter, och det skulle undanröja behovet för medlemsstaterna att individuellt förbättra regler, standarder och förväntningar när det gäller operativ motståndskraft och cybersäkerhet som ett svar på den nuvarande begränsade omfattningen av EU:s regler och den allmänna utformningen av direktivet om säkerhet i nätverks- och informationssystem.

Förväntat mervärde för unionen (i efterhand):

En åtgärd från unionens sida skulle avsevärt öka politikens effektivitet och samtidigt minska komplexiteten och minska den finansiella och administrativa bördan för alla finansiella enheter. Den skulle innebära en harmonisering av ett ekonomiskt område som är så nära sammanlänkat och integrerat och som redan omfattas av en enda uppsättning regler och tillsyn. När det gäller den IKT-relaterade incidentrapporteringen skulle förslaget innebära en minskad rapporteringsbörda – och de implicita kostnaderna – för att rapportera samma IKT-relaterade incident till olika EU-myndigheter och/eller nationella myndigheter. Det kommer också att underlätta ömsesidigt erkännande/godtagande av testresultat från enheter som bedriver gränsöverskridande verksamhet och som är föremål för flera provningsramar i olika medlemsstater.

1.5.3. Erfarenheter från tidigare liknande åtgärder

Nytt initiativ

1.5.4. Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

Syftet med detta förslag är förenligt med ett antal andra EU-strategier och pågående initiativ, särskilt direktivet om nätverks- och informationssäkerhet och direktivet om europeisk kritisk infrastruktur. Förslaget innebär att fördelarna med den övergripande ramen för cybersäkerhet bibehålls genom att de tre finansiella delsektorerna behålls i tillämpningsområdet för direktivet om säkerhet i nätverks- och informationssystem. Genom att de finansiella tillsynsmyndigheterna fortsätter att vara kopplade till ekosystemet för säkerhet i nätverks- och informationssystem skulle kunna utbyta relevant information med myndigheter för säkerhet i nätverks- och informationssystem och delta i samarbetsgruppen för nätverks- och informationssäkerhet. Förslaget skulle inte påverka direktivet om säkerhet i nätverks- och informationssystem utan vara en vidareutveckling av det, där eventuella överlappningar hanteras genom ett lex specialis-undantag. Samspelet mellan förordningen om finansiella tjänster och direktivet om säkerhet i nätverks- och informationssystem skulle även i fortsättningen regleras av en lex specialis-klausul enligt vilken finansiella enheter undantas från de materiella kraven i direktivet om säkerhet i nätverks- och informationssystem, för att undvika överlappningar mellan de två rättsakterna. Förslaget är dessutom förenligt med direktivet om europeisk kritisk infrastruktur, som för närvarande håller på att ses över för att förbättra skyddet av och motståndskraften hos kritisk infrastruktur mot andra hot än cyberhot.

Detta förslag skulle inte påverka den fleråriga budgetramen. För det första kommer tillsynsramen för kritiska tredjepartsleverantörer inom IKT att finansieras fullt ut genom avgifter som tas ut av dessa leverantörer. För det andra kommer de ytterligare tillsynsuppgifter i fråga om digital operativ motståndskraft som anförtros de europeiska tillsynsmyndigheterna att fullgöras genom intern omplacering av befintlig personal.

Detta kommer att leda till ett förslag om att utöka byråns bemyndigade personal under det kommande årliga budgetförfarandet. Byrån kommer att fortsätta att arbeta för att skapa största möjliga synergieffekter och effektivitetsvinster (bl.a. via it-system) och noga övervaka den ytterligare arbetsbörda som är förknippad med detta förslag, vilket skulle återspeglas i den nivå av bemyndigad personal som byrån begär i det årliga budgetförfarandet.

1.5.5. En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

Flera finansieringsalternativ övervägdes:

För det första skulle merkostnaderna kunna finansieras genom de europeiska tillsynsmyndigheternas vanliga finansieringsmekanism. Detta skulle dock innebära en betydande ökning av EU:s bidrag till de europeiska tillsynsmyndigheternas finansiella resurser.

Detta alternativ väljs för kostnader i samband med de tillsynsuppgifter som är kopplade till detta förslag. De europeiska tillsynsmyndigheterna kommer att omfördela befintlig personal för att utveckla ett antal tekniska standarder. De extra kostnaderna i samband med tillsynen av kritiska tredjepartsleverantörer kunde dock inte täckas genom en omfördelning av resurser inom de europeiska tillsynsmyndigheterna som också har andra uppgifter utöver dem som föreskrivs i detta förslag och enligt annan unionslagstiftning. För tillsynsuppgifter som rör digital operativ motståndskraft krävs dessutom särskild teknisk kunskap och expertis. Eftersom de europeiska tillsynsmyndigheternas nuvarande resurser för detta inte är tillräckliga, behövs ytterligare resurser.

Enligt förslagen kommer slutligen avgifter att tas ut av de kritiska IKT-tredjepartsleverantörer som är omfattas av tillsynen. Dessa är avsedda att täcka alla extra resurser som de europeiska tillsynsmyndigheterna behöver för att fullgöra sina nya uppgifter och befogenheter.

1.6. Varaktighet för och budgetkonsekvenser av förslaget eller initiativet

☐ **begränsad varaktighet**

☐ Förslaget eller initiativet ska gälla från [den DD/MM]ÅÅÅÅ till [den DD/MM]ÅÅÅÅ.

☐ Det påverkar resursanvändningen från ÅÅÅÅ till ÅÅÅÅ.

☑ **obegränsad varaktighet**

Efter en inledande period från 2021

beräknas verksamheten vara fullskalig.

1.7. Planerad metod för genomförandet[51]

Direkt förvaltning av kommissionen genom

☐ genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☑ **Indirekt förvaltning** genom att genomförandeuppgifter anförtros åt

☐ internationella organisationer och organ kopplade till dem (ange vilka)

☐ EIB och Europeiska investeringsfonden

☑ organ som avses i artiklarna 70 och 71

☐ offentligrättsliga organ

☐ privaträttsliga organ som anförtrotts uppgifter som faller inom offentlig förvaltning och som lämnat tillräckliga ekonomiska garantier

☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts uppgifter inom ramen för ett offentligt-privat partnerskap och som lämnar tillräckliga ekonomiska garantier, samt

☐ personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder inom Gusp som följer av avdelning V i fördraget om Europeiska unionen och som anges ställs i den grundläggande rättsakten.

Kommentarer

–

[51] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder

I linje med redan befintliga arrangemang utarbetar de europeiska tillsynsmyndigheterna regelbundna rapporter om sin verksamhet (inklusive intern rapportering till ledningen och styrelserna och upprättande av årsrapporten). Revisionsrätten och internrevisionstjänsten granskar deras resursanvändning och funktion. Övervakning och rapportering av de åtgärder som ingår i förslaget kommer att stämma överens med de redan befintliga kraven samt eventuella nya krav som detta förslag ger upphov till.

2.2. Förvaltnings- och kontrollsystem

2.2.1. Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

Förvaltningen kommer att skötas indirekt genom de europeiska tillsynsmyndigheterna. Finansieringsmekanismen skulle genomföras genom avgifter som tas ut från de berörda kritiska IKT-tredjepartsleverantörerna.

2.2.2. Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

För den rättsliga, ekonomiska, effektiva och ändamålsenliga användningen av anslag som förslaget ger upphov till förväntas förslaget inte medföra nya betydande risker som inte skulle täckas av ett befintligt internt kontrollramverk. En ny utmaning kan dock vara att säkerställa att avgifter tas ut i tid från de berörda kritiska IKT-tredjepartsleverantörerna.

2.2.3. Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

Förvaltnings- och kontrollsystem i enlighet med förordningarna om de europeiska tillsynsmyndigheterna tillämpas redan. De europeiska tillsynsmyndigheterna samarbetar nära med kommissionens internrevisionstjänst för att säkerställa att lämpliga standarder uppfylls inom alla områden av internkontrollen. Dessa arrangemang kommer att gälla även med avseende på de europeiska tillsynsmyndigheternas roll enligt detta förslag. Dessutom beviljar Europaparlamentet varje budgetår, på rekommendation av kommissionen, ansvarsfrihet för varje europeisk tillsynsmyndighet för genomförandet av deras budget.

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

Specificera befintliga eller planerade förebyggande åtgärder och skyddsåtgärder, t.ex. från strategin för mot bedrägerier.

För att bekämpa bedrägeri, korruption och annan olaglig verksamhet gäller bestämmelserna i Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 av den 11 september 2013 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) för de europeiska tillsynsmyndigheterna utan begränsningar.

De europeiska tillsynsmyndigheterna har en särskild strategi mot bedrägerier och en åtföljande handlingsplan. De europeiska tillsynsmyndigheternas ökade insatser inom bedrägeribekämpning kommer att vara förenliga med reglerna och vägledningen i budgetförordningen (bestämmelser om bedrägeribekämpning som en del av en sund ekonomisk förvaltning), Olafs bedrägeriförebyggande insatser, bestämmelserna i kommissionens strategi mot bedrägerier (KOM(2011) 376) samt med den gemensamma strategin om decentraliserade EU-myndigheter (juli 2012) och den tillhörande färdplanen.

Dessutom fastställs bestämmelserna om genomförande och kontroll av de europeiska tillsynsmyndigheternas budget och tillämpliga finansiella regler i de förordningar som inrättar de europeiska tillsynsmyndigheterna samt deras budgetförordningar, även regler som syftar till att förebygga bedrägerier och oriktigheter.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd.

Rubrik i den fleråriga budgetramen	Budgetrubrik	Type of utgifter	Bidrag			
	Nummer	Diff./Icke-diff.[52]	från Efta-länder[53]	från kandidat-länder[54]	från tredje-länder	enligt artikel 21.2 b i budget-förordningen

Nya budgetrubriker som föreslås

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd.

Rubrik i den fleråriga budgetramen	Budgetrubrik	Type of utgifter	Bidrag			
	Nummer	Diff./Icke-diff.	från Efta-länder	från kandidat-länder	från tredje-länder	enligt artikel 21.2 b i budget-förordningen

52 Differentierade respektive icke-differentierade anslag.

53 Efta: Europeiska frihandelssammanslutningen.

54 Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Beräknad inverkan på utgifterna

3.3. Sammanfattning av den beräknade inverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	Nummer	Rubrik

GD: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**TOTALT**
	Åtaganden	(1)									
	Utbetalningar	(2)									
TOTALA anslag för GD <>	Åtaganden										
	Utbetalningar										

Rubrik i den fleråriga budgetramen		

Miljoner euro (avrundat till tre decimaler)

		2022	2023	2024	2025	2026	2027	**TOTALT**
Generaldirektorat:								
• Personalresurser								
• Övriga administrativa utgifter<>								
GD TOTALT	Anslag							

TOTALA anslag under RUBRIK i den fleråriga budgetramen	(summa åtaganden = summa betalningar)							

Miljoner euro (avrundat till tre decimaler), fasta priser

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTALT**
TOTALA anslag under RUBRIKERNA 1 i den fleråriga budgetramen	Åtaganden							
	Utbetalningar							

3.3.1. Beräknad inverkan på anslagen

☑ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

☐ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler) i fasta priser

Mål- och resultatbetecknin ⇩			2022		2023		2024		2025		2026		2027		**TOTALT**	
	RESULTAT															
	Typ[55]	Genomsnittlig kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Totalt antal	Totala kostnader
SPECIFIKT MÅL nr 1[56]…																
– Resultat																
Delsumma för specifikt mål nr 1																
SPECIFIKT MÅL nr 2…																
– Resultat																
Delsumma specifikt mål nr 2																
TOTALA KOSTNADER																

55 Resultaten som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

56 Mål som redovisats under punkt 1.4.2. ”Specifikt/specifika mål…”.

3.3.2. Beräknad påverkan på personalbehov

3.3.2.1. Sammanfattning

☐ Förslaget/initiativet kräver inte att administrativa anslag tas i anspråk

☑ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler), fasta priser

EBA, Eiopa, Esma	2022	2023	2024	2025	2026	2027	**TOTALT**
Tillfälligt anställda (AD-tjänster)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Tillfälligt anställda (AST-tjänster)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Kontraktsanställda							
Utstationerade nationella experter							
TOTALT	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Personalbehov (heltidsekvivalenter):

EBA, Eiopa, Esma och EEA	2022	2023	2024	2025	2026	2027	**TOTALT**
Tillfälligt anställda (AD-tjänster) EBA = 5, Eiopa = 5, Esma = 5	15	15	15	15	15	15	15
Tillfälligt anställda (AST-tjänster) EBA = 1, Eiopa = 1, EEA = 1	3	3	3	3	3	3	3
Kontraktsanställda							
Utstationerade nationella experter							
TOTALT	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Beräknade krav på personalresurser för (ansvariga) generaldirektorat.

☑ Förslaget/initiativet kräver inte att personalresurser tas i anspråk.

☐ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltal (eller med högst en decimal)

		2022	2023	2024	2025	2026	2027
• **Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)**							
• **Extern personal (i heltidsekvivalenter)**[57]							
XX 01 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)							
XX 01 02 02 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)							
XX 01 04 ***åå***[58]	– vid huvudkontoret [59]						
	– vid delegationer						
XX 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med indirekta forskningsåtgärder)							
10 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med direkta forskningsåtgärder)							
Annan budgetrubrik (ange vilken)							
TOTALT							

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet som redan har avdelats för att förvalta åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	

[57] [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

[58] Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

[59] Framför allt för strukturfonderna, Europeiska jordbruksfonden för landsbygdsutveckling (Ejflu) och Europeiska fiskerifonden (EFF).

Extern personal	

En beskrivning av beräkningen av kostnaden för heltidsekvivalenten bör införas i avsnitt 3 i bilaga V.

3.3.3. Förenlighet med den gällande fleråriga budgetramen

☑ Förslaget/initiativet är förenligt med den gällande fleråriga budgetramen

☐ Förslaget/initiativet kräver omfördelningar under den berörda rubriken i den fleråriga budgetramen

☐ Förslaget/initiativet förutsätter att flexibilitetsmekanismen utnyttjas eller att den fleråriga budgetramen revideras[60].

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt belopp. […]

3.3.4. Bidrag från tredje part

☐ Det ingår inga bidrag från tredje part i det aktuella förslaget eller initiativet.

☑ Förslaget eller initiativet kommer att medfinansieras enligt följande:

Miljoner euro (avrundat till tre decimaler)

EBA

	2022	2023	2024	2025	2026	2027	Totalt
Kostnaderna ska täckas till 100 % av avgifter som tas ut av de enheter som står under tillsyn[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTALA anslag som tillförs genom medfinansiering	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Eiopa

	2022	2023	2024	2025	2026	2027	Totalt
Kostnaderna ska täckas till 100 % av avgifter som tas ut av de enheter som står under tillsyn[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTALA anslag som tillförs genom medfinansiering	1,305	1,811	1,611	1,611	1,611	1,611	9,560

Esma

60 Se artiklarna 11 och 17 i rådets förordning (EU, Euratom) nr 1311/2013 om den fleråriga budgetramen för 2014–2020.

61 100 % av den totala beräknade kostnaden plus arbetsgivarens pensionsavgifter i sin helhet.

62 100 % av den totala beräknade kostnaden plus arbetsgivarens pensionsavgifter i sin helhet.

	2022	2023	2024	2025	2026	2027	Totalt
Kostnaderna ska täckas till 100 % av avgifter som tas ut av de enheter som står under tillsyn[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTALA anslag som tillförs genom medfinansiering	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Beräknad inverkan på inkomsterna

☑ Förslaget/initiativet påverkar inte budgetens inkomstsida.

☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

☐ Påverkan på egna medel

☐ Påverkan på andra inkomster

☐ Ange om inkomsterna har avsatts för utgiftsposter

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstdel:	Disponibla anslag under innevarande budgetår	Förslagets eller initiativets inverkan på inkomsterna[64]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	För in så många år som behövs för att redovisa inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel…….								

Ange vilka budgetrubriker i utgiftsdelen som berörs i de fall där inkomster i diversekategorin kommer att avsättas för särskilda ändamål.

[…]

Ange med vilken metod inverkan på inkomsterna har beräknats.

[…]

63 100 % av den totala beräknade kostnaden plus arbetsgivarens pensionsavgifter i sin helhet.

64 Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.

BILAGA

Allmänna antaganden

Avdelning I – Personalkostnader

Följande särskilda antaganden har tillämpats vid beräkningen av personalutgifterna på grundval av de identifierade personalbehov som beskrivs nedan:

- Den ytterligare personal som anställs under 2022 kostnadsberäknas för sex månader med tanke på den tid som antas behövas för att rekrytera den.
- Den genomsnittliga årskostnaden för en tillfälligt anställd är 150 000 euro, för en kontraktsanställd 85 000 euro och för en utstationerad nationell expert 80 000 euro, och dessa belopp innefattar kringkostnader på 25 000 euro (fastigheter, it osv.).
- De korrigeringskoefficienter som är tillämpliga på personalens löner i Paris (EBA och Esma) och Frankfurt (Eiopa) är 117,7 respektive 99,4.
- Arbetsgivarens pensionsavgifter för tillfälligt anställda har baserats på de standardgrundlöner som ingår i de normala genomsnittliga årskostnaderna, dvs. 95 660 euro.
- De ytterligare tillfälligt anställda tillhör kategorierna AD5 och AST.

Avdelning II – Infrastrukturs- och driftsutgifter

Kostnaderna bygger på att antalet anställda under den andel av ett år som de är anställda multipliceras med standardkringkostnaden, dvs. 25 000 euro.

Avdelning III – Driftsutgifter

Kostnaderna beräknas på grundval av följande antaganden:

- Översättningskostnaderna fastställs till 350 000 euro per år för var och en av de europeiska tillsynsmyndigheterna.
- Engångskostnaderna på 500 000 euro per europeisk tillsynsmyndighet antas genomföras under de två åren 2022 och 2023 på grundval av en uppdelning på 50 %–50 %. De årliga underhållskostnaderna från och med 2024 beräknas till 50 000 EUR per ESA.
- De årliga tillsynskostnaderna på plats uppskattas till 200 000 euro per europeisk tillsynsmyndighet.

Dessa beräkningar leder till följande kostnader per år:

Rubrik i den fleråriga budgetramen	Nummer	

Fasta priser

EBA:			2022	2023	2024	2025	2026	2027	**TOTAL T**
Avdelning 1:	Åtaganden	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Utbetalningar	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Avdelning 2:	Åtaganden	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Utbetalningar	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Avdelning 3:	Åtaganden	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Utbetalningar	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTALA anslag för EBA	Åtaganden	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Utbetalningar	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Eiopa:			2022	2023	2024	2025	2026	2027	**TOTAL T**
Avdelning 1:	Åtaganden	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Utbetalningar	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Avdelning 2:	Åtaganden	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Utbetalningar	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Avdelning 3:	Åtaganden	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Utbetalningar	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000

TOTALA anslag för Eiopa	Åtaganden	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Utbetalningar	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

Esma:			2022	2023	2024	2025	2026	2027	**TOTAL T**
Avdelning 1:	Åtaganden	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Utbetalningar	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Avdelning 2:	Åtaganden	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Utbetalningar	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Avdelning 3:	Åtaganden	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Utbetalningar	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTALA anslag för Esma	Åtaganden	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Utbetalningar	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Förslaget kräver att driftsanslag tas i anspråk enligt följande:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler) i fasta priser

EBA

Mål- och resultatbetecknin ⇩			2022		2023		2024		2025		2026		2027			
	RESULTAT															
	Typ[65]	Genomsnittlig kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Totalt antal	Totala kostnader
SPECIFIKT MÅL NR 1[66] Direkt tillsyn av kritiska IKT-tredjepartsleverantörer																
– Resultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Delsumma för specifikt mål nr 1																
SPECIFIKT MÅL nr 2…																
– Resultat																
Delsumma specifikt mål nr 2																
TOTALA KOSTNADER				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

Eiopa

Mål- och resultatbetecknin ⇩			2022		2023		2024		2025		2026		2027			
	RESULTAT															
	Typ[67]	Genomsnittlig kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Totalt antal	Totala kostnader
SPECIFIKT MÅL NR 1[68] Direkt tillsyn av kritiska IKT-tredjepartsleverantörer																
– Resultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Delsumma för specifikt mål nr 1																
SPECIFIKT MÅL nr 2…																

65 Resultaten som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

66 Mål som redovisats under punkt 1.4.2. ”Specifikt/specifika mål…”.

67 Resultaten som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

68 Mål som redovisats under punkt 1.4.2. ”Specifikt/specifika mål…”.

– Resultat																
Delsumma specifikt mål nr 2																
TOTALA KOSTNADER				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

Esma

Mål- och resultatbetecknin ⇩			2022		2023		2024		2025		2026		2027			
	RESULTAT															
	Typ[69]	Genomsnittlig kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Nej	Kostnad	Totalt antal	Totala kostnader
SPECIFIKT MÅL NR 1[70] Direkt tillsyn av kritiska IKT-tredjepartsleverantörer																
– Resultat				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Delsumma för specifikt mål nr 1																
SPECIFIKT MÅL nr 2…																
– Resultat																
Delsumma specifikt mål nr 2																
TOTALA KOSTNADER				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

Tillsynsverksamheten ska finansieras fullt ut genom avgifter som tas ut av de enheter som omfattas av tillsyn enligt följande:

EBA

	2022	2023	2024	2025	2026	2027	Totalt

[69] Resultaten som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

[70] Mål som redovisats under punkt 1.4.2. ”Specifikt/specifika mål…”.

Kostnaderna ska täckas till 100 % av avgifter som tas ut av de enheter som omfattas av tillsyn[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTALA anslag som tillförs genom medfinansiering	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Eiopa

	2022	2023	2024	2025	2026	2027	Totalt
Kostnaderna ska täckas till 100 % av avgifter som tas ut av de enheter som omfattas av tillsyn[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTALA anslag som tillförs genom medfinansiering	1,305	1,811	1,611	1,611	1,611	1,611	9,560

Esma

	2022	2023	2024	2025	2026	2027	Totalt
Kostnaderna ska täckas till 100 % av avgifter som tas ut av de enheter som omfattas av tillsyn[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTALA anslag som tillförs genom medfinansiering	1,373	1,948	1,748	1,748	1,748	1,748	10,313

SPECIFIKA UPPGIFTER

Direkta tillsynsbefogenheter

Inledningsvis bör det erinras om att enheter som står under Esmas direkta tillsyn bör betala avgifter till Esma (engångskostnader för registrering och löpande kostnader för kontinuerlig tillsyn). Detta är fallet för kreditvärderingsinstitut (se kommissionens delegerade förordning (EU) nr 272/2012) och transaktionsregister (kommissionens delegerade förordning (EU) nr 1003/2013).

Enligt detta lagstiftningsförslag kommer de europeiska tillsynsmyndigheterna att anförtros nya uppgifter som syftar till att främja konvergens när det gäller tillsynsstrategier för IKT-tredjepartsrisker inom finanssektorn genom att låta kritiska tredjepartsleverantörer av IKT-tjänster omfattas av en unionstillsynsram.

Den tillsynsram som föreskrivs i detta förslag bygger på den befintliga institutionella strukturen på området finansiella tjänster, där de europeiska tillsynsmyndigheternas gemensamma kommitté

[71] 100 % av den totala beräknade kostnaden plus arbetsgivarens pensionsavgifter i sin helhet.
[72] 100 % av den totala beräknade kostnaden plus arbetsgivarens pensionsavgifter i sin helhet.
[73] 100 % av den totala beräknade kostnaden plus arbetsgivarens pensionsavgifter i sin helhet.

säkerställer sektorsövergripande samordning i alla frågor som rör IKT-risker, i enlighet med sina uppgifter i fråga om cybersäkerhet, med stöd av den relevanta underkommitté (tillsynsforum) som utför förberedande arbete inför enskilda beslut och kollektiva rekommendationer till kritiska tredjepartsleverantörer av IKT-tjänster.

Genom denna ram får de europeiska tillsynsmyndigheter som har utsetts som ledande tillsynsorgan för varje kritisk tredjepartsleverantör av IKT-tjänster befogenheter att se till att leverantörer av tekniska tjänster som spelar en avgörande roll för den finansiella sektorns funktion övervakas på ett adekvat sätt på europeisk nivå. Tillsynsskyldigheterna anges i förslaget och förtydligas ytterligare i motiveringen. De omfattar rätten att begära all relevant information och dokumentation för att genomföra allmänna utredningar och kontroller, lämna rekommendationer och därefter lägga fram rapporter om de åtgärder som vidtagits eller åtgärder som vidtagits för att följa rekommendationerna.

För att utföra de nya uppgifter som avses i detta förslag ska därför ytterligare personal som är specialiserad på IKT-risker och som är inriktad på att bedöma beroendeförhållanden till tredje part anställas av de europeiska tillsynsmyndigheterna.

Personalbehovet kan uppskattas till 6 heltidsekvivalenter för varje myndighet (5 AD och 1 AST som stöd för dem). De europeiska tillsynsmyndigheterna kommer också att ådra sig ytterligare it-kostnader, uppskattningsvis 500 000 euro (engångskostnader) och 50 000 euro per år för var och en av de tre europeiska tillsynsmyndigheterna för underhållskostnader. Ett viktigt inslag i fullgörandet av de nya uppgifterna är uppdragen att utföra kontroller och revisioner på plats, som kan uppskattas till 200 000 euro per år för varje europeisk tillsynsmyndighet. Översättningskostnader för de olika dokument som de europeiska tillsynsmyndigheterna skulle erhålla från de kritiska tredjepartsleverantörerna av IKT-tjänster ingår också i raden om driftskostnader och uppgår till 350 000 euro per år.

Alla de administrativa kostnader som nämns ovan kommer att finansieras helt genom de årliga avgifter som de europeiska tillsynsmyndigheterna tar ut från de övervakade kritiska leverantörerna av IKT-tjänster (ingen påverkan på EU:s budget).