I

(Lagstiftningsakter)

FÖRORDNINGAR

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2022/2554

av den 14 december 2022

om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011

(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 ([1]),

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([2]),

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) I den digitala tidsåldern stöder informations- och kommunikationstekniken (IKT) komplexa system som används för dagliga aktiviteter. Den får våra ekonomier att fungera inom viktiga sektorer, inbegripet finanssektorn, och förbättrar den inre marknadens funktion. Ökad digitalisering och sammanlänkning ökar också IKT-risk och gör samhället som helhet – och i synnerhet det finansiella systemet – mer sårbart för cyberhot eller IKT-avbrott. Den allmänt utbredda användningen av IKT-system och hög digitalisering och konnektivitet är i dag centrala inslag i den verksamhet som bedrivs av unionens finansiella entiteter, men deras digitala motståndskraft måste fortfarande hanteras bättre och integreras i deras bredare operativa ramar.

(2) Användningen av IKT har under de senaste årtiondena fått en avgörande roll inom tillhandahållandet av finansiella tjänster och har nått den punkt där den i dag är avgörande för driften av alla finansiella entiteters vanliga dagliga funktioner. Digitaliseringen omfattar i dag 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, skadereglering och back-office-verksamhet. Försäkringssektorn har också omvandlats genom användningen av IKT,

([1]) EUT C 343, 26.8.2021, s. 1.
([2]) EUT C 155, 30.4.2021, s. 38.
([3]) Europaparlamentets ståndpunkt av den 10 november 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 28 november 2022.

från framväxten av försäkringsförmedlare som erbjuder sina tjänster online med hjälp av försäkringsteknik (insurtech), till digital försäkringsgarantiverksamhet. Hela finanssektorn har blivit till stor del digital, och digitaliseringen har också fördjupat sammanlänkningarna och beroendena inom finanssektorn och med tredjepartsinfrastruktur och tredjepartstjänsteleverantörer.

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

(4) På senare år har IKT-risk uppmärksammats av internationella, unionens och nationella beslutsfattare, tillsynsmyndigheter och standardiseringsorgan i ett försök att öka den digitala motståndskraften, fastställa standarder och samordna reglerings- eller tillsynsarbete. På internationell nivå har Baselkommittén för banktillsyn, kommittén för betalningar och marknadsinfrastruktur, rådet för finansiell stabilitet, Financial Stability Institute samt G7 och G20 som mål att förse behöriga myndigheter och marknadsoperatörer inom olika jurisdiktioner med verktyg för att stärka motståndskraften hos deras finansiella system. Det arbetet har också motiverats av behovet av att vederbörligen beakta IKT-risk i ett globalt finansiellt system som är starkt sammanlänkat och eftersträva större samstämmighet vad gäller relevant bästa praxis.

(5) Trots unionens och nationella riktade politiska initiativ och lagstiftningsinitiativ fortsätter IKT-risk att utgöra en utmaning för den operativa motståndskraften, prestandan och stabiliteten i unionens finansiella system. De reformer 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 och tillsynsmässiga perspektiv samt vad gäller marknadsbeteende. Även om IKT-säkerhet och digital motståndskraft ingår i de operativa riskerna har de inte uppmärksammats lika mycket i lagstiftningsagendan efter finanskrisen och har bara utvecklats inom vissa områden av unionens politik och regelverk för finansiella tjänster, eller endast i ett fåtal medlemsstater.

(6) I sitt meddelande av den 8 mars 2018 med titeln *Handlingsplanen för fintech: – ett viktigt steg mot en mer konkurrenskraftig europeisk finanssektor* betonade kommissionen att det är ytterst viktigt att göra unionens finanssektor mer motståndskraftig, inbegripet ur ett operativt perspektiv för att säkerställa dess tekniska säkerhet och goda funktion, och dess snabba återställning efter IKT-relaterade överträdelser och IKT-incidenter, så att finansiella tjänster i förlängningen kan tillhandahållas på ett effektivt och smidigt sätt i hela unionen, inbegripet i stressituationer, samtidigt som konsumenternas och marknadens förtroende bevaras.

(7) I april 2019 utfärdade gemensamt Europeiska tillsynsmyndigheten (Europeiska bankmyndigheten, EBA) inrättad genom Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([4]), Europeiska tillsynsmyndigheten (Europeiska försäkrings- och tjänstepensionsmyndigheten, Eiopa) inrättad genom Europaparlamentets och rådets förordning (EU) nr 1094/2010 ([5]), och Europeiska tillsynsmyndigheten (Europeiska värdepappers- och

([4]) Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

([5]) Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48).

marknadsmyndigheten, Esma) inrättad genom Europaparlamentets och rådets förordning (EU) nr 1095/2010 ([6]) (gemensamt kallade *de europeiska tillsynsmyndigheterna*) teknisk rådgivning och efterlyste ett enhetligt tillvägagångssätt för IKT-risk inom finanssektorn och rekommenderade en proportionell förstärkning av den digitala operativa motståndskraften i sektorn för finansiella tjänster genom ett sektorsspecifikt initiativ från unionen.

(8) Unionens finansiella sektor regleras genom ett 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 digital operativ motståndskraft, genom att behöriga myndigheters mandat stärks så att de kan övervaka hanteringen av IKT-risk inom den finansiella sektorn i syfte att skydda den inre marknadens integritet och effektivitet samt för att främja dess korrekta funktion.

(9) Skillnader i lagstiftning och olika nationella reglerings- eller tillsynsstrategier för IKT-risk skapar hinder för den inre marknadens funktion för finansiella tjänster och hindrar ett smidigt utövande av etableringsfriheten och tillhandahållandet av tjänster för finansiella entiteter som bedriver gränsöverskridande verksamhet. Konkurrensen mellan samma typ av finansiella entiteter med verksamhet i olika medlemsstater skulle också kunna snedvridas. Detta gäller särskilt de områden där unionens harmonisering har varit mycket begränsad, såsom testning av digital operativ motståndskraft, eller saknas, såsom övervakning av IKT-tredjepartsrisk. Skillnader som härrör från den planerade utvecklingen på nationell nivå skulle kunna skapa ytterligare hinder för den inre marknadens funktion, till skada för marknadsaktörer och finansiell stabilitet.

(10) På grund av att bestämmelser i fråga om IKT-risk endast delvis behandlas på unionsnivå finns för närvarande luckor eller överlappningar på viktiga områden, t.ex. när det gäller IKT-relaterad incidentrapportering och testning av digital operativ motståndskraft, samt 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 entiteter som bedriver gränsöverskridande verksamhet eller som innehar flera tillstånd (en finansiell entitet 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-risk 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 entiteter. Utvecklingen av IKT-kapacitet och övergripande motståndskraft hos finansiella entiteter baserat på dessa 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 fördraget om Europeiska unionens funktionssätt (EUF-fördraget), så som artikeln tolkats i Europeiska unionens domstols (domstolen) fasta rättspraxis.

(12) Denna förordning syftar till att konsolidera och uppgradera IKT-riskkraven som en del av de operativa riskkraven, vilka hittills har behandlats separat i olika unionsrättsakter. Även om dessa akter omfattade de huvudsakliga kategorierna av finansiell risk (t.ex. kreditrisk, marknadsrisk, motpartsrisk, likviditetsrisk och marknadsbeteenderisker), behandlades inte alla komponenter i den operativa motståndskraften på ett heltäckande sätt när dessa akter antogs. När reglerna rörande operativa risker närmare utformades i dessa unionsrättsakter föredrogs ofta en traditionell kvantitativ strategi för riskhantering (nämligen fastställande av ett kapitalkrav för att täcka IKT-risk) i stället för riktade kvalitativa regler avseende skydd, upptäckt, begränsning, återställning och avhjälpande av IKT-relaterade incidenter eller avseende rapporteringskapacitet och digital testkapacitet. Dessa akter var i första hand

([6]) Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84).

avsedda att omfatta och uppdatera grundläggande regler om tillsyn, marknadsintegritet eller marknadsbeteende. Genom att olika regler för IKT-risk konsolideras och uppgraderas bör alla bestämmelser om digitala risker inom finanssektorn för första gången samlas på ett enhetligt sätt i en enda rättsakt. Denna förordning täpper till luckorna eller avhjälper bristen på konsekvens i vissa av de tidigare rättsakterna, inbegripet i fråga om den terminologi som används i dem och som uttryckligen hänvisar till IKT-risk genom riktade regler om IKT-riskhanteringsförmåga, incidentrapportering, testning av operativ motståndskraft och övervakning av IKT-tredjepartsrisk. Denna förordning bör därför också öka medvetenheten om IKT-risk och understryka att IKT-incidenter och bristande operativ motståndskraft kan äventyra finansiella entiteters sundhet.

(13) Finansiella entiteter bör följa samma tillvägagångssätt och samma principbaserade regler i sin hantering av IKT-risk med beaktande av sin storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser. Enhetlighet bidrar till att öka förtroendet för det finansiella systemet och bevara dess stabilitet, särskilt i tider av starkt beroende av IKT-system, IKT-plattformar och IKT-infrastrukturer, vilket medför ökad digital risk. Iakttagande av grundläggande cyberhygien bör också leda till att det går att undvika höga kostnader för ekonomin, genom att effekterna av och kostnaderna för IKT-avbrott minimeras.

(14) En förordning bidrar till att minska lagstiftningens komplexitet, främjar konvergens i tillsynen och ökar rättssäkerheten, och bidrar också till att begränsa efterlevnadskostnaderna, särskilt för finansiella entiteter som bedriver gränsöverskridande verksamhet, och till att minska snedvridningen av konkurrensen. Därför är valet av en förordning för inrättandet av en gemensam ram för finansiella entiteters digitala operativa motståndskraft det lämpligaste sättet att garantera en enhetlig och samstämmig tillämpning av alla delar av IKT-riskhanteringen inom unionens finanssektor.

(15) Europaparlamentets och rådets direktiv (EU) 2016/1148 ([7]) var den första övergripande ramen för cybersäkerhet som antogs på unionsnivå och som också tillämpas på tre typer av finansiella entiteter, nämligen kreditinstitut, handelsplatser och centrala motparter. Eftersom det i direktiv (EU) 2016/1148 fastställdes en mekanism för identifiering på nationell nivå av leverantörer av samhällsviktiga tjänster, var det endast vissa kreditinstitut, handelsplatser och centrala motparter som identifierades av medlemsstaterna som inkluderades i direktivets tillämpningsområde i praktiken och därmed är skyldiga att uppfylla de rapporteringskrav i fråga om IKT-säkerhet och IKT-incidenter som fastställs i direktivet. I Europaparlamentets och rådets direktiv (EU) 2022/2555 ([8]) fastställs enhetliga kriterier för att avgöra vilka entiteter som omfattas av dess tillämpningsområde (storleksbaserad regel) samtidigt som de tre typerna av finansiella entiteter behålls inom dess tillämpningsområde.

(16) Eftersom denna förordning leder till en ökad harmonisering av de olika komponenterna av digital motståndskraft genom att det införs strängare krav på IKT-riskhantering och IKT-relaterad incidentrapportering än de som fastställs i den nuvarande unionsrätten avseende finansiella tjänster, innebär denna högre nivå en ökad harmonisering även jämfört med kraven i direktiv (EU) 2022/2555. Denna förordning utgör följaktligen *lex specialis* i förhållande till direktiv (EU) 2022/2555. Det är samtidigt mycket viktigt att upprätthålla en stark koppling mellan finanssektorn och unionens övergripande ram för cybersäkerhet, som för närvarande fastställs i direktiv (EU) 2022/2555 för att säkerställa överensstämmelse med de strategier för cybersäkerhet som antagits av medlemsstaterna och göra det möjligt för finansiella tillsynsmyndigheter att få kännedom om cyberincidenter som påverkar andra sektorer som omfattas av det direktivet.

([7]) 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).

([8]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (se sidan 80 i detta nummer av EUT).

(17) I enlighet med artikel 4.2 i fördraget om Europeiska unionen och utan att det påverkar domstolens rättsliga prövning bör denna förordning inte påverka medlemsstaternas ansvar vad gäller väsentliga statliga funktioner rörande allmän säkerhet, försvar och skyddet av den nationella säkerheten, till exempel när det gäller tillhandahållande av information som står i strid med skyddet av den nationella säkerheten.

(18) För att möjliggöra sektorsövergripande lärande och effektivt ta vara på erfarenheter från andra sektorer när det gäller att hantera cyberhot bör de finansiella entiteter som avses i direktiv (EU) 2022/2555 fortsätta att ingå i ”ekosystemet” i det direktivet (t.ex. samarbetsgrupp samt nätverket av entiteter för hantering av it-säkerhetsincidenter (CSIRT-enheter)). De europeiska tillsynsmyndigheterna och de nationella behöriga myndigheterna bör kunna delta i de strategiska politiska diskussionerna och det tekniska arbetet i samarbetsgruppen enligt det direktivet och kunna utbyta information och samarbeta ytterligare med de gemensamma kontaktpunkter som har utsetts eller inrättats i enlighet med det direktivet. De behöriga myndigheterna enligt denna förordning bör också samråda och samarbeta med CSIRT-enheter. De behöriga myndigheterna bör också kunna begära teknisk rådgivning från de behöriga myndigheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555 samt inrätta samarbetsarrangemang i syfte att säkerställa effektiva och snabba samordningsmekanismer.

(19) Med tanke på de starka sambanden mellan finansiella entiteters digitala motståndskraft och fysiska motståndskraft krävs ett enhetligt tillvägagångssätt för kritiska entiteters motståndskraft i denna förordning och i Europaparlamentets och rådets direktiv (EU) 2022/2557 ([9]). Eftersom finansiella entiteters fysiska motståndskraft behandlas övergripande i de skyldigheter rörande IKT-riskhantering och rapportering som omfattas av denna förordning, bör de skyldigheter som fastställs i kapitlen III och IV i direktiv (EU) 2022/2557 inte tillämpas på finansiella entiteter som omfattas av tillämpningsområdet för det direktivet.

(20) Leverantörer av molntjänster är en kategori av leverantörer av digitala infrastrukturer som omfattas av direktiv (EU) 2022/2555. Den unionstillsynsram (*tillsynsramen*) som inrättas genom denna förordning är tillämplig på alla kritiska tredjepartsleverantörer av IKT-tjänster, inbegripet leverantörer av molntjänster som tillhandahåller IKT-tjänster till finansiella entiteter, och bör betraktas som ett komplement till den tillsyn som utförs enligt direktiv (EU) 2022/2555. Den tillsynsram som inrättas genom denna förordning bör dessutom omfatta leverantörer av molntjänster, i avsaknad av en unionsomfattande sektorsövergripande ram för inrättande av en digital tillsynsmyndighet.

(21) För att finansiella entiteter ska kunna upprätthålla full kontroll över IKT-risk måste de ha övergripande kapacitet som möjliggör en kraftfull och effektiv IKT-riskhantering, liksom särskilda mekanismer och riktlinjer för att hantera alla IKT-relaterade incidenter och rapportera allvarliga IKT-relaterade incidenter. På samma sätt bör finansiella entiteter ha inrättat strategier för testning av IKT-system, IKT-kontroller och IKT-processer samt för hantering av IKT-tredjepartsrisk. Referensnivån för digital operativ motståndskraft hos finansiella entiteter bör höjas och samtidigt möjliggöra en proportionell tillämpning av kraven för vissa finansiella entiteter, särskilt mikroföretag, liksom finansiella entiteter som är föremål för en förenklad IKT-riskhanteringsram. För att underlätta en effektiv tillsyn av tjänstepensionsinstitut som är proportionell och tillgodoser behovet att minska de behöriga myndigheternas administrativa bördor bör relevanta nationella tillsynsramar för sådana finansiella entiteter beakta deras storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser, även när de relevanta trösklar som fastställs i artikel 5 i Europaparlamentets och rådets direktiv (EU) 2016/2341 ([10]) överskrids. Framför allt bör tillsynsverksamhet i första hand inriktas på behovet av att hantera allvarliga risker i samband med IKT-riskhantering i en särskild entitet.

([9]) Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och upphävande av rådets direktiv 2008/114/EG (se sidan 164 i detta nummer av EUT).

([10]) Europaparlamentets och rådets direktiv (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut (EUT L 354, 23.12.2016, s. 37).

De behöriga myndigheterna bör också upprätthålla ett vaksamt men proportionellt tillvägagångssätt vad gäller tillsyn över tjänstepensionsinstitut som, i enlighet med artikel 31 i direktiv (EU) 2016/2341, utkontrakterar en betydande del av sin kärnverksamhet, till exempel kapitalförvaltning, försäkringstekniska beräkningar, redovisning och databehandling till tjänsteleverantörer.

(22) Tröskelvärden och taxonomier för rapportering av IKT-relaterade incidenter varierar avsevärt på nationell nivå. Även om en samsyn kan uppnås genom det relevanta arbete som utförs av Europeiska unionens cybersäkerhetsbyrå (Enisa), som inrättats genom Europaparlamentets och rådets förordning (EU) 2019/881 ([11]), och samarbetsgruppen enligt direktiv (EU) 2022/2555, kan det fortfarande förekomma eller växa fram olika strategier för tröskelvärden och taxonomier för andra finansiella entiteter. Dessa skillnader medför flera krav som finansiella entiteter måste uppfylla, särskilt när de är verksamma i flera medlemsstater och när de ingår i en finansiell koncern. Sådana skillnader kan dessutom hindra inrättandet av ytterligare enhetliga eller centraliserade mekanismer på unionsnivå som påskyndar rapporteringsprocessen och underlättar ett snabbt och smidigt informationsutbyte mellan behöriga myndigheter, vilket är avgörande för att hantera IKT-risk vid storskaliga attacker med eventuella konsekvenser för det finansiella systemet.

(23) För att minska den administrativa bördan och eventuellt dubbla rapporteringsskyldigheter för vissa finansiella entiteter bör kravet på incidentrapportering enligt Europaparlamentets och rådets direktiv (EU) 2015/2366 ([12]) upphöra att tillämpas för betaltjänstleverantörer som omfattas av tillämpningsområdet för denna förordning. Därför bör de kreditinstitut, institut för elektroniska pengar, betalningsinstitut och leverantörer av kontoinformationstjänster som avses i artikel 33.1 i det direktivet, från och med tillämpningsdagen för denna förordning rapportera enligt denna förordning, alla betalningsrelaterade operativa incidenter eller säkerhetsincidenter som tidigare rapporterades enligt det direktivet, oavsett om sådana incidenter är IKT-relaterade.

(24) För att de behöriga myndigheterna ska kunna fullgöra 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, bör denna förordning fastställa regler för att uppnå ett stabilt rapporteringssystem för IKT-relaterade incidenter, där relevanta krav åtgärdar befintliga luckor i rätten avseende finansiella tjänster och undanröjer överlappningar och dubbleringar för att minska kostnaderna. Det är därför viktigt att harmonisera rapporteringssystemet för IKT-relaterade incidenter genom att kräva att alla finansiella entiteter rapporterar till sina behöriga myndigheter genom en harmoniserad ram i enlighet med denna förordning. Dessutom bör de europeiska tillsynsmyndigheterna ges befogenhet att närmare specificera relevanta delar i ramen för rapportering av IKT-relaterade incidenter, såsom taxonomi, tidsramar, datamängder, mallar och tillämpliga tröskelvärden. För att säkerställa fullständig överensstämmelse med direktiv (EU) 2022/2555 bör finansiella entiteter på frivillig basis tillåtas rapportera betydande cyberhot till den relevanta behöriga myndigheten, när de anser att cyberhotet är relevant för det finansiella systemet, tjänsteanvändare eller kunder.

(25) Krav på testning av digital operativ motståndskraft har utarbetats i vissa finansiella delsektorer med ramar som inte alltid är harmoniserade fullt ut. Detta leder till potentiellt dubbla kostnader för gränsöverskridande finansiella entiteter och gör ett ömsesidigt erkännande av testresultaten för digital operativ motståndskraft komplicerat, vilket i sin tur kan fragmentera den inre marknaden.

([11]) 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).

([12]) Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35).

(26) I de fall där det inte krävs någon IKT-testning förblir dessutom sårbarheter oupptäckta och leder till att en finansiell entitet utsätts för IKT-risk, och skapar i förlängningen en högre risk för den finansiella sektorns stabilitet och integritet. Utan unionsåtgärder skulle testningen av digital operativ motståndskraft fortsätta att vara inkonsekvent och det skulle inte finnas något system för ömsesidigt erkännande av IKT-testresultat i olika jurisdiktioner. Eftersom det dessutom är osannolikt att andra finansiella delsektorer skulle anta testsystem i en meningsfull omfattning skulle de också gå miste om de potentiella fördelarna med en testram, t.ex. att avslöja IKT-sårbarheter och IKT-risker, och att testa försvarskapacitet och driftskontinuitet, vilket bidrar till att öka kundernas, leverantörernas och affärspartnernas förtroende. För att åtgärda dessa överlappningar, skillnader och luckor är det nödvändigt att fastställa regler som syftar till ett samordnat testsystem för finansiella entiteter, för att på så sätt underlätta ömsesidigt erkännande av avancerade tester för de finansiella entiteter som uppfyller de krav som fastställs i denna förordning.

(27) Finansinstitutens beroende av användningen 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.

(28) Den omfattande användningen av IKT-tjänster framgår av komplexa kontraktsmässiga arrangemang, där finansiella entiteter 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, även när dessa är inskrivna i deras kontraktsmässiga arrangemang. Många av de kontraktsmässiga arrangemangen innehåller dessutom inte tillräckliga skyddsåtgärder som möjliggör en fullständig övervakning av utkontrakteringsprocesser, vilket gör att den finansiella entiteten 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 kontraktsmässiga arrangemang inte alltid tillgodoser finansbranschaktörernas individuella eller särskilda behov.

(29) Även om unionsrätten avseende finansiella tjänster omfattar vissa allmänna regler om utkontraktering är övervakningen av avtalsdimensionen inte helt förankrad i unionsrätten. Tydliga och skräddarsydda unionsstandarder som är tillämpliga på de kontraktsmässiga arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster saknas, och därmed hanteras inte den externa IKT-riskkällan på ett heltäckande sätt. Det är därför nödvändigt att fastställa vissa nyckelprinciper för att vägleda finansiella entiteters hantering av IKT-tredjepartsrisker, vilka är särskilt viktiga när finansiella entiteter använder tredjepartsleverantörer av IKT-tjänster för att stödja kritiska eller viktiga funktioner. Dessa principer bör åtföljas av en uppsättning grundläggande avtalsenliga rättigheter i samband med flera aspekter av fullgörandet och avslutandet av kontraktsmässiga arrangemang i syfte att tillhandahålla vissa minimiskyddsåtgärder för att stärka finansiella entiteters förmåga att effektivt övervaka alla IKT-risker som uppstår på tredjepartstjänsteleverantörsnivå. De principerna kompletterar den sektorsrätt som är tillämplig på utkontraktering.

(30) Det är i dagsläget uppenbart att det råder en viss brist på homogenitet och konvergens vad gäller övervakningen av IKT-tredjepartsrisker och beroende av IKT-tredjeparter. Trots ansträngningarna för att hantera utkontraktering, t.ex. EBA:s riktlinjer för utkontraktering från 2019 och Esmas riktlinjer för utkontraktering till molntjänstleverantörer från 2021, behandlas den större frågan om att motverka systemrisker som kan utlösas av finanssektorns exponering mot ett begränsat antal kritiska tredjepartsleverantörer av IKT-tjänster inte i tillräcklig utsträckning i unionsrätten. Denna avsaknad av regler på unionsnivå förvärras av att det inte finns några nationella regler för mandat och verktyg som gör det möjligt för finansiella tillsynsmyndigheter att skaffa sig en god bild av beroendet av IKT-tredjeparter och att på lämpligt sätt övervaka risker som uppstår till följd av koncentration av beroenden av IKT-tredjeparter.

(31) Med hänsyn till de potentiella systemrisker som den ökade utkontrakteringen och koncentrationen av IKT-tredjeparter medför, och till de otillräckliga nationella mekanismer som ger finansiella tillsynsmyndigheter lämpliga verktyg för att kvantitativt och kvalitativt fastställa och åtgärda konsekvenserna av IKT-risk som uppstår hos kritiska tredjepartsleverantörer av IKT-tjänster, är det nödvändigt att inrätta en lämplig tillsynsram som möjliggör en kontinuerlig övervakning av verksamheten hos tredjepartsleverantörer av IKT-tjänster som är kritiska tredjepartsleverantörer av IKT-tjänster till finansiella entiteter, och samtidigt säkerställa konfidentialitet och säkerhet för kunder som inte är finansiella entiteter. Tillhandahållandet av IKT-tjänster inom en koncern medför specifika risker och fördelar, men det bör inte automatiskt anses mindre riskfyllt än tillhandahållande av IKT-tjänster från leverantörer utanför en finansiell koncern, och bör därför omfattas av samma regelverk. När IKT-tjänster tillhandahålls inom samma finansiella koncern kan dock finansiella entiteter ha större kontroll över koncerninterna leverantörer, vilket bör beaktas vid den övergripande riskbedömningen.

(32) I och med att IKT-risker blir alltmer komplexa och sofistikerade kommer effektiva åtgärder för att upptäcka och förebygga IKT-risk att i hög grad vara beroende av regelbundet utbyte mellan finansiella entiteter av underrättelser om hot och sårbarhet. Informationsutbyte bidrar till att skapa ökad medvetenhet om cyberhot. Detta ökar i sin tur finansiella entiteters förmåga att förhindra att cyberhot blir verkliga IKT-relaterade incidenter, och gör det möjligt för finansiella entiteter att på ett mer effektivt sätt begränsa IKT-relaterade incidenters inverkan och att återhämta sig snabbare. I avsaknad av vägledning på unionsnivå verkar flera faktorer ha hindrat sådant utbyte av underrättelser, särskilt osäkerhet om förenligheten med dataskyddsregler, antitrustregler och ansvarsregler.

(33) 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 därför i nuläget fortfarande begränsad och fragmenterad, med relevanta utbyten som oftast görs lokalt (via nationella initiativ) och inga enhetliga unionsomfattande arrangemang för informationsutbyte som är anpassade till behoven i ett integrerat finansiellt system. Det är därför viktigt att stärka dessa kommunikationskanaler.

(34) Finansiella entiteter bör därför uppmuntras att sinsemellan utbyta information och underrättelser om cyberhot, och 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 genom att delta i arrangemang för informationsutbyte. 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 cyberhot genom att snabbt begränsa spridningen av IKT-risk och hindra potentiella spridningseffekter genom de finansiella kanalerna. Dessa mekanismer bör överensstämma med unionens tillämpliga konkurrensrättsliga regler som anges i kommissionens meddelande av den 14 januari 2011 med titeln *Riktlinjer för tillämpningen av artikel 101 i fördraget om Europeiska unionens funktionssätt på horisontella samarbetsavtal* samt med unionens dataskyddsregler, särskilt Europaparlamentets och rådets förordning (EU) 2016/679 ([13]). De bör fungera på grundval av en eller flera av de rättsliga grunder som fastställs i artikel 6 i den förordningen, till exempel i samband med sådan behandling av personuppgifter som är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, enligt artikel 6.1 f i den förordningen, liksom i samband med den behandling av personuppgifter som är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige, som är nödvändig för att utföra en uppgift i allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning, enligt artikel 6.1 c respektive e i den förordningen.

([13]) 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).

(35) För att upprätthålla en hög nivå av digital operativ motståndskraft i hela den finansiella sektorn, och samtidigt hålla jämna steg med den tekniska utvecklingen, bör denna förordning hantera de risker som härrör från alla typer av IKT-tjänster. I det syftet bör definitionen av IKT-tjänster inom ramen för denna förordning ges en vid tolkning för att omfatta digitala tjänster och datatjänster som tillhandahålls fortlöpande genom IKT-system till en eller flera interna eller externa användare. Den definitionen bör till exempel omfatta s.k. over-the-top-tjänster, som omfattas av kategorin elektroniska kommunikationstjänster. Den bör endast utesluta den begränsade kategori av traditionella analoga telefonitjänster som räknas som tjänster inom det allmänna telefonnätet (PSTN), tjänster inom fasta nät, konventionella telefontjänster (POTS) eller telefonitjänster inom fasta nät.

(36) Trots den breda täckning som föreskrivs i denna förordning bör vid tillämpningen av reglerna om digital operativ motståndskraft beaktas betydande skillnader mellan finansiella entiteter i fråga om deras storlek och allmänna riskprofil. Som en allmän princip bör finansiella entiteter, när de fördelar resurser och kapacitet till genomförandet av IKT-riskhanteringsramen, på lämpligt sätt väga sina IKT-relaterade behov mot sin storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser medan de behöriga myndigheterna bör fortsätta att bedöma och se över tillvägagångssättet för en sådan fördelning.

(37) Leverantörer av kontoinformationstjänster, som avses i artikel 33.1 i direktiv (EU) 2015/2366, omfattas uttryckligen av denna förordnings tillämpningsområde, med hänsyn till den specifika arten av deras verksamhet och de risker som den ger upphov till. Dessutom omfattas institut för elektroniska pengar och betalningsinstitut och som är undantagna enligt artikel 9.1 i Europaparlamentets och rådets direktiv 2009/110/EG ([14]) och artikel 32.1 i direktiv (EU) 2015/2366 av tillämpningsområdet för denna förordning även om de inte har beviljats auktorisation i enlighet med direktiv 2009/110/EG att ge ut elektroniska pengar, eller om de inte har auktoriserats i enlighet med direktiv (EU) 2015/2366 att tillhandahålla och genomföra betaltjänster. De postgiroinstitut som avses i artikel 2.5.3 i Europaparlamentets och rådets direktiv 2013/36/EU ([15]) är dock undantagna från denna förordnings tillämpningsområde. Den behöriga myndigheten för betalningsinstitut som är undantagna enligt direktiv (EU) 2015/2366, institut för elektroniska pengar som är undantagna enligt direktiv 2009/110/EG och leverantörer av kontoinformationstjänster som avses i artikel 33.1 i direktiv (EU) 2015/2366, bör vara den behöriga myndighet som utsetts i enlighet med artikel 22 i direktiv (EU) 2015/2366.

(38) Eftersom större finansiella entiteter skulle kunna ha mer omfattande resurser och snabbt kan använda medel för att utveckla styrningsstrukturer och inrätta olika företagsstrategier, bör endast finansiella entiteter som inte är mikroföretag i den mening som avses i denna förordning vara skyldiga att inrätta mer komplexa styrformer. Framför allt är sådana entiteter 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 inrätta en intern riskhanterings- och kontrollmodell och låta sin IKT-riskhanteringsram undergå interna revisioner.

(39) Vissa finansiella entiteter är undantagna från eller omfattas av ett mycket begränsat regelverk enligt relevant sektorsspecifik unionsrätt. Sådana finansiella entiteter omfattar förvaltare av alternativa investeringsfonder som avses i artikel 3.2 i Europaparlamentets och rådets direktiv 2011/61/EU ([16]), försäkrings- och återförsäkringsföretag som avses i artikel 4 i Europaparlamentets och rådets direktiv 2009/138/EG ([17]) samt tjänstepensionsinstitut som förvaltar pensionsplaner som tillsammans inte har fler än totalt 15 medlemmar. Mot bakgrund av dessa undantag

([14]) 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).

([15]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

([16]) Europaparlamentets och rådets direktiv 2011/61/EU av den 8 juni 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv 2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010 (EUT L 174, 1.7.2011, s. 1).

([17]) Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1).

skulle det inte vara proportionellt att inkludera sådana finansiella entiteter i denna förordnings tillämpningsområde. Denna förordning erkänner dessutom försäkringsförmedlingsmarknadens särdrag, vilket innebär att försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet och som räknas som mikroföretag eller som små eller medelstora företag inte bör omfattas av denna förordning.

(40) Eftersom de entiteter som avses i artikel 2.5.4–2.5.23 i direktiv 2013/36/EU är undantagna från det direktivets tillämpningsområde bör medlemsstaterna därför kunna välja att från denna förordning undanta sådana institut som är belägna inom deras respektive territorier.

(41) För att anpassa denna förordning till tillämpningsområdet för Europaparlamentets och rådets direktiv 2014/65/EU ([18]) är det också lämpligt att från denna förordnings tillämpningsområde utesluta de fysiska och juridiska personer som avses i artiklarna 2 och 3 i det direktivet och som får tillhandahålla investeringstjänster utan att behöva erhålla auktorisation enligt direktiv 2014/65/EU. Dock utesluts även enligt artikel 2 i direktiv 2014/65/EU från tillämpningsområdet för det direktivet entiteter som räknas som finansiella entiteter enligt denna förordning, till exempel värdepapperscentraler, företag för kollektiva investeringar eller försäkrings- och återförsäkringsföretag. Uteslutningen från denna förordnings tillämpningsområde för personer och entiteter som avses i artiklarna 2 och 3 i det direktivet bör inte omfatta dessa värdepapperscentraler, företag för kollektiva investeringar eller försäkrings- och återförsäkringsföretag.

(42) Enligt sektorsspecifik unionsrätt omfattas vissa finansiella entiteter av förenklade krav eller undantag av skäl som rör deras storlek eller de tjänster de tillhandahåller. Den kategorin av finansiella entiteter omfattar små och icke sammanlänkade värdepappersföretag, små tjänstepensionsinstitut som får uteslutas från tillämpningsområdet för direktiv (EU) 2016/2341 enligt de villkor som fastställs i artikel 5 i det direktivet av den berörda medlemsstaten och som har pensionsplaner som tillsammans inte omfattar fler än 100 personer totalt, liksom institut som är undantagna enligt direktiv 2013/36/EU. Det är därför lämpligt att, i enlighet med proportionalitetsprincipen och för att bevara andan av sektorsspecifik unionsrätt, låta de finansiella entiteterna omfattas av en förenklad IKT-riskhanteringsram enligt denna förordning. Den proportionella karaktären i den förenklade IKT-riskhanteringsram som omfattar dessa finansiella entiteter bör inte ändras av de lagstadgade tekniska standarder som ska utarbetas av de europeiska tillsynsmyndigheterna. I enlighet med proportionalitetsprincipen är det dessutom lämpligt att även låta de betalningsinstitut som avses i artikel 32.1 i direktiv (EU) 2015/2366 och de institut för elektroniska pengar som avses i artikel 9 i direktiv 2009/110/EG som är undantagna i enlighet med nationellt rätt som införlivar dessa unionsrättsakter omfattas av en förenklad IKT-riskhanteringsram enligt denna förordning, medan betalningsinstitut och institut för elektroniska pengar som inte har undantagits i enlighet med respektive nationell rätt som införlivar sektorsspecifik unionsrätt bör följa den allmänna ram som fastställs i denna förordning.

(43) På samma sätt bör finansiella entiteter som räknas som mikroföretag eller som omfattas av den förenklade IKT-riskhanteringsramen enligt denna förordning inte vara skyldiga att inrätta en funktion för att övervaka de arrangemang som de ingått med IKT-tredjepartsleverantörer för användning av IKT-tjänster; eller att utse en medlem av den högre ledningen till ansvarig för att övervaka den åtföljande riskexponeringen och relevant dokumentation; att överföra ansvaret för att hantera och övervaka IKT-risk till en kontrollfunktion och säkerställa en lämplig nivå av oberoende för den kontrollfunktionen för att undvika intressekonflikter; att minst en gång om året dokumentera och se över IKT-riskhanteringsramen; att regelbundet låta IKT-riskhanteringsramen undergå en internrevision; att göra djupgående bedömningar efter större förändringar i deras infrastruktur och processer för nätverks- och informationssystem; att regelbundet genomföra riskanalyser av befintliga IKT-system; att låta genomförandet av åtgärds- och återställningsplaner avseende IKT undergå oberoende interna granskningar; att inrätta en krishanteringsfunktion, att utöka testningen av driftskontinuitet och åtgärds- och återställningsplaner för att fånga upp överflyttningsscenarier mellan primär IKT-infrastruktur och reservanläggningar, att på begäran av de behöriga myndigheterna lämna en uppskattning av de totala årliga kostnader och förluster som orsakas av allvarliga IKT-relaterade incidenter, att upprätthålla IKT-reservkapacitet; att till de nationella behöriga myndigheterna meddela

([18]) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

vilka förändringar som genomfördes efter efterhandsöversyner av IKT-relaterade incidenter; att kontinuerligt övervaka relevant teknisk utveckling, att inrätta ett heltäckande program för testning av digital operativ motståndskraft som en integrerad del av den IKT-riskhanteringsram som föreskrivs i den här förordningen, eller att anta och regelbundet se över en strategi för IKT-tredjepartsrisk. Mikroföretag ska dessutom endast bedöma behovet av att upprätthålla sådan IKT-reservkapacitet med utgångspunkt i vilken riskprofil de har. Mikroföretag bör omfattas av ett mer flexibelt system vad gäller program för testning av digital operativ motståndskraft. När de överväger vilken typ och frekvens av testning som ska utföras bör de vederbörligen väga målet att upprätthålla en hög digital operativ motståndskraft, de tillgängliga resurserna och sin allmänna riskprofil. Mikroföretag och finansiella entiteter som omfattas av den förenklade IKT-riskhanteringsramen enligt denna förordning bör undantas från kravet på avancerad testning av IKT-verktyg, IKT-system och IKT-processer baserad på hotbildsstyrd penetrationstestning, eftersom endast finansiella entiteter som uppfyller de krav som fastställs i denna förordning bör vara skyldiga att utföra sådan testning. Mot bakgrund av sin begränsade kapacitet bör mikroföretag kunna komma överens med tredjepartsleverantören av IKT-tjänster att delegera den finansiella entiteten rätt till tillgång, inspektion och revision till en oberoende tredje part som utsetts av tredjepartsleverantören av IKT-tjänster, under förutsättning att den finansiella entiteten, när som helst, kan begära all relevant information och försäkran om tredjepartsleverantörens prestanda från respektive oberoende tredje part.

(44) Eftersom endast de finansiella entiteter som har identifierats vid tillämpning av avancerad testning av digital motståndskraft bör vara skyldiga att utföra hotbildsstyrda penetrationstester, bör dessutom de administrativa processer och finansiella kostnader som genomförandet av sådana tester medför överföras till en liten andel av finansiella entiteter.

(45) För att säkerställa fullständig anpassning och övergripande konsekvens mellan finansiella entiteters affärsstrategier, å ena sidan, och genomförandet av IKT-riskhantering, å andra sidan, bör finansiella entiteters ledningsorgan vara skyldiga att ha en central och aktiv roll i styrningen och anpassningen av IKT-riskhanteringsramen och den övergripande strategin för digital operativ motståndskraft. Ledningsorganens 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 cyberrisker och ett åtagande att tillämpa en strikt cyberhygien på alla nivåer. Ledningsorganets yttersta ansvar för att hantera en finansiell entitets IKT-risk bör utgöra en övergripande princip för den heltäckande strategin och omsättas i ett fortlöpande engagemang hos ledningen för att kontrollera övervakningen av IKT-riskhanteringen.

(46) Principen om ledningsorganets fullständiga och slutgiltiga ansvar för hanteringen av IKT-risken för en finansiell entitet går hand i hand med behovet av att säkerställa en nivå för IKT-relaterade investeringar och en övergripande budget för den finansiella entiteten som skulle möjliggöra för den finansiella entiteten att uppnå en hög nivå av digital operativ motståndskraft.

(47) Med inspiration från relevanta internationella, nationella och branschspecifika bästa praxis, riktlinjer, rekommendationer och strategier för hantering av cyberrisker, förordas i denna förordning en uppsättning principer som underlättar den övergripande strukturering av IKT-riskhanteringen. Så länge finansiella entiteters huvudsakliga kapacitet uppfyller de olika funktionerna för IKT-riskhantering (identifiering, skydd och förebyggande, upptäckt, åtgärd och återställning, lärande och utveckling samt kommunikation) som anges i denna förordning, bör det följaktligen stå finansiella entiteter fritt att använda IKT-riskhanteringsmodeller som utformas eller kategoriseras på olika sätt.

(48) För att hålla jämna steg med den föränderliga cyberhotbilden bör finansiella entiteter upprätthålla uppdaterade IKT-system som är tillförlitliga och har kapacitet, inte bara för att garantera den behandling av data som krävs för deras tjänster, utan också för att säkerställa tillräcklig teknisk motståndskraft som gör det möjligt för dem att på ett adekvat sätt hantera ytterligare databehandlingsbehov på grund av stressade marknadsförhållanden eller andra ogynnsamma situationer.

(49) Effektiva kontinuitets- och återställningsplaner krävs för att finansiella entiteter snabbt ska kunna åtgärda IKT-relaterade incidenter, särskilt cyberangrepp, genom att begränsa skador och prioritera återupptagande av verksamhet och återställningsåtgärder i enlighet med sina beredskapsplaner. Ett sådant återupptagande bör dock inte på något sätt äventyra integriteten och säkerheten i nätverks- eller informationssystemen eller uppgifternas tillgänglighet, äkthet, integritet eller konfidentialitet.

(50) Denna förordning innebär att finansiella entiteter kan fastställa sina mål för återställningstid och återskapandepunkt på ett flexibelt sätt och därvid fullt ut ta hänsyn till den berörda funktionens egenskaper och kritikalitet och till eventuella särskilda verksamhetsbehov, men det bör också krävas att de gör en bedömning av den eventuella övergripande inverkan på marknadseffektiviteten när sådana mål fastställs.

(51) Spridare av cyberangrepp tenderar att eftersträva ekonomisk vinning direkt vid källan, vilket utsätter finansiella entiteter för betydande konsekvenser. I syfte att förhindra att IKT-system förlorar integritet eller blir otillgängliga, och därmed undvika dataintrång och skador för den fysiska IKT-infrastrukturen, bör finansiella entiteters rapportering av allvarliga IKT-relaterade incidenter avsevärt förbättras och förenklas. IKT-relaterad incidentrapportering bör harmoniseras genom införande av ett krav för alla finansiella entiteter att rapportera direkt till sina berörda behöriga myndigheter. Om en finansiell entitet är föremål för tillsyn av mer än en nationell behörig myndighet bör medlemsstaterna utse en enda behörig myndighet som mottagare av sådan rapportering. Kreditinstitut som klassificerats som betydande i enlighet med artikel 6.4 i rådets förordning (EU) nr 1024/2013 ([19]) bör förelägga de nationella behöriga myndigheterna sådan rapportering, och dessa bör därefter översända rapporten till Europeiska centralbanken (ECB).

(52) Direkt rapportering bör göra det möjligt för finansiella tillsynsmyndigheter att få omedelbar tillgång till information om allvarliga IKT-relaterade incidenter. Finansiella tillsynsmyndigheter bör i sin tur vidarebefordra närmare detaljer om allvarliga IKT-relaterade incidenter till offentliga icke-finansiella myndigheter (t.ex. behöriga myndigheter och gemensamma kontaktpunkter enligt direktiv (EU) 2022/2555, nationella dataskyddsmyndigheter och brottsbekämpande myndigheter för allvarliga IKT-relaterade incidenter av brottslig karaktär) för att öka dessa myndigheters medvetenhet om sådana incidenter, och vad gäller CSIRT-enheter, för att underlätta snabbt stöd som kan ges till finansiella entiteter när så är lämpligt. Dessutom bör medlemsstaterna kunna avgöra huruvida finansiella entiteter själva bör tillhandahålla sådan information till offentliga myndigheter utanför området för finansiella tjänster. Dessa informationsflöden bör göra det möjligt för finansiella entiteter att snabbt dra fördel av relevanta tekniska uppgifter, råd om åtgärder och uppföljning från sådana myndigheter. Informationen om allvarliga IKT-relaterade incidenter bör förmedlas ömsesidigt: de finansiella tillsynsmyndigheterna bör ge all nödvändig återkoppling eller vägledning till den finansiella entiteten, medan de europeiska tillsynsmyndigheterna bör dela anonymiserade uppgifter om cyberhot och sårbarheter i samband med en incident, till stöd för ett bredare kollektivt försvar.

(53) Även om det bör krävas att alla finansiella entiteter rapporterar incidenter förväntas inte det kravet påverka dem alla på samma sätt. Relevanta väsentlighetströsklar och rapporteringsfrister bör vederbörligen anpassas, inom ramen för delegerade akter grundade på tekniska standarder för tillsyn som utarbetas av de europeiska tillsynsmyndigheterna, med syftet att endast omfatta allvarliga IKT-relaterade incidenter. Dessutom bör finansiella entiteters särdrag beaktas när fristerna för rapporteringsskyldigheter fastställs.

(54) Denna förordning bör innehålla krav på att kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar rapporterar alla betalningsrelaterade operativa incidenter eller säkerhetsincidenter – som tidigare rapporterades enligt direktiv (EU) 2015/2366 – oavsett om incidenten är IKT-relaterad eller inte.

([19]) 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).

(55) De europeiska tillsynsmyndigheterna bör få i uppdrag att bedöma genomförbarheten av och villkoren för en eventuell centralisering av IKT-relaterade incidentrapporter på unionsnivå. Sådan centralisering kan bestå av en gemensam EU-knutpunkt för rapportering av allvarliga IKT-relaterade incidenter, som antingen direkt tar emot relevanta rapporter och automatiskt underrättar nationella behöriga myndigheter, eller som enbart centraliserar relevanta rapporter från de nationella behöriga myndigheterna och därmed fyller en samordnande funktion. De europeiska tillsynsmyndigheterna bör få i uppdrag att i samråd med ECB och Enisa utarbeta en gemensam rapport om möjligheten att inrätta en gemensam EU-knutpunkt.

(56) För att uppnå en hög nivå av digital operativ motståndskraft, och i linje med både relevanta internationella standarder (t.ex. G7-gruppens Fundamental Elements for Threat-Led Penetration Testing), och med de ramar som tillämpas inom unionen, till exempel TIBER-EU bör finansiella entiteter regelbundet testa sina IKT-system och sin personal med IKT-ansvar med avseende på hur effektiv deras kapacitet är för förebyggande, upptäckt, åtgärd och återställning, för att upptäcka och åtgärda potentiella IKT-sårbarheter. För att återspegla de skillnader som finns mellan och inom de olika finansiella undersektorerna vad gäller nivån på finansiella entiteters 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 för skanning, källkodsgranskningar när så är möjligt, scenariobaserade tester, kompatibilitetstester, prestandatester eller tester ändpunkt till ändpunkt (*end-to-end*)) till mer avancerade tester genom hotbildsstyrd penetrationstestning. Sådana avancerade tester bör krävas endast av finansiella entiteter som är tillräckligt mogna ur ett IKT-perspektiv för att utföra dem på ett rimligt sätt. Den testning av den digitala operativa motståndskraften som krävs enligt denna förordning bör därför vara mer krävande för de finansiella entiteterna som uppfyller de krav som fastställs i denna förordning (t.ex. stora, systematiska och IKT-mogna kreditinstitut, fondbörser, värdepapperscentraler och centrala motparter) än för andra finansiella entiteter. Samtidigt bör testning av digital operativ motståndskraft genom hotbildsstyrd penetrationstestning vara mer relevant för finansiella entiteter som är verksamma inom delsektorer för centrala finansiella tjänster och som har en central betydelse för systemet (t.ex. betalningar, bankverksamhet, och clearing och avveckling) och mindre relevant för andra delsektorer (t.ex. kapitalförvaltare och kreditvärderingsinstitut).

(57) Finansiella entiteter som bedriver gränsöverskridande verksamhet och som utövar friheten att etablera sig eller tillhandahålla tjänster inom unionen bör uppfylla en enda uppsättning avancerade testkrav (t.ex. hotbildsstyrd penetrationstestning) i sin hemmedlemsstat, vilka bör omfatta IKT-infrastrukturerna i alla jurisdiktioner i unionen där den gränsöverskridande finansiella koncernen bedriver verksamhet, vilket innebär att relaterade IKT-testningskostnader uppstår i endast en jurisdiktion för sådana gränsöverskridande finansiella koncerner.

(58) För att dra nytta av den expertis som redan förvärvats av vissa behöriga myndigheter, särskilt med avseende på genomförandet av TIBER-EU-ramen, bör denna förordning ge medlemsstaterna möjligheten att utse en enda offentlig myndighet med ansvar för den finansiella sektorn, på nationell nivå, för alla frågor som rör hotbildsstyrd penetrationstestning eller, om ingen sådan myndighet utsetts, för behöriga myndigheter att delegera uppgifter som rör hotbildsstyrd penetrationstestning till en annan nationell finansiell behörig myndighet.

(59) Eftersom denna förordning inte kräver att finansiella entiteter täcker alla kritiska eller viktiga funktioner i en enda hotbildsstyrd penetrationstestning, bör finansiella entiteter vara fria att avgöra vilka och hur många kritiska eller viktiga funktioner som bör omfattas av ett sådant test.

(60) Gemensam testning i den mening som avses i denna förordning – som inbegriper deltagande av flera finansiella entiteter i en hotbildsstyrd penetrationstestning och för vilken en tredjepartsleverantör av IKT-tjänster direkt kan ingå kontraktsmässiga arrangemang med en extern testare – bör endast tillåtas om kvaliteten eller säkerheten för de tjänster som utförs av tredjepartsleverantören av IKT-tjänster åt kunder som är entiteter utanför denna förordnings tillämpningsområde, eller för konfidentialiteten för data som är relaterade till sådana tjänster, rimligen kan förväntas påverkas negativt, gemensam testning bör också omfattas av skyddsåtgärder (under ledning av en utsedd finansiell entitet, med kalibrering av antalet deltagande finansiella entiteter) för att för de berörda finansiella entiteterna säkerställa ett strikt testutförande som uppfyller målen för den hotbildsstyrda penetrationstestningen enligt denna förordning.

(61) För att dra fördel av de interna resurser som är tillgängliga på företagsnivå, bör denna förordning tillåta användningen av interna testare i syfte att utföra hotbildsstyrd penetrationstestning, under förutsättning att tillsynsmyndigheten godkänner det, att inga intressekonflikter föreligger och att användningen av interna och externa testare alternerar periodiskt (vart tredje test), och samtidigt kräver att den som tillhandahåller underrättelser om hot för den hotbildsstyrda penetrationstestningen alltid är extern i förhållande till den finansiella entiteten. Ansvaret för att genomföra hotbildsstyrd penetrationstestning bör till fullo ligga kvar hos den finansiella entiteten. Intyg från myndigheterna bör användas enbart för ömsesidigt erkännande och bör inte utesluta några uppföljningsåtgärder som krävs för att hantera den IKT-risk som den finansiella entiteten är utsatt för, och inte heller betraktas som tillsynsmyndighetens godkännande av den finansiella entitetens kapacitet att hantera och begränsa IKT-risk.

(62) För att säkerställa en sund övervakning av IKT-tredjepartsrisk i den finansiella sektorn är det nödvändigt att fastställa en uppsättning principbaserade regler för att vägleda finansiella entiteter vid övervakning av risker som uppstår i samband med funktioner som utkontrakterats till tredjepartsleverantörer av IKT-tjänster, särskilt för IKT-tjänster som stöder kritiska eller viktiga funktioner, liksom mer allmänt inom ramen för alla IKT-tredjepartsberoenden.

(63) För att hantera komplexiteten i de olika källorna till IKT-risk, och samtidigt ta hänsyn till den mångfald av leverantörer av tekniska lösningar som möjliggör ett smidigt tillhandahållande av finansiella tjänster, bör denna förordning omfatta många olika tredjepartsleverantörer av IKT-tjänster, inbegripet leverantörer av molntjänster, programvara, dataanalystjänster och leverantörer av datacentraltjänster. Eftersom finansiella entiteter effektivt och konsekvent bör identifiera och hantera alla typer av risker, inbegripet i samband med IKT-tjänster som tillhandahålls inom en finansiell koncern, bör det på samma sätt klargöras att företag som ingår i en finansiell koncern och som tillhandahåller IKT-tjänster främst till sitt moderföretag, eller till dess dotterbolag eller filialer, liksom finansiella entiteter som tillhandahåller IKT-tjänster till andra finansiella entiteter, också bör betraktas som tredjepartsleverantörer av IKT-tjänster enligt denna förordning. Slutligen bör, mot bakgrund av att marknaden för betaltjänster blir mer och mer beroende av komplexa tekniska lösningar, och med beaktande av framväxande typer av betaltjänster och betalningsrelaterade lösningar, deltagare i ekosystemet för betaltjänster som tillhandahåller betalningshanteringstjänster, eller som driver betalningsinfrastrukturer, också anses som tredjepartsleverantörer av IKT-tjänster enligt denna förordning, med undantag för centralbankers hantering av betalningssystem eller system för värdepappersavveckling, samt offentliga myndigheters tillhandahållande av IKT-relaterade tjänster vid uppfyllandet av statliga funktioner.

(64) En finansiell entitet bör alltid ha det fulla ansvaret för att uppfylla sina skyldigheter enligt denna förordning. Finansiella entiteter bör tillämpa ett proportionellt tillvägagångssätt vid övervakningen av de risker som uppstår hos tredjepartsleverantörer av IKT-tjänster, genom att vederbörlig hänsyn tas till karaktären på och omfattningen av, komplexiteten hos och betydelsen av sina IKT-relaterade beroenden, kritikaliteten hos eller betydelsen av de tjänster, processer eller funktioner som omfattas av de kontraktsmässiga arrangemangen och, i förlängningen, på grundval av en noggrann bedömning av eventuella effekter på kontinuiteten och kvaliteten hos finansiella tjänster på individuell nivå och koncernnivå, beroende på vad som är lämpligt.

(65) Denna övervakning bör följa ett strategiskt tillvägagångssätt för IKT-tredjepartsrisker som inrättas formellt genom att den finansiella entitetens ledningsorgan antar en särskild strategi för IKT-tredjepartsrisker som bygger på en kontinuerlig granskning av alla beroenden av IKT-tredjeparter. För att öka tillsynsmyndigheternas medvetenhet om beroenden av IKT-tredjeparter och ytterligare stödja arbetet i samband med den tillsynsram som inrättas genom denna förordning, bör alla finansiella entiteter ha skyldighet att upprätthålla ett informationsregister med alla kontraktsmässiga arrangemang som rör användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster. Finansiella tillsynsmyndigheter bör kunna begära tillgång till hela registret eller be om särskilda avsnitt av registret, och därigenom få viktig information för en bredare förståelse av finansiella entiteters IKT-relaterade beroenden.

(66) En grundlig förhandsanalys bör underbygga och föregå formellt ingående av kontraktsmässiga arrangemang, särskilt genom fokusering på inslag som kritikalitet eller betydelse av de tjänster som understöds av det planerade IKT-kontraktet, nödvändiga godkännanden från tillsynsmyndigheter eller andra villkor, den eventuella koncentrationsrisk som detta medför, liksom due diligence-granskning i förfarandet för urval och bedömning av tredjepartsleverantörer av IKT-tjänster och bedömning av potentiella intressekonflikter. Vad gäller kontraktsmässiga arrangemang rörande kritiska eller viktiga funktioner bör finansiella entiteter beakta tredjepartsleverantörer av IKT-tjänsters användning av de senaste och högsta standarderna för informationssäkerhet. Uppsägning av kontraktsmässiga arrangemang kan föranledas av åtminstone ett antal omständigheter som visar på brister hos tredjepartsleverantören av IKT-tjänster,

särskilt betydande överträdelser av lagar eller avtalsvillkor, omständigheter som påvisar en potentiell förändring av prestandan i de funktioner som avses i de kontraktsmässiga arrangemangen, bevis på svagheter hos tredjepartsleverantören av IKT-tjänster i den övergripande hanteringen av IKT-risk, eller omständigheter som tyder på att den berörda behöriga myndigheten inte har förmåga att effektivt övervaka den finansiella entiteten.

(67) För att hantera systemeffekterna av koncentrationsrisken för IKT-tredjeparter främjar denna förordning en balanserad lösning genom en flexibel och gradvis strategi för sådana koncentrationsrisker, eftersom införandet av strikta tak eller strikta begränsningar kan hindra företagens affärsverksamhet och begränsa avtalsfriheten. Finansiella entiteter bör göra en grundlig bedömning av sina planerade kontraktsmässiga arrangemang för att fastställa sannolikheten för att en sådan risk uppstår, bland annat genom djupgående analyser av underleverantörsavtal, 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 regler för strikta tak och gränser för exponeringar mot IKT-tredjeparter. I samband med översynsramen bör en ledande tillsynsmyndighet, som utsetts enligt denna förordning, med avseende på kritiska tredjepartsleverantörer av IKT-tjänster ägna särskild uppmärksamhet åt att fullt ut förstå omfattningen av ömsesidiga beroenden, 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 specifika risk har identifierats.

(68) För att regelbundet utvärdera och övervaka förmågan hos en tredjepartsleverantör av IKT-tjänster att säkert tillhandahålla tjänster till en finansiell entitet utan negativa effekter på den finansiella entitetens digitala operativa motståndskraft, bör flera centrala avtalsdelar med tredjepartsleverantörer av IKT-tjänster harmoniseras. En sådan harmonisering bör omfatta åtminstone de områden som är avgörande för att den finansiella entiteten ska kunna bedriva en fullständig övervakning av de risker som kan uppstå genom tredjepartsleverantören av IKT-tjänster, utifrån en finansiell entitets behov av att säkerställa sin digitala motståndskraft eftersom den är beroende av stabiliteten, funktionaliteten, tillgängligheten och säkerheten hos de IKT-tjänster som den använder.

(69) När de omförhandlar kontraktsmässiga arrangemang för att anpassa sig till kraven i denna förordning bör finansiella entiteter och tredjepartsleverantören av IKT-tjänster säkerställa att de viktiga avtalsbestämmelser som anges i denna förordning omfattas.

(70) Den definition av *kritisk eller viktig funktion* som anges i denna förordning omfattar de *kritiska funktioner* som anges i artikel 2.1.35 i Europaparlamentets och rådets direktiv 2014/59/EU ([20]). I enlighet med detta är de funktioner som anses vara kritiska enligt direktiv 2014/59/EU inbegripna i definitionen av kritiska funktioner i den mening som avses i denna förordning.

(71) Oavsett kritikaliteten hos eller betydelsen av den funktion som stöds av IKT-tjänsterna bör kontraktsmässiga arrangemang särskilt innehålla en specifikation med heltäckande beskrivningar av funktioner och tjänster, platser där sådana funktioner tillhandahålls och där uppgifterna kommer att behandlas, samt beskrivningar av servicenivån. Andra grundläggande delar för att möjliggöra en finansiell entitets övervakning av IKT-tredjepartsrisker är: avtalsbestämmelser som anger hur åtkomst, tillgänglighet, integritet, säkerhet och skydd av personuppgifter säkerställs av tredjepartsleverantören av IKT-tjänster, bestämmelser som fastställer relevanta garantier för att säkerställa åtkomst, återvinning och återlämnande av uppgifter vid insolvens, resolution eller nedläggning av affärsverksamheten hos tredjepartsleverantören av IKT-tjänster samt bestämmelser som kräver att tredjepartsleverantören av IKT-tjänster ger stöd vid IKT-incidenter i samband med de tjänster som tillhandahålls,

([20]) Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag och om ändring av rådets direktiv 82/891/EEG och Europaparlamentets och rådets direktiv 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU och 2013/36/EU samt Europaparlamentets och rådets förordningar (EU) nr 1093/2010 och (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 190).

utan ytterligare kostnad eller till en kostnad som fastställts på förhand, bestämmelser om skyldigheten för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut med de behöriga myndigheterna och resolutionsmyndigheterna för den finansiella entiteten, samt bestämmelser om uppsägningsrätt och tillhörande minsta uppsägningstid för kontraktsmässiga arrangemang, i enlighet med de behöriga myndigheternas och resolutionsmyndigheternas förväntningar.

(72) Utöver sådana avtalsbestämmelser, och i syfte att säkerställa att finansiella entiteter behåller full kontroll över all utveckling som sker på tredjepartsnivå och som kan försämra deras IKT-säkerhet, bör avtalen om tillhandahållande av IKT-tjänster som stöder kritiska eller viktiga funktioner också innehålla bestämmelser om fullständiga beskrivningar av servicenivån, med exakta kvantitativa och kvalitativa prestationsmål, för att utan onödigt dröjsmål möjliggöra lämpliga korrigerande åtgärder om de överenskomna servicenivåerna inte uppnås, relevanta tidsfrister för anmälan och rapporteringsskyldigheter för tredjepartsleverantören av IKT-tjänster för händelser som kan ha en väsentlig inverkan på tredjepartsleverantörens förmåga att effektivt tillhandahålla respektive IKT-tjänster, ett krav på att tredjepartsleverantören av IKT-tjänster ska genomföra och testa beredskapsplaner för verksamheten och införa IKT-säkerhetsåtgärder, IKT-verktyg och IKT-strategier som möjliggör ett säkert tillhandahållande av tjänster, samt delta och samarbeta fullt ut i den hotbildsstyrda penetrationstestningen som utförs av den finansiella entiteten.

(73) Avtalen om tillhandahållande av IKT-tjänster som stöder kritiska eller viktiga funktioner bör också innehålla bestämmelser om den finansiella entitetens eller en utsedd tredjeparts rätt till åtkomst, inspektion och revision samt rätten att ta kopior som avgörande verktyg i finansiella entiteters fortlöpande övervakning av IKT-tredjepartsleverantörens prestanda, i kombination med att den sistnämnda samarbetar fullt ut under inspektionerna. På samma sätt bör den finansiella entitetens behöriga myndighet ha rätt att, på grundval av anmälningar, kontrollera och granska tredjepartsleverantören av IKT-tjänster, med förbehåll för sekretesskrav.

(74) Sådana kontraktsmässiga arrangemang bör också innehålla särskilda exitstrategier som i synnerhet möjliggör obligatoriska övergångsperioder under vilka tredjepartsleverantörer av IKT-tjänster bör fortsätta att tillhandahålla relevanta tjänster för att minska risken för avbrott på finansiell enhetsnivå eller göra det möjligt för den finansiella entiteten att på ett effektivt sätt byta till andra tredjepartsleverantörer av IKT-tjänster, eller byta till interna lösningar som är förenliga med den tillhandahållna IKT- tjänstens komplexitet. Dessutom bör finansiella entiteter som omfattas av direktiv 2014/59/EU säkerställa att relevanta avtal för IKT-tjänster är solida och kan hävdas i händelse av resolution av finansiella entiteter. I linje med resolutionsmyndigheternas förväntningar bör dessa finansiella entiteter därför säkerställa att relevanta avtal för IKT-tjänster är motståndskraftiga mot resolution. Så länge de fortsätter att uppfylla sina betalningsskyldigheter bör dessa finansiella entiteter bland annat säkerställa att relevanta avtal för IKT-tjänster innehåller klausuler om att de inte får sägas upp, inte får upphävas tillfälligt och inte ändras på grund av omstrukturering eller resolution.

(75) Dessutom kan frivillig användning av standardavtalsklausuler som offentliga myndigheter eller unionens institutioner har utarbetat, särskilt användningen av avtalsklausuler som kommissionen har utarbetat för molntjänster, underlätta ytterligare för finansiella entiteter och tredjepartsleverantörer av IKT-tjänster genom att öka rättssäkerheten avseende den finansiella sektorns användning av molntjänster, i fullständig överensstämmelse med de krav och förväntningar som fastställs i unionsrätten avseende finansiella tjänster. Utarbetandet av standardavtalsklausuler bygger på åtgärder som planerades redan i 2018 års handlingsplan för fintech, där kommissionen tillkännagav sin avsikt att uppmuntra och underlätta utarbetandet av standardavtalsklausuler för finansiella entiteters utkontraktering till molntjänster, genom att bygga på de branschöverskridande ansträngningar från molntjänstintressenternas sida som kommissionen redan har bidragit till med den finansiella sektorns medverkan.

(76) I syfte att främja konvergens och effektivitet när det gäller tillsynsstrategier för IKT-tredjepartsrisker i den finansiella sektorn, och för att stärka den digitala operativa motståndskraften hos finansiella entiteter som är beroende av kritiska tredjepartsleverantörer av IKT-tjänster för att tillhandahålla IKT-tjänster som stöder tillhandahållandet av finansiella tjänster, och därmed bidra till att bevara stabiliteten i unionens finansiella system och integriteten på den inre marknaden för finansiella tjänster, bör kritiska tredjepartsleverantörer av IKT-tjänster omfattas av en tillsynsram på unionsnivå. Inrättandet av tillsynsramen motiveras av mervärdet av att vidta åtgärder på unionsnivå

och av särdragen hos användningen av IKT-tjänster och den roll de spelar vid tillhandahållandet av finansiella tjänster, men det bör samtidigt erinras om att denna lösning endast förefaller vara lämplig inom ramen för denna förordning, som specifikt behandlar digital operativ motståndskraft inom finanssektorn. En sådan tillsynsram bör dock inte betraktas som en ny modell för unionstillsyn på andra områden av finansiella tjänster och finansiell verksamhet.

(77) Tillsynsramen bör endast tillämpas på kritiska tredjepartsleverantörer av IKT-tjänster. Det bör därför inrättas en klassificeringsmekanism för att ta hänsyn till omfattningen och arten av den finansiella sektorns beroende av sådana tredjepartsleverantörer av IKT-tjänster. Den mekanismen bör inbegripa en uppsättning kvantitativa och kvalitativa kriterier för att fastställa kritikalitetsparametrarna som en grund för inkludering i tillsynsramen. För att säkerställa att den bedömningen är korrekt, och oavsett företagsstrukturen hos tredjepartsleverantören av IKT-tjänster, bör sådana kriterier, när det gäller en tredjepartsleverantör av IKT-tjänster som ingår i en större koncern, beakta hela koncernstrukturen hos tredjepartsleverantören av IKT-tjänster. Å ena sidan bör kritiska tredjepartsleverantörer av IKT-tjänster som inte automatiskt utses genom tillämpning av dessa kriterier ha möjlighet att på frivillig basis delta i tillsynsramen, å andra sidan bör de tredjepartsleverantörer av IKT-tjänster som redan omfattas av tillsynsramar för fullgörandet av Europeiska centralbankssystemet uppgifter enligt artikel 127.2 i EUF-fördraget undantas.

(78) På samma sätt bör finansiella entiteter som tillhandahåller IKT-tjänster till andra finansiella entiteter, även om de tillhör kategorin tredjepartsleverantörer av IKT-tjänster enligt denna förordning, också undantas från tillsynsramen eftersom de redan omfattas av tillsynsmekanismer som inrättats genom relevant unionsrätt avseende finansiella tjänster. I tillämpliga fall bör de behöriga myndigheterna inom ramen för sin tillsynsverksamhet beakta den IKT-risk som finansiella entiteter som tillhandahåller IKT-tjänster utgör för finansiella entiteter. På samma sätt bör, på grund av de befintliga riskövervakningsmekanismerna på koncernnivå, samma undantag införas för tredjepartsleverantörer av IKT-tjänster som huvudsakligen tillhandahåller tjänster till entiteter i den egna koncernen. Tredjepartsleverantörer av IKT-tjänster som endast tillhandahåller IKT-tjänster i en medlemsstat till finansiella entiteter som endast är verksamma i den medlemsstaten bör också undantas från klassificeringsmekanismen på grund av sin begränsade verksamhet och avsaknad av gränsöverskridande inverkan.

(79) Digitaliseringen av finansiella tjänster har lett till en användning och ett beroende av IKT-tjänster som aldrig tidigare skådats. Eftersom det har blivit otänkbart att tillhandahålla finansiella tjänster utan användning av molntjänster, programvarulösningar och datarelaterade tjänster, har unionens finansiella ekosystem i sig blivit beroende av vissa IKT-tjänster som tillhandahålls av leverantörer av IKT-tjänster. Vissa av dessa leverantörer är innovatörer när det gäller att utveckla och tillämpa IKT-baserad teknik, och spelar en viktig roll i tillhandahållandet av finansiella tjänster eller har integrerats i värdekedjan för finansiella tjänster. De har därför blivit kritiska för stabiliteten och integriteten i unionens finansiella system. Detta utbredda beroende av tjänster som tillhandahålls av kritiska tredjepartsleverantörer av IKT-tjänster, i kombination med det ömsesidiga beroendet mellan olika marknadsoperatörers informationssystem, skapar en direkt och potentiellt allvarlig risk för unionens system för finansiella tjänster och för kontinuiteten i tillhandahållandet av finansiella tjänster, om kritiska tredjepartsleverantörer av IKT-tjänster skulle påverkas av operativa störningar eller allvarliga cyberincidenter. Cyberincidenter har en särskild förmåga att föröka sig och sprida sig i hela det finansiella systemet i en betydligt snabbare takt än andra typer av risker som övervakas inom finanssektorn och kan sträcka sig över sektorer och över geografiska gränser. De har potential att utvecklas till en systemkris där förtroendet för det finansiella systemet har urholkats på grund av störningar i funktioner som stöder realekonomin, eller betydande finansiella förluster som når en nivå som det finansiella systemet inte kan klara, eller som kräver omfattande åtgärder för att absorbera stora chocker. För att förhindra att dessa scenarier inträffar och därmed äventyrar unionens finansiella stabilitet och integritet, är det viktigt att skapa konvergens i tillsynspraxis för IKT-tredjepartsrisker inom finanssektorn, särskilt genom nya regler som möjliggör unionstillsyn av kritiska tredjepartsleverantörer av IKT-tjänster.

(80) Tillsynsramen är till stor del beroende av graden av samarbete mellan den ledande tillsynsmyndigheten och den kritiska tredjepartsleverantör av IKT-tjänster som levererar tjänster till finansiella entiteter som påverkar tillhandahållandet av finansiella tjänster. En framgångsrik tillsyn är beroende av bland annat den ledande tillsynsmyndighetens förmåga att effektivt genomföra övervakningsuppdrag och inspektioner för att bedöma de regler, kontroller och processer som används av kritiska tredjepartsleverantörer av IKT-tjänster, samt bedöma den potentiella kumulativa effekten av deras verksamhet på den finansiella stabiliteten och det finansiella systemets integritet. Samtidigt är det mycket viktigt att kritiska tredjepartsleverantörer av IKT-tjänster följer den ledande tillsynsmyndighetens rekommendationer och åtgärdar dess farhågor. Eftersom bristande samarbete från en kritisk tredjepartsleverantör av IKT-tjänster som tillhandahåller tjänster som påverkar tillhandahållandet av finansiella tjänster, såsom vägran att bevilja tillträde till sina lokaler eller att lämna information, i slutändan skulle beröva den ledande tillsynsmyndigheten dess grundläggande verktyg för att bedöma IKT-tredjepartsrisker och skulle kunna inverka negativt på det finansiella systemets stabilitet och integritet, är det nödvändigt att även föreskriva ett proportionellt sanktionssystem.

(81) Mot denna bakgrund bör den ledande tillsynsmyndighetens behov av att ålägga viten för att tvinga kritiska tredjepartsleverantörer av IKT-tjänster att uppfylla de skyldigheter rörande transparens och tillträde som fastställs i denna förordning inte äventyras av svårigheter som uppstår till följd av verkställandet av dessa viten i förhållande till kritiska tredjepartsleverantörer av IKT-tjänster som är etablerade i tredjeländer. För att säkerställa sådana sanktioners verkställbarhet, och för att möjliggöra ett snabbt införande av förfaranden som upprätthåller de kritiska IKT-tredjepartsleverantörernas rätt till försvar inom ramen för klassificeringsmekanismen och utfärdandet av rekommendationer, bör de kritiska tredjepartsleverantörerna av IKT-tjänster som tillhandahåller tjänster till finansiella entiteter som påverkar tillhandahållandet av finansiella tjänster vara skyldiga att upprätthålla en tillräcklig verksamhet i unionen. På grund av tillsynens karaktär och avsaknaden av jämförbara arrangemang i andra jurisdiktioner finns det inga lämpliga alternativa mekanismer som säkerställer detta mål genom ett effektivt samarbete med finansiella tillsynsmyndigheter i tredjeländer när det gäller övervakningen av effekterna av de digitala operativa risker som systemviktiga tredjepartsleverantörer av IKT-tjänster, vilka räknas som kritiska tredjepartsleverantörer av IKT-tjänster som är etablerade i tredjeländer, utgör. I syfte att fortsätta att tillhandahålla IKT-tjänster till finansiella entiteter i unionen bör därför en tredjepartsleverantör av IKT-tjänster som är etablerad i tredjeländer som klassificerats som kritisk i enlighet med denna förordning vidta, inom tolv månader efter en sådan klassificering, alla nödvändiga arrangemang för att säkerställa dess inkorporering i unionen genom att inrätta en filial, enligt unionens regelverk, närmare bestämt i Europaparlamentets och rådets direktiv 2013/34/EU ([21]).

(82) Kravet på att inrätta ett dotterbolag i unionen bör inte hindra den kritiska tredjepartsleverantören av IKT-tjänster från att tillhandahålla IKT-tjänster och tillhörande teknisk support från anläggningar och infrastruktur utanför unionen. Denna förordning inför inte någon datalokaliseringsplikt eftersom den inte kräver att datalagring eller databehandling ska utföras i unionen.

(83) Kritiska tredjepartsleverantörer av IKT-tjänster bör kunna tillhandahålla IKT-tjänster från vilken plats som helst i världen, och inte nödvändigtvis eller inte bara från lokaler som är belägna i unionen. Tillsynsverksamheten bör först genomföras i lokaler som är belägna i unionen och genom interaktion med entiteter som är belägna i unionen, inbegripet dotterbolag som inrättats av kritiska tredjepartsleverantörer av IKT-tjänster enligt denna förordning. Sådana åtgärder inom unionen kan dock vara otillräckliga för att den ledande tillsynsmyndigheten fullt ut och effektivt ska kunna utföra sina uppgifter enligt denna förordning. Den ledande tillsynsmyndigheten bör därför också kunna utöva sina relevanta tillsynsbefogenheter i tredjeländer. Utövandet av dessa befogenheter i tredjeländer bör göra det möjligt för den ledande tillsynsmyndigheten att undersöka de faciliteter från vilka IKT-tjänsterna eller teknisk supporttjänsterna faktiskt tillhandahålls eller förvaltas av den kritiska tredjepartsleverantören av IKT-tjänster och bör ge den ledande tillsynsmyndigheten en heltäckande och operativ förståelse av IKT-riskhanteringen hos den kritiska tredjepartsleverantören av IKT-tjänster. Möjligheten för den ledande tillsynsmyndigheten, i egenskap av unionsbyrå, att utöva befogenheter utanför unionens territorium bör vederbörligen avgränsas av relevanta villkor, särskilt samtycke från den berörda kritiska tredjepartsleverantören av IKT-tjänster. På samma sätt bör de berörda myndigheterna i tredjelandet informeras om, och inte ha invänt mot, utövandet av den ledande tillsynsmyndighetens verksamhet på tredjelandets eget territorium. För att säkerställa ett effektivt genomförande, och utan att det påverkar

([21]) Europaparlamentets och rådets direktiv 2013/34/EU av den 26 juni 2013 om årsbokslut, koncernredovisning och rapporter i vissa typer av företag, om ändring av Europaparlamentets och rådets direktiv 2006/43/EG och om upphävande av rådets direktiv 78/660/EEG och 83/349/EEG (EUT L 182, 29.6.2013, s. 19).

unionsinstitutionernas och medlemsstaternas respektive befogenheter, måste dock sådana befogenheter också vara fullt förankrade i ingåendet av avtal om administrativt samarbete med de relevanta myndigheterna i det berörda tredjelandet. Denna förordning bör därför göra det möjligt för de europeiska tillsynsmyndigheterna att ingå avtal om administrativt samarbete med relevanta myndigheter i tredjeländer, vilka inte på annat sätt bör skapa rättsliga skyldigheter för unionen och dess medlemsstater.

(84) För att underlätta kommunikationen med den ledande tillsynsmyndigheten och säkerställa lämplig representation bör kritiska tredjepartsleverantörer av IKT-tjänster som ingår i en koncern utse en juridisk person till sin samordningspunkt.

(85) Tillsynsramen bör inte påverka medlemsstaternas behörighet att utföra egna tillsyns- eller övervakningsuppdrag avseende tredjepartsleverantörer av IKT-tjänster som inte klassificeras som kritiska enligt denna förordning, men som anses vara viktiga på nationell nivå.

(86) För att utnyttja den 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-risk, i enlighet med sina uppgifter i fråga om cybersäkerhet. Detta arbete bör stödjas av en ny underkommitté (*tillsynsforumet*) som utför förberedande arbete både för de enskilda beslut som riktar sig till kritiska tredjepartsleverantörer av IKT-tjänster, och för utfärdande av kollektiva rekommendationer, särskilt i förhållande till riktmärkning av tillsynsprogram för kritiska tredjepartsleverantörer av IKT-tjänster, och fastställande av bästa praxis för hantering av IKT-koncentrationsrisker.

(87) För att säkerställa att kritiska tredjepartsleverantörer av IKT-tjänster lämpligt och effektivt övervakas på unionsnivå föreskriver denna förordning att var och en av de tre europeiska tillsynsmyndigheterna kan utses till ledande tillsynsmyndighet. Den enskilda tilldelningen av en kritisk tredjepartsleverantör av IKT-tjänster till en av de tre europeiska tillsynsmyndigheterna bör vara resultatet av en bedömning av den övervägande andelen finansiella entiteter som är verksamma inom de finansiella sektorer för vilka den europeiska tillsynsmyndigheten har ansvar. Detta tillvägagångssätt bör leda till en välavvägd fördelning av uppgifter och ansvar mellan de tre europeiska tillsynsmyndigheterna i samband med utövandet av tillsynsfunktionerna och bör på bästa sätt utnyttja de personalresurser och den tekniska expertis som finns i var och en av de tre europeiska tillsynsmyndigheterna.

(88) Ledande tillsynsmyndigheter bör tilldelas de befogenheter som krävs för att genomföra undersökningar, inspektioner på plats och på annan plats i kritiska tredjepartsleverantörer av IKT-tjänsters lokaler och platser och få fullständig och uppdaterad information. De befogenheterna bör göra det möjligt för den ledande tillsynsmyndigheten att få verklig inblick i typen, omfattningen och effekten av den IKT-tredjepartsrisk som finansiella entiteter och i förlängningen unionens finansiella system utsätts för. Att de europeiska tillsynsmyndigheterna anförtros den ledande tillsynsrollen är en förutsättning för att kunna få grepp om och ta itu med den systemrelaterade dimensionen av IKT-risk inom finanssektorn. Den inverkan som kritiska tredjepartsleverantörer av IKT-tjänster har på unionens sektor för finansiella tjänster och de potentiella problemen med den därmed förknippade IKT-koncentrationsrisken kräver en gemensam strategi på unionsnivå. Det samtidiga utförandet av ett stort antal revisioner och åtkomsträttigheter som utnyttjas separat av en mängd behöriga myndigheter med liten eller ingen samordning sinsemellan, skulle förhindra finansiella tillsynsmyndigheter från att erhålla en fullständig och övergripande överblick över IKT-tredjepartsriskerna inom unionen, och skulle samtidigt innebära redundans, börda och komplexitet för kritiska tredjepartsleverantörer av IKT-tjänster om dessa vore föremål för en mängd förfrågningar om övervakning och inspektion.

(89) På grund av den betydande inverkan som klassificeringen som kritisk har, bör denna förordning säkerställa att rättigheterna för kritiska tredjepartsleverantörer av IKT-tjänster respekteras inom hela genomförandet av tillsynsramen. Innan sådana leverantörer klassificeras som kritiska bör de t.ex. ha rätt att till den ledande tillsynsmyndigheten lämna in ett motiverat utlåtande med all information som är relevant för den bedömning som rör klassificeringen. Eftersom den ledande tillsynsmyndigheten bör ha befogenhet att lämna rekommendationer om IKT-riskfrågor och lämpliga åtgärder för hantering av dessa, vilket inbegriper befogenheten att motsätta sig vissa avtalsarrangemang som i slutändan påverkar stabiliteten i den finansiella entiteten eller det finansiella systemet, bör kritiska tredjepartsleverantörer av IKT-tjänster också, innan de rekommendationerna färdigställs, ges möjlighet att lämna förklaringar om vilka effekter de föreslagna lösningarna i rekommendationerna förväntas ha på kunder som är entiteter som faller utanför denna förordnings tillämpningsområde samt utarbeta lösningar för att minska riskerna. Kritiska tredjepartsleverantörer av IKT-tjänster som invänder mot rekommendationerna bör lämna en

motiverad förklaring gällande deras avsikt att inte godta rekommendationen. Om en sådan motiverad förklaring inte lämnas eller där den bedöms vara otillräcklig bör den ledande tillsynsmyndigheten utfärda ett offentligt meddelande med en kortfattad beskrivning av den bristande efterlevnaden.

(90) De behöriga myndigheterna bör vederbörligen låta uppgiften att kontrollera den faktiska efterlevnaden av rekommendationer som utfärdats av den ledande tillsynsmyndigheten ingå i deras uppdrag i fråga om tillsyn över finansiella entiteter. De behöriga myndigheterna bör kunna begära att finansiella entiteter vidtar ytterligare åtgärder för att hantera de risker som har identifierats i den ledande tillsynsmyndighetens rekommendationer, och bör i sinom tid utfärda meddelanden om detta. Om den ledande tillsynsmyndigheten riktar rekommendationer till kritiska tredjepartsleverantörer av IKT-tjänster som står under tillsyn enligt direktiv (EU) 2022/2555 bör de behöriga myndigheterna, på frivillig basis och innan ytterligare åtgärder antas, kunna samråda med de behöriga myndigheterna enligt det direktivet i syfte att främja en samordnad strategi för hantering av de berörda kritiska tredjepartsleverantörerna av IKT-tjänster.

(91) Utövandet av tillsyn bör styras av tre operativa principer som syftar till att säkerställa a) nära samordning mellan de europeiska tillsynsmyndigheterna i deras roller som ledande tillsynsmyndigheter, genom ett gemensamt tillsynsnätverk, b) överensstämmelse med den ram som inrättas genom direktiv (EU) 2022/2555 (genom frivilligt samråd med organ enligt det direktivet i syfte att undvika överlappning av åtgärder som är riktade till kritiska tredjepartsleverantörer av IKT-tjänster), och c) omsorg för att minimera den potentiella risken för avbrott i tjänster som kritiska tredjepartsleverantörer av IKT-tjänster tillhandahåller kunder som är entiteter som faller utanför denna förordnings tillämpningsområde.

(92) Tillsynsramen bör inte ersätta eller på något sätt eller i någon del användas i stället för kravet på att finansiella entiteter själva ska hantera de risker som är förknippade med användningen av tredjepartsleverantörer av IKT-tjänster, inbegripet deras skyldighet att upprätthålla en fortlöpande övervakning av avtal med kritiska tredjepartsleverantörer av IKT-tjänster. På motsvarande sätt bör tillsynsramen inte påverka finansiella entiteters fulla ansvar för att efterleva och uppfylla alla rättsliga skyldigheter som fastställs i denna förordning och i den relevanta rätten avseende finansiella tjänster.

(93) För att undvika dubbelarbete och överlappningar bör de behöriga myndigheterna avstå från att enskilt vidta åtgärder som syftar till att övervaka riskerna i samband med den kritiska tredjepartsleverantören av IKT-tjänster och bör i detta avseende förlita sig på den relevanta ledande tillsynsmyndighetens bedömning. Alla åtgärder bör under alla förhållanden i förväg samordnas och överenskommas med den ledande tillsynsmyndigheten vid fullgörandet av uppgifter inom tillsynsramen.

(94) För att främja konvergens på internationell nivå när det gäller användning av bästa praxis vid granskningen och övervakningen av den digitala riskhanteringen hos tredjepartsleverantörer av IKT-tjänster bör de europeiska tillsynsmyndigheterna uppmuntras att ingå samarbetsavtal med relevanta tillsynsmyndigheter och reglerande myndigheter i tredjeländer.

(95) För att dra nytta av den särskilda kompetensen, de tekniska färdigheterna och expertisen hos personal som är specialiserad på operativa risker och IKT-risk inom de behöriga myndigheterna bör de tre europeiska tillsynsmyndigheterna och, på frivillig basis, de behöriga myndigheterna enligt direktiv (EU) 2022/2555, den ledande tillsynsmyndigheten ta vara på nationell tillsynsförmåga och tillsynskunskap och inrätta särskilda granskningsgrupper för varje kritisk tredjepartsleverantör av IKT-tjänster, för att samla sektorsövergripande grupper till stöd för förberedelserna och genomförandet av tillsynsverksamhet, inbegripet allmänna utredningar och inspektioner av kritiska tredjepartsleverantörer av IKT-tjänster, samt för eventuell nödvändig uppföljning av dem.

(96) Medan kostnader som uppstår till följd av tillsynsuppgifter till fullo skulle finansieras genom avgifter som tas ut av kritiska tredjepartsleverantörer av IKT-tjänster, kommer de europeiska tillsynsmyndigheterna sannolikt, innan tillsynsramen börjar tillämpas, att ådra sig kostnader för genomförandet av särskilda IKT-system till stöd för den kommande tillsynen, eftersom särskilda IKT-system skulle behöva utvecklas och införas i förväg. I denna förordning föreskrivs därför en hybridfinansieringsmodell, enligt vilken själva tillsynsramen till fullo skulle finansieras genom avgifter, medan utvecklingen av de europeiska tillsynsmyndigheternas IKT-system skulle finansieras genom bidrag från unionen och nationella behöriga myndigheter.

(97) De behöriga myndigheterna bör ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att säkerställa ett korrekt fullgörande av sina skyldigheter enligt denna förordning. De bör i princip offentliggöra meddelanden om de administrativa sanktioner som de ålägger. Eftersom finansiella entiteter och tredjepartsleverantörer av IKT-tjänster kan vara etablerade i olika medlemsstater och övervakas av olika behöriga myndigheter bör tillämpningen av denna förordning underlättas, å ena sidan, av 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, och, å andra sidan, av samråd med de europeiska tillsynsmyndigheterna genom ömsesidigt informationsutbyte och bistånd inom ramen för den relevanta tillsynsverksamheten.

(98) För att ytterligare kvantitativt och kvalitativt fastställa kriterierna för klassificering av tredjepartsleverantörer av IKT-tjänster som kritiska och harmonisera tillsynsavgifterna bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen för att komplettera denna förordning med närmare specificering av den systempåverkan som ett fel eller en driftstörning hos en tredjepartsleverantör av IKT-tjänster skulle kunna ha på de finansiella entiteter som den levererar IKT-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 data och IKT-arbetsbelastningar till en annan tredjepartsleverantör av IKT-tjänster 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 av den 13 april 2016 om bättre lagstiftning ([22]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter bör Europaparlamentet och rådet erhålla alla handlingar samtidigt som medlemsstaternas experter, och deras experter bör ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(99) Tekniska standarder för tillsyn bör säkerställa en konsekvent harmonisering av kraven i denna förordning. De europeiska tillsynsmyndigheterna bör i sina roller som organ med högspecialiserad expertis 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 av allvarliga IKT-relaterade incidenter och testning samt med avseende på nyckelkrav för en sund övervakning av IKT-tredjepartsrisker. Kommissionen och de europeiska tillsynsmyndigheterna bör säkerställa att dessa standarder och krav kan tillämpas av alla finansiella entiteter på ett sätt som står i proportion till deras storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser. Kommissionen bör ges befogenhet att anta dessa tekniska standarder för tillsyn genom delegerade akter i enlighet med artikel 290 i EUF-fördraget och i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

(100) För att göra det lättare att jämföra rapporter om allvarliga IKT-relaterade incidenter och allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, samt säkerställa insyn avseende avtalsarrangemang för användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster, bör de europeiska tillsynsmyndigheterna utarbeta förslag till tekniska standarder för genomförande där det fastställs standardiserade mallar, formulär och förfaranden för finansiella entiteter för rapportering av allvarliga IKT-relaterade incidenter och allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, samt standardiserade mallar för registrering av information. När de europeiska tillsynsmyndigheterna utarbetar dessa standarder bör de ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser. Kommissionen bör ges befogenhet att anta dessa tekniska standarder för genomförande genom genomförandeakter i enlighet med artikel 291 i EUF-fördraget och i enlighet med artikel 15 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

([22]) EUT L 123, 12.5.2016, s. 1.

(101) Eftersom ytterligare krav redan har specificerats genom delegerade akter och genomförandeakter baserade på tekniska standarder för tillsyn och genomförande i Europaparlamentets och rådets förordningar (EG) nr 1060/2009 ([23]), (EU) nr 648/2012 ([24]), (EU) nr 600/2014 ([25]) och (EU) nr 909/2014 ([26]) 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.

(102) Eftersom denna förordning, tillsammans med Europaparlamentets och rådets direktiv (EU) 2022/2556 ([27]), innebär en konsolidering av IKT-riskhanteringsbestämmelser i flera förordningar och direktiv i unionens regelverk om finansiella tjänster, inbegripet förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014 samt Europaparlamentets och rådets förordning (EU) 2016/1011 ([28]), bör dessa förordningar ändras för att säkerställa fullständig enhetlighet och klargöra att de tillämpliga bestämmelserna om IKT-risker fastställs i den här förordningen.

(103) Följaktligen bör tillämpningsområdet för de relevanta artiklar som rör operativ risk, för vilka delegerade akter och genomförandeakter ska antas enligt befogenheterna i förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, begränsas så att alla bestämmelser som omfattar aspekter av digital operativ motståndskraft och som i dag ingår i de förordningarna överförs till den här förordningen.

(104) Den potentiella systemrisk på cyberområdet som är förknippad med användningen av IKT-infrastrukturer som möjliggör drift av betalningssystem och tillhandahållande av betalningshantering bör vederbörligen hanteras på unionsnivå genom harmoniserade regler om digital motståndskraft. I detta syfte bör kommissionen snabbt bedöma behovet av en översyn av denna förordnings tillämpningsområde och samtidigt anpassa en sådan översyn till resultatet av den omfattande översyn som avses i direktiv (EU) 2015/2366. Många storskaliga attacker som genomförts under det senaste årtiondet visar hur betalningssystemen har blivit en ingång för cyberhot. Betalningssystem och betalningshantering, som ligger i centrum av betaltjänstkedjan och uppvisar en hög grad av sammanlänkning med det övergripande finansiella systemet, har fått en avgörande betydelse för unionens finansmarknaders funktion. Cyberangrepp mot sådana system kan orsaka allvarliga driftstörningar i verksamheten med direkta konsekvenser för viktiga ekonomiska funktioner, såsom underlättande av betalningar, och indirekta effekter på därmed sammanhängande ekonomiska processer. Till dess att ett harmoniserat system för och tillsyn över operatörer av betalningssystem och hanteringsentiteter har införts på unionsnivå, får medlemsstaterna, i syfte att tillämpa liknande marknadspraxis, hämta inspiration från de krav på digital operativ motståndskraft som fastställs i denna förordning när de tillämpar regler på operatörer av betalningssystem och hanteringsentiteter som står under tillsyn inom deras egna jurisdiktioner.

([23]) Europaparlamentets och rådets förordning (EG) nr 1060/2009 av den 16 september 2009 om kreditvärderingsinstitut (EUT L 302, 17.11.2009, s. 1).

([24]) Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1).

([25]) Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 84).

([26]) Europaparlamentets och rådets förordning (EU) nr 909/2014 av den 23 juli 2014 om förbättrad värdepappersavveckling i Europeiska unionen och om värdepapperscentraler samt ändring av direktiv 98/26/EG och 2014/65/EU och förordning (EU) nr 236/2012 (EUT L 257, 28.8.2014, s. 1).

([27]) Europaparlamentets och rådets direktiv (EU) 2022/2556 av den 14 december 2022 om ändring av direktiven 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 och (EU) 2016/2341 vad gäller digital operativ motståndskraft för finanssektorn (se sidan 153 i detta nummer av EUT).

([28]) 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).

(105) Eftersom målet för denna förordning, dvs. att uppnå en hög nivå av digital operativ motståndskraft för reglerade finansiella entiteter, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna eftersom det kräver harmonisering av en mängd olika regler i unionsrätten och nationell rätt, utan snarare, på grund av dess omfattning och verkningar, kan uppnås bättre på unionsnivå, kan 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.

(106) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([29]) och avgav ett yttrande den 10 maj 2021 ([30]).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Innehåll

1. I syfte att uppnå en hög gemensam nivå av digital operativ motståndskraft fastställs i denna förordning enhetliga krav avseende säkerhet i nätverks- och informationssystem som stöder finansiella entiteters affärsprocesser enligt följande:

a) Krav som är tillämpliga på finansiella entiteter i fråga om

   i) riskhantering inom informations- och kommunikationsteknik (IKT),

   ii) rapportering av allvarliga IKT-relaterade incidenter och underrättande om, på frivillig grund, betydande cyberhot till de behöriga myndigheterna,

   iii) rapportering av allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter till de behöriga myndigheterna av de finansiella entiteter som avses i artikel 2.1 a–d,

   iv) testning av digital operativ motståndskraft,

   v) utbyte av information och underrättelser i samband med cyberhot och cybersårbarheter,

   vi) åtgärder för en sund hantering av tredjepartsrelaterad IKT-risk.

b) Krav i samband med de kontraktsmässiga arrangemang som har ingåtts mellan tredjepartsleverantörer av IKT-tjänster och finansiella entiteter.

c) Regler för inrättandet och genomförandet av tillsynsramen för kritiska tredjepartsleverantörer av IKT-tjänster när de tillhandahåller tjänster till finansiella entiteter.

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 entiteter som har identifierats som leverantörer av väsentliga eller viktiga entiteter enligt nationella regler som införlivar artikel 3 i direktiv (EU) 2022/2555 ska denna förordning betraktas som en sektorsspecifik unionsrättsakt vid tillämpningen av artikel 4 i det direktivet.

3. Denna förordning påverkar inte medlemsstaternas ansvar vad gäller väsentliga statliga funktioner inom områdena allmän säkerhet, försvar och nationell säkerhet i enlighet med unionsrätten.

([29]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

([30]) EUT C 229, 15.6.2021, s. 16.

Artikel 2

Tillämpningsområde

1. Utan att det påverkar tillämpningen av punkterna 3 och 4 är denna förordning tillämplig på följande entiteter:

a) Kreditinstitut.

b) Betalningsinstitut, inbegripet sådana betalningsinstitut som är undantagna enligt direktiv (EU) 2015/2366.

c) Leverantörer av kontoinformationstjänster.

d) Institut för elektroniska pengar, inbegripet sådana institut för elektroniska pengar som är undantagna enligt direktiv 2009/110/EG.

e) Värdepappersföretag.

f) Leverantörer av kryptotillgångstjänster, auktoriserade enligt en Europaparlamentets och rådets förordning om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 och direktiven 2013/36/EU och (EU) 2019/1937 (*förordningen om kryptotillgångar*) och emittenter av tillgångsanknutna token.

g) Värdepapperscentraler.

h) Centrala motparter.

i) Handelsplatser.

j) Transaktionsregister.

k) Förvaltare av alternativa investeringsfonder.

l) Förvaltningsbolag.

m) Leverantörer av datarapporteringstjänster.

n) Försäkrings- och återförsäkringsföretag.

o) Försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet.

p) Tjänstepensionsinstitut.

q) Kreditvärderingsinstitut.

r) Administratörer av kritiska referensvärden.

s) Leverantörer av gräsrotsfinansieringstjänster.

t) Värdepapperiseringsregister.

u) Tredjepartsleverantörer av IKT-tjänster.

2. Vid tillämpningen av denna förordning ska de entiteter som avses i punkt 1 a–t tillsammans benämnas *finansiella entiteter*.

3. Denna förordning är inte tillämplig på

a) förvaltare av alternativa investeringsfonder som avses i artikel 3.2 i direktiv 2011/61/EU,

b) försäkrings- och återförsäkringsföretag som avses i artikel 4 i direktiv 2009/138/EG,

c) tjänstepensionsinstitut som förvaltar pensionsplaner som tillsammans inte har fler än totalt 15 medlemmar,

d) fysiska eller juridiska personer som är undantagna enligt artiklarna 2 och 3 i direktiv 2014/65/EU,

e) försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet som är mikroföretag eller små eller medelstora företag,

f) postgiroinstitut som avses i artikel 2.5.3 i direktiv 2013/36/EU.

4. Medlemsstaterna får från tillämpningsområdet för denna förordning utesluta sådana enheter som avses i artikel 2.5.4–2.5.23 i direktiv 2013/36/EU om de är belägna inom deras respektive territorier. Om en medlemsstat utnyttjar en sådan möjlighet ska den informera kommissionen om detta samt om eventuella senare ändringar av detta. Kommissionen ska offentliggöra informationen på sin webbplats eller på annat lättillgängligt vis.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

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

2. *nätverks- och informationssystem*: ett nätverks- och informationssystem enligt definitionen i artikel 6.1 i direktiv (EU) 2022/2555.

3. *äldre IKT-system*: ett IKT-system som har nått slutet på sin livscykel, som inte lämpar sig för uppgraderingar eller justeringar, av tekniska eller kommersiella skäl, eller som inte längre stöds av leverantören eller av en tredjepartsleverantör av IKT-tjänster, men som fortfarande används och stöder den finansiella entitetens funktioner.

4. *säkerhet i nätverks- och informationssystem*: ett säkerhet i nätverks- och informationssystem enligt definitionen i artikel 6.2 i direktiv (EU) 2022/2555.

5. *IKT-risk*: varje rimligen identifierbar omständighet i samband med användningen av nätverks- och informationssystem som, om de inträffar, kan äventyra säkerheten i nätverks- och informationssystem, verktyg eller processer som är teknikberoende, funktioner och processer eller tillhandahållandet av tjänster genom att orsaka negativa effekter i den digitala eller fysiska miljön.

6. *informationstillgång*: en samling materiell eller immateriell skyddsvärd information.

7. *IKT-tillgång*: en programvaru- eller maskinvarutillgång i nätverks- och informationssystemen som används av den finansiella entiteten.

8. *IKT-relaterad incident*: en enskild händelse eller en serie sammankopplade händelser som inte planerats av den finansiella entiteten och som äventyrar säkerheten i nätverks- och informationssystemen och har negativ inverkan på tillgängligheten, äktheten, integriteten eller konfidentialiteten vad gäller datan eller de tjänster som tillhandahålls av den finansiella entiteten.

9. *betalningsrelaterad operativ incident eller säkerhetsincident*: en enskild händelse eller en serie sammankopplade händelser som inte planerats av de finansiella entiteter som avses i artikel 2.1 a–d och som kan vara IKT-relaterade men inte behöver vara det och har negativ inverkan på tillgängligheten, äktheten, integriteten eller konfidentialiteten vad gäller betalningsrelaterade data eller de betalningsrelaterade tjänster som tillhandahålls av den finansiella entiteten.

10. *allvarlig IKT-relaterad incident*: en IKT-relaterad incident som har stor negativ inverkan på nätverks- och informationssystem som stöder den finansiella entitetens kritiska eller viktiga funktioner.

11. *allvarlig betalningsrelaterad operativ incident eller säkerhetsincident*: en betalningsrelaterad operativ incident eller säkerhetsincident som har stor negativ inverkan på de betalningsrelaterade tjänster som tillhandahålls.

12. *cyberhot*: ett *cyberhot* enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

13. *betydande cyberhot*: ett cyberhot vars tekniska egenskaper indikerar att det potentiellt kan leda till en allvarlig IKT-relaterad incident eller allvarlig betalningsrelaterad operativ incident eller säkerhetsincident.

14. *cyberangrepp*: en skadlig IKT-relaterad incident orsakad av ett försök av en fientlig aktör att förstöra, exponera, ändra, deaktivera, stjäla eller få obehörig åtkomst till eller obehörigt utnyttja en tillgång.

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

16. *sårbarhet*: en svaghet, mottaglighet eller brist hos en tillgång, ett system, en process eller en kontroll som kan utnyttjas.

17. *hotbildsstyrd 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 (rött lag) test av de kritiska produktionssystem som är i drift hos den finansiella entiteten.

18. *IKT-tredjepartsrisk*: en IKT-risk som kan uppstå för en finansiell entitet i samband med dess användning av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster eller av underleverantörer till sådana leverantörer, inbegripet genom utkontrakteringsarrangemang.

19. *tredjepartsleverantör av IKT-tjänster*: ett företag som tillhandahåller IKT-tjänster.

20. *koncernintern IKT-tjänsteleverantör*: ett företag som ingår i en finansiell koncern och som huvudsakligen tillhandahåller IKT-tjänster till finansiella entiteter inom samma koncern eller till finansiella entiteter som tillhör samma institutionella skyddssystem, inbegripet till deras moderföretag, dotterföretag, filialer eller andra entiteter som står under samma ägarskap eller kontroll.

21. *IKT-tjänster*: digitala tjänster och datatjänster som fortlöpande tillhandahålls genom IKT-system till en eller flera interna eller externa användare, inbegripet maskinvara som tjänst och maskinvarutjänster som inbegriper tillhandahållande av teknisk support genom uppdateringar av programvara eller fast programvara från maskinvaruleverantören, ej inbegripet traditionella analoga telefontjänster.

22. *kritisk eller viktig funktion*: en funktion vars avbrott väsentligt skulle försämra den finansiella entitetens finansiella resultat eller sundheten eller kontinuiteten i dess tjänster och verksamhet, eller om funktionens upphörande, brister eller misslyckande väsentligt skulle försämra en finansiell entitets fortsatta efterlevnad av villkoren och skyldigheterna i auktorisationen eller av dess övriga skyldigheter enligt tillämplig rätt avseende finansiella tjänster.

23. *kritisk tredjepartsleverantör av IKT-tjänster*: en tredjepartsleverantör av IKT-tjänster som har klassificerats som kritisk i enlighet med artikel 31.

24. *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 och som har ingått ett kontraktsmässigt arrangemang med en finansiell entitet om tillhandahållande av IKT-tjänster.

25. *dotterföretag*: ett dotterföretag i den mening som avses i artiklarna 2.10 och 22 i direktiv 2013/34/EU.

26. *koncern*: en koncern enligt definitionen i artikel 2.11 i direktiv 2013/34/EU.

27. *moderföretag*: ett moderföretag i den mening som avses i artiklarna 2.9 och 22 i direktiv 2013/34/EU.

28. *IKT-underleverantör etablerad i ett tredjeland*: en IKT-underleverantör som är en juridisk person som är etablerad i ett tredjeland och som har ingått ett kontraktsmässigt arrangemang antingen med en tredjepartsleverantör av IKT-tjänster eller med en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland.

29. *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 sådana leverantörer kan komma att äventyra förmågan hos en finansiell entitet att tillhandahålla kritiska eller viktiga funktioner eller leda till andra typer av negativa effekter, inbegripet stora förluster, eller äventyra den finansiella stabiliteten i unionen som helhet.

30. *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 Europaparlamentets och rådets direktiv 2009/65/EG ([31]), artikel 2.1.45 i förordning (EU) nr 909/2014, artikel 3.1.20 i förordning (EU) 2016/1011 och i de relevanta bestämmelserna i förordningen om kryptotillgångar, eller motsvarande personer som i praktiken leder entiteten eller har nyckelfunktioner i enlighet med relevant unionsrätt eller nationell rätt.

31. *kreditinstitut*: ett kreditinstitut enligt definitionen i artikel 4.1.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 ([32]).

32. *institut undantaget enligt direktiv 2013/36/EU*: en sådan enhet som avses i artikel 2.5.4–2.5.23 i direktiv 2013/36/EU.

33. *värdepappersföretag*: ett värdepappersföretag enligt definitionen i artikel 4.1.1 i direktiv 2014/65/EU.

34. *litet och icke-sammanlänkat värdepappersföretag*: ett värdepappersföretag som uppfyller villkoren i artikel 12.1 i Europaparlamentets och rådets förordning (EU) 2019/2033 ([33]).

35. *betalningsinstitut*: ett betalningsinstitut enligt definitionen i artikel 4.4 i direktiv (EU) 2015/2366.

36. *betalningsinstitut undantaget enligt direktiv (EU) 2015/2366*: sådana betalningsinstitut som är undantagna enligt artikel 32.1 i direktiv (EU) 2015/2366.

37. *leverantör av kontoinformationstjänster*: sådana leverantörer av kontoinformationstjänster som avses i artikel 33.1 i direktiv (EU) 2015/2366.

38. *institut för elektroniska pengar*: ett institut för elektroniska pengar enligt definitionen i artikel 2.1 i Europaparlamentets och rådets direktiv 2009/110/EG.

39. *institut för elektroniska pengar undantaget enligt direktiv 2009/110/EG*: ett institut för elektroniska pengar som omfattas av ett undantag enligt artikel 9.1 i direktiv 2009/110/EG.

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

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

42. *värdepapperscentral*: en värdepapperscentral enligt definitionen i artikel 2.1.1 i förordning (EU) nr 909/2014.

43. *handelsplats*: en handelsplats enligt definitionen i artikel 4.1.24 i direktiv 2014/65/EU.

44. *förvaltare av alternativa investeringsfonder*: en förvaltare av alternativa investeringsfonder enligt definitionen i artikel 4.1 b i direktiv 2011/61/EU.

45. *förvaltningsbolag*: ett förvaltningsbolag enligt definitionen i artikel 2.1 b i direktiv 2009/65/EG.

46. *leverantör av datarapporteringstjänster*: en leverantör av datarapporteringstjänster i enlighet med vad som avses i artikel 2.1.34–36 i förordning (EU) nr 600/2014.

47. *försäkringsföretag*: ett försäkringsföretag enligt definitionen i artikel 13.1 i direktiv 2009/138/EG.

48. *återförsäkringsföretag*: ett återförsäkringsföretag enligt definitionen i artikel 13.4 i direktiv 2009/138/EG.

([31]) Europaparlamentets och rådets direktiv 2009/65/EG av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag) (EUT L 302, 17.11.2009, s. 32).

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

([33]) Europaparlamentets och rådets förordning (EU) 2019/2033 av den 27 november 2019 om tillsynskrav för värdepappersföretag och om ändring av förordningarna (EU) nr 1093/2010, (EU) nr 575/2013, (EU) nr 600/2014 och (EU) nr 806/2014 (EUT L 314, 5.12.2019, s. 1).

49. *försäkringsförmedlare*: en försäkringsförmedlare enligt definitionen i artikel 2.1.3 i Europaparlamentets och rådets direktiv (EU) 2016/97 ([34]).

50. *försäkringsförmedlare som bedriver förmedling som sidoverksamhet*: en försäkringsförmedlare som bedriver förmedling som sidoverksamhet enligt definitionen i artikel 2.1.4 i direktiv (EU) 2016/97.

51. *återförsäkringsförmedlare*: en återförsäkringsförmedlare enligt definitionen i artikel 2.1.5 i direktiv (EU) 2016/97.

52. *tjänstepensionsinstitut*: ett tjänstepensionsinstitut enligt definitionen i artikel 6.1 i direktiv (EU) 2016/2341.

53. *litet tjänstepensionsinstitut*: ett tjänstepensionsinstitut som förvaltar pensionsplaner som tillsammans inte har fler än totalt 100 medlemmar.

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

55. *leverantör av kryptotillgångstjänster*: en leverantör av kryptotillgångstjänster enligt definitionen i de relevanta bestämmelserna i förordningen om kryptotillgångar.

56. *emittent av tillgångsanknutna token*: en emittent av tillgångsanknutna token enligt definitionen i de relevanta bestämmelserna i förordningen om kryptotillgångar.

57. *administratör av kritiska referensvärden*: en administratör av *kritiska referensvärden* enligt definitionen i artikel 3.1.25 i förordning (EU) 2016/1011.

58. *leverantör av gräsrotsfinansieringstjänster*: en leverantör av gräsrotsfinansieringstjänster enligt definitionen i artikel 2.1 e i Europaparlamentets och rådets förordning (EU) 2020/1503 ([35]).

59. *värdepapperiseringsregister*: ett värdepapperiseringsregister enligt definitionen i artikel 2.23 i Europaparlamentets och rådets förordning (EU) 2017/2402 ([36]).

60. *mikroföretag*: en finansiell entitet, som inte är en handelsplats, en central motpart, ett transaktionsregister eller en värdepapperscentral, och som har färre än 10 anställda och en årsomsättning och/eller årlig balansomslutning som inte överstiger 2 miljoner EUR.

61. *ledande tillsynsmyndighet*: den europeiska tillsynsmyndighet som utses i enlighet med artikel 31.1 b i denna förordning.

62. *den gemensamma kommittén*: den kommitté som avses i artikel 54 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

63. *litet företag*: en finansiell entitet med tio eller fler anställda men färre än 50 anställda och en årsomsättning och/eller årlig balansomslutning som överstiger 2 miljoner EUR men som inte överstiger 10 miljoner EUR.

64. *medelstort företag*: en finansiell entitet som inte är ett litet företag och som har färre än 250 anställda och en årsomsättning som inte överstiger 50 miljoner EUR och/eller en årlig balansomslutning som inte överstiger 43 miljoner EUR.

65. *offentlig myndighet*: alla statliga entiteter eller andra entiteter inom offentlig förvaltning, inbegripet nationella centralbanker.

([34]) Europaparlamentets och rådets direktiv (EU) 2016/97 av den 20 januari 2016 om försäkringsdistribution (EUT L 26, 2.2.2016, s. 19).

([35]) Europaparlamentets och rådets förordning (EU) 2020/1503 av den 7 oktober 2020 om europeiska leverantörer av gräsrotsfinansieringstjänster för företag och om ändring av förordning (EU) 2017/1129 och direktiv (EU) 2019/1937 (EUT L 347, 20.10.2020, s. 1).

([36]) Europaparlamentets och rådets förordning (EU) 2017/2402 av den 12 december 2017 om ett allmänt ramverk för värdepapperisering och om inrättande av ett särskilt ramverk för enkel, transparent och standardiserad värdepapperisering samt om ändring av direktiven 2009/65/EG, 2009/138/EG och 2011/61/EU och förordningarna (EG) nr 1060/2009 och (EU) nr 648/2012 (EUT L 347, 28.12.2017, s. 35).

Artikel 4

Proportionalitetsprincipen

1. Finansiella entiteter ska genomföra reglerna i kapitel II i enlighet med proportionalitetsprincipen, och med beaktande av sin storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, sin verksamhet och sina insatser.

2. Dessutom ska finansiella entiteters tillämpning av kapitlen III, IV och V, avsnitt I, stå i proportion till deras storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser, i enlighet med vad som specificeras i de relevanta reglerna i dessa kapitel.

3. De behöriga myndigheterna ska beakta finansiella entiteters tillämpning av proportionalitetsprincipen när de ser över enhetligheten i IKT-riskhanteringsramen baserat på de rapporter som lämnats in på begäran av de behöriga myndigheterna enligt artiklarna 6.5 och 16.2.

KAPITEL II

IKT-riskhantering

Avsnitt I

Artikel 5

Styrning och organisation

1. Finansiella entiteter ska ha en intern styrnings- och kontrollram som säkerställer en effektiv och ansvarsfull hantering av IKT-risk i enlighet med artikel 6.4, i syfte att åstadkomma en hög nivå av digital operativ motståndskraft.

2. Den finansiella entitetens ledningsorgan ska fastställa, godkänna, övervaka och ansvara för genomförandet av alla arrangemang som rör den IKT-riskhanteringsram som avses i artikel 6.1.

Vid tillämpning av det första stycket ska ledningsorganet

a) ha det slutliga ansvaret för att hantera den finansiella entitetens IKT-risk,

b) införa strategier som syftar till att säkerställa bibehållandet av höga standarder för tillgänglighet, äkthet, integritet och konfidentialitet för data,

c) fastställa tydliga roller och ansvarsområden för alla IKT-relaterade funktioner och inrätta lämpliga styrformer för att säkerställa kommunikation, samarbete och samordning på ett effektivt och skyndsamt sätt mellan dessa funktioner,

d) ha det övergripande ansvaret för att fastställa och godkänna strategin för digital operativ motståndskraft enligt artikel 6.8, inbegripet fastställandet av en lämplig risktoleransnivå för IKT-risk för den finansiella entiteten, enligt vad som avses i artikel 6.8 b,

e) godkänna, övervaka och regelbundet se över genomförandet av den IKT-kontinuitetspolicy och de åtgärds- och återställningsplaner avseende IKT för den finansiella entiteten som avses i artikel 11.1 respektive 11.3, vilka kan antas som särskilda specifika planer och utgöra integrerade delar av den finansiella entitetens övergripande kontinuitetsplan och åtgärds- och återställningsplan,

f) godkänna och regelbundet se över den finansiella entitetens IKT-internrevisionsplaner, IKT-revisioner och väsentliga ändringar av dessa,

g) anslå och regelbundet se över den lämpliga budgeten för att uppfylla den finansiella entitetens behov av digital operativ motståndskraft när det gäller alla typer av resurser, inbegripet relevanta program för medvetenhet om IKT-säkerhet och sådan utbildning om digital operativ motståndskraft som avses i artikel 13.6 och IKT-färdigheter för all personal,

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

i) på verksamhetsnivå etablera rapporteringskanaler som gör det möjligt att vederbörligen informeras om

i) arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster,

ii) alla relevanta planerade väsentliga ändringar som rör tredjepartsleverantörerna av IKT-tjänster,

iii) den potentiella effekten av sådana ändringar på de kritiska eller viktiga funktioner som omfattas av dessa arrangemang, inbegripet en sammanfattning av riskanalysen för att bedöma effekterna av dessa ändringar och åtminstone allvarliga IKT-relaterade incidenter och deras inverkan liksom åtgärder, återställande och korrigerande åtgärder.

3. Andra finansiella entiteter 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 den finansiella entitetens ledningsorgan ska aktivt upprätthålla tillräckliga och aktuella kunskaper och färdigheter för att förstå och bedöma IKT-risk och deras inverkan på den finansiella entitetens verksamhet, inbegripet genom att regelbundet genomgå särskild utbildning som står i proportion till den IKT-risk som hanteras.

Avsnitt II

Artikel 6

IKT-riskhanteringsram

1. Finansiella entiteter ska ha en sund, heltäckande och väldokumenterad IKT-riskhanteringsram som en del av sitt övergripande riskhanteringssystem och den ska göra det möjligt för dem att snabbt, effektivt och heltäckande hantera IKT-risk och säkerställa en hög nivå av digital operativ motståndskraft.

2. IKT-riskhanteringsramen ska omfatta åtminstone de strategier, riktlinjer, förfaranden, IKT-protokoll och IKT-verktyg som är nödvändiga för att på ett vederbörligt och adekvat sätt skydda alla informations- och IKT-tillgångar, inbegripet datorprogramvara, datormaskinvara och servrar, och skydda alla relevanta fysiska komponenter och infrastrukturer, såsom lokaler, datacentraler och känsliga angivna områden, för att säkerställa att alla informations- och IKT-tillgångar är tillräckligt skyddade mot risker, inbegripet skada och obehörig åtkomst eller användning.

3. I enlighet med sin IKT-riskhanteringsram ska finansiella entiteter minimera effekterna av IKT-risk genom att införa lämpliga strategier, riktlinjer, förfaranden, IKT-protokoll och verktyg. De ska tillhandahålla fullständig och uppdaterad information om IKT-risk och om sin IKT-riskhanteringsram till de behöriga myndigheterna när dessa begär det.

4. Andra finansiella entiteter än mikroföretag ska överföra ansvaret för att hantera och övervaka IKT-risk till en kontrollfunktion och säkerställa en lämplig nivå av oberoende för den kontrollfunktionen för att undvika intressekonflikter. Finansiella entiteter ska säkerställa lämplig åtskillnad mellan och lämpligt oberoende för riskhanteringsfunktioner, kontrollfunktioner och interna revisionsfunktioner avseende IKT, enligt modellen med tre försvarslinjer eller en intern riskhanterings- och kontrollmodell.

5. IKT-riskhanteringsramen ska dokumenteras och ses över minst en gång per år, eller regelbundet när det gäller mikroföretag, liksom vid uppkomsten av allvarliga IKT-relaterade incidenter, och i enlighet med tillsynsinstruktioner eller slutsatser från relevanta testnings- eller revisionsprocesser för digital operativ motståndskraft. Ramen ska förbättras fortlöpande baserat på erfarenheterna från genomförande och övervakning. En rapport om översynen av IKT-riskhanteringsramen ska överlämnas till den behöriga myndigheten på dess begäran.

6. IKT-riskhanteringsramen hos andra finansiella entiteter än mikroföretag ska vara föremål för en internrevision av revisorer på regelbunden basis och i enlighet med finansiella entiteters revisionsplan. Dessa revisorer ska ha tillräckliga kunskaper, färdigheter och expertis om IKT-risker, samt ha en lämplig nivå av oberoende. IKT-revisionernas frekvens och inriktning ska stå i proportion till den finansiella entitetens IKT-risk.

7. Finansiella entiteter ska baserat på slutsatserna från den interna revisionsrapporten inrätta en formell uppföljningsprocess, inbegripet regler för snabb kontroll och snabbt åtgärdande av kritiska resultat från IKT-revisionen.

8. IKT-riskhanteringsramen ska omfatta en strategi för digital operativ motståndskraft där det anges hur ramen ska genomföras. För detta ändamål ska strategin för digital operativ motståndskraft inbegripa metoder för att hantera IKT-risk och uppnå specifika IKT-mål på följande sätt:

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

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

c) Fastställa tydliga informationssäkerhetsmål, inbegripet nyckelprestationsindikatorer och viktiga riskmått.

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 IKT-relaterade incidenter, förebygga deras effekter och ge skydd däremot.

f) Lägga fram bevis för den befintliga situationen vad gäller digital operativ motståndskraft baserat på antalet rapporterade allvarliga IKT-relaterade incidenter och de förebyggande åtgärdernas effektivitet.

g) Genomföra tester av den digitala operativa motståndskraften, i enlighet med kapitel IV i denna förordning.

h) Beskriva en kommunikationsstrategi vid IKT-relaterade incidenter; vars offentliggörande föreskrivs i artikel 14.

9. Finansiella entiteter får, när det gäller den strategi för digital operativ motståndskraft som avses i punkt 8, utforma en holistisk strategi med flera olika leverantörer av IKT-tjänster på koncern- eller entitetsnivå som visar de viktigaste beroendena av tredjepartsleverantörer av IKT-tjänster och förklarar logiken bakom upphandlingsmixen av tredjepartsleverantörer av IKT-tjänster.

10. Finansiella entiteter får, i enlighet med unionsrätten och den nationella rätten på området utkontraktera uppgiften att kontrollera efterlevnaden av IKT-riskhanteringskraven till koncerninterna eller externa företag. Vid sådan utkontraktering bär den finansiella entiteten det fulla ansvaret för kontrollen av efterlevnaden av IKT-riskhanteringskraven.

Artikel 7

IKT-system, IKT-protokoll och IKT-verktyg

Finansiella entiteter ska för att åtgärda och hantera IKT-risk använda och upprätthålla uppdaterade IKT-system, IKT-protokoll och IKT-verktyg som

a) är lämpliga med hänsyn till omfattningen hos de transaktioner som ligger till grund för deras verksamhet, i enlighet med den proportionalitetsprincip som anges i artikel 4,

b) är tillförlitliga,

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

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

Artikel 8

Identifiering

1. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter identifiera, klassificera och på lämpligt sätt dokumentera alla IKT-stödda affärsfunktioner, roller och ansvarsområden, de informationstillgångar och IKT-tillgångar som stöder dessa funktioner och deras roller och beroenden i förhållande till IKT-risk. Finansiella entiteter ska vid behov, och minst en gång per år, granska lämpligheten i denna klassificering och i all relevant dokumentation.

2. Finansiella entiteter ska fortlöpande identifiera alla källor till IKT-risk, särskilt riskexponeringen mot och från andra finansiella entiteter, och bedöma cyberhot och IKT-sårbarheter som är relevanta för deras IKT-stödda affärsfunktioner, informationstillgångar och IKT-tillgångar. Finansiella entiteter ska regelbundet och minst en gång per år se över de riskscenarier som påverkar dem.

3. Andra finansiella entiteter än mikroföretag ska göra en riskbedömning vid varje större förändring av nätverks- och informationssystemets infrastruktur, av de processer eller förfaranden som påverkar deras IKT-stödda affärsfunktioner, informationstillgångar eller IKT-tillgångar.

4. Finansiella entiteter ska identifiera alla informationstillgångar och IKT-tillgångar, inbegripet sådana på fjärrplatser, nätverksresurser och maskinvaruutrustning, och kartlägga de som anses vara kritiska. De ska kartlägga informationstillgångarnas och IKT-tillgångarnas konfiguration samt länkarna och det ömsesidiga beroendet mellan de olika informationstillgångarna och IKT-tillgångarna.

5. Finansiella entiteter ska identifiera och dokumentera alla processer som är beroende av tredjepartsleverantörer av IKT-tjänster och identifiera kopplingar till de tredjepartsleverantörer av IKT-tjänster som tillhandahåller tjänster som stöder kritiska eller viktiga funktioner.

6. Vid tillämpning av punkterna 1, 4 och 5 ska finansiella entiteter upprätthålla relevanta inventeringar och uppdatera dem regelbundet och varje gång en sådan större förändring som avses i punkt 3 inträffar.

7. Andra finansiella entiteter än mikroföretag ska regelbundet, och minst en gång per år, genomföra en särskild IKT-riskbedömning av alla äldre IKT-system, och i varje fall före och efter sammanlänkning av tekniker, tillämpningar eller system.

Artikel 9

Skydd och förebyggande

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

2. Finansiella entiteter ska utforma, upphandla och genomföra IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som syftar till att säkerställa IKT-systemens motståndskraft, kontinuitet och tillgänglighet, i synnerhet för de system som stöder kritiska eller viktiga funktioner, och upprätthålla höga standarder för tillgänglighet, äkthet, integritet och konfidentialitet avseende 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 finansiella entiteter använda IKT-lösningar och IKT-processer som är lämpliga i enlighet med artikel 4. Dessa IKT-lösningar och IKT-processer ska

a) säkerställa skyddet vid dataöverföring,

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

c) förhindra bristen på tillgänglighet, försvagandet av äkthet och integritet, överträdelserna av konfidentialitet, och förlusten av data,

d) säkerställa att uppgifterna skyddas mot risker som uppstår från datahanteringen, inbegripet bristfällig förvaltning, processrelaterade risker och den mänskliga faktorn.

4. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter

a) utarbeta och dokumentera riktlinjer för informationssäkerhet där det fastställs regler för att skydda tillgängligheten, äktheten, integriteten och konfidentialiteten hos data, informationstillgångar och IKT-tillgångar, inbegripet hos deras kunder, när så är tillämpligt,

b) enligt en riskbaserad strategi upprätta en sund struktur för förvaltning av nätverk och infrastruktur med hjälp av lämpliga tekniker, metoder och protokoll, vilket kan inbegripa införande av automatiserade mekanismer för att isolera berörda informationstillgångar vid cyberangrepp,

c) genomföra strategier för att begränsa den fysiska eller logiska åtkomsten till informationstillgångar och IKT-tillgångar till enbart det som krävs för legitima och godkända funktioner och verksamheter, och för detta ändamål fastställa en uppsättning strategier, förfaranden och kontroller för åtkomsträttigheter och säkerställa en sund förvaltning av dessa,

d) genomföra strategier och protokoll för starka äkthetsmekanismer, baserade på relevanta standarder och särskilda kontrollsystem, samt skyddsåtgärder för kryptografiska nycklar där data krypteras baserat på resultat från godkända processer för klassificering och IKT-riskbedömning,

e) genomföra dokumenterade strategier, förfaranden och kontroller för hantering av IKT-förändringar, inbegripet ändringar av programvara, maskinvara, fasta programvarukomponenter, system eller säkerhetsparametrar, som bygger på en riskbedömningsmetod och är en integrerad del av den finansiella entitetens 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 dokumenterade strategier för programfixar och uppdateringar.

Vid tillämpning av första stycket led b ska finansiella entiteter utforma infrastrukturen för nätanslutning på ett sätt som gör att den omedelbart kan avskiljas eller segmenteras i syfte att minimera och förhindra spridning, särskilt för sammanlänkade finansiella processer.

Vid tillämpning av första stycket led e ska processen för hantering av IKT-förändringar godkännas av lämpliga ledningsnivåer och ska ha särskilda protokoll på plats

Artikel 10

Upptäckt

1. Finansiella entiteter ska ha mekanismer för att snabbt upptäcka onormal verksamhet i enlighet med artikel 17, inbegripet frågor som rör IKT-nätverkens prestanda och IKT-relaterade incidenter, och för att identifiera potentiella väsentliga systemkritiska felpunkter (*single points of failure*).

Alla upptäcktsmekanismer som avses i första stycket ska testas regelbundet i enlighet med artikel 25.

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

3. Finansiella entiteter ska avsätta tillräckligt med resurser och kapacitet för att övervaka användarnas verksamhet, förekomsten av IKT-avvikelser och IKT-relaterade incidenter, särskilt cyberangrepp.

4. Leverantörer av datarapporteringstjänster 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 dessa rapporter.

Artikel 11

Åtgärder och återställande

1. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 och baserat på identifieringskraven i artikel 8 ska finansiella entiteter införa en heltäckande IKT-kontinuitetspolicy, vilken kan antas som en särskild specifik plan och utgöra en integrerad del av den finansiella entitetens övergripande kontinuitetsplan.

2. Finansiella entiteter ska genomföra IKT-kontinuitetspolicyn genom särskilda, lämpliga och dokumenterade arrangemang, planer, förfaranden och mekanismer som syftar till att

a) säkerställa kontinuiteten i den finansiella entitetens kritiska eller viktiga funktioner,

b) snabbt, lämpligt och effektivt reagera på och lösa alla IKT-relaterade incidenter på ett sätt som begränsar skador och prioriterar återupptagandet av verksamhet och återställningsåtgärder,

c) 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 12,

d) beräkna preliminära effekter, skador och förluster,

e) fastställa kommunikations- och krishanteringsinsatser som säkerställer att uppdaterad information överförs till all berörd intern personal och alla externa berörda parter i enlighet med artikel 14 och rapportera till behöriga myndigheter i enlighet med artikel 19.

3. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter genomföra åtföljande åtgärds- och återställningsplaner avseende IKT som, när det gäller andra finansiella entiteter än mikroföretag, ska bli föremål för oberoende interna granskningar.

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

5. Finansiella entiteter ska som en del av sin övergripande IKT-kontinuitetspolicy genomföra en verksamhetskonsekvensanalys av hur exponerade de är mot allvarliga störningar i verksamheten. I verksamhetskonsekvensanalysen ska finansiella entiteter bedöma vilka potentiella följder som allvarliga störningar i verksamheten kan få genom kvantitativa och kvalitativa kriterier och med hjälp av interna och externa data och scenarioanalys, beroende på vad som är lämpligt. I verksamhetskonsekvensanalysen ska hänsyn tas till kritikaliteten i de identifierade och kartlagda affärsfunktionerna, stödprocesserna, tredjepartsberoendena och informationstillgångarna, samt deras ömsesidiga beroende. Finansiella entiteter ska säkerställa att IKT-tillgångarna och IKT-tjänsterna är utformade och används i full samstämmighet med verksamhetskonsekvensanalysen, särskilt vad gäller att i tillräcklig utsträckning säkerställa reservkapaciteten för alla kritiska komponenter.

6. Som en del av sin övergripande IKT-riskhantering ska finansiella entiteter

a) testa IKT-kontinuitetsplanerna och åtgärds- och återställningsplanerna avseende IKT för de IKT-system som stöder alla funktioner minst en gång per år samt i samband med omfattande ändringar av de IKT-system som stöder kritiska eller viktiga funktioner,

b) testa de kriskommunikationsplaner som har upprättats i enlighet med artikel 14.

Vid tillämpning av första stycket led a ska andra finansiella entiteter än mikroföretag i testplanerna inkludera scenarier för cyberangrepp 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 12.

Finansiella entiteter ska regelbundet se över sin IKT-kontinuitetspolicy och sina åtgärds- och återställningsplaner avseende IKT med hänsyn till resultatet av tester som har utförts i enlighet med första stycket och rekommendationer från revisionskontroller eller tillsynsgranskningar.

7. Andra finansiella entiteter än mikroföretag ska ha en krishanteringsfunktion som, om deras IKT-kontinuitetsplaner eller åtgärds- och återställningsplaner avseende IKT aktiveras, bland annat ska innehålla tydliga förfaranden för hantering av intern och extern kriskommunikation i enlighet med artikel 14.

8. Finansiella entiteter ska ha lättillgänglig dokumentation om den verksamhet som pågår före och under avbrott när deras IKT-kontinuitetsplaner och åtgärds- och återställningsplaner avseende IKT aktiveras.

9. Värdepapperscentraler ska förse de behöriga myndigheterna med kopior av resultatet av IKT-kontinuitetstesterna eller liknande övningar.

10. Andra finansiella entiteter än mikroföretag ska på begäran till de behöriga myndigheterna lämna en uppskattning av de totala årliga kostnader och förluster som orsakas av allvarliga IKT-relaterade incidenter.

11. I enlighet med artikel 16 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 ska de europeiska tillsynsmyndigheterna genom den gemensamma kommittén senast den 17 juli 2024 utarbeta gemensamma riktlinjer om uppskattningen av de totala årliga kostnaderna och förlusterna som avses i punkt 10.

Artikel 12

Strategier och förfaranden för säkerhetskopiering och förfaranden och metoder för återskapande och återställning

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

a) strategier och förfaranden för säkerhetskopiering där de anger omfattningen av de data som ska säkerhetskopieras och minimifrekvensen för säkerhetskopieringen, baserat på informationens kritikalitet eller uppgifternas konfidentialitetsnivå,

b) förfaranden och metoder för återskapande och återställning.

2. Finansiella entiteter ska skapa säkerhetskopieringssystem som kan aktiveras i enlighet med strategierna och förfarandena för säkerhetskopiering samt med förfarande och metoder för återskapande och återställning. Aktiveringen av säkerhetskopieringssystem får inte äventyra säkerheten i nätverks- och informationssystemen eller datans tillgänglighet, äkthet, integritet eller konfidentialitet. Testning av säkerhetskopieringsförfarandena och förfarande och metoder för återskapande och återställning och metoderna ska genomföras regelbundet.

3. När finansiella entiteter återställer säkerhetskopierade data med hjälp av egna system ska de använda IKT-system som är fysiskt och logiskt segregerade från det IKT-system som är källan. IKT-systemen ska ha ett säkert skydd mot obehörig åtkomst eller IKT-förvanskning och medge ett snabbt återupptagande av tjänster, med hjälp av säkerhetskopior av data och system efter behov.

För centrala motparter 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.

Leverantörer av datarapporteringstjänster ska dessutom ha tillräckliga resurser och ha anläggningar för säkerhetskopiering och återskapande, så att de alltid kan erbjuda och upprätthålla sina tjänster.

4. Andra finansiella entiteter än mikroföretag ska upprätthålla IKT-reservkapacitet med resurser, förmåga och funktioner som är adekvata för att säkerställa verksamhetens behov. Mikroföretag ska bedöma behovet av att upprätthålla sådan IKT-reservkapacitet med utgångspunkt i vilken riskprofil de har.

5. Värdepapperscentraler ska ha minst ett sekundärt driftsställe med adekvata resurser, kapacitet, funktioner och personalarrangemang för att säkerställa 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 åtskild riskprofil och hindrar det från att påverkas av den händelse som påverkar det primära driftsstället,

b) kunna säkra driftskontinuiteten i kritiska eller viktiga funktioner som är identiska med det primära driftsstället eller tillhandahålla den servicenivå som är nödvändig för att säkerställa att den finansiella entiteten kan bedriva sin kritiska verksamhet inom ramen för återställningsmålen,

c) vara omedelbart tillgängligt för den finansiella entitetens personal i syfte att säkra driftskontinuitet i dess kritiska eller viktiga funktioner om det primära driftsstället inte är tillgängligt.

6. När finansiella entiteter fastställer återställningstid och återställningspunktmål för varje funktion ska de ta hänsyn till huruvida det är en kritisk eller viktig funktion och den eventuella övergripande inverkan på marknadseffektiviteten. Tidsmålen ska säkerställa att de överenskomna servicenivåerna uppnås i extrema scenarier.

7. När finansiella entiteter återställer verksamheten efter en IKT-relaterad incident ska de göra nödvändiga kontroller, inbegripet flera kontroller och 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 13

Lärande och utveckling

1. Finansiella entiteter ska ha lämplig kapacitet och personal för att samla in information om sårbarheter och cyberhot, IKT-relaterade incidenter, särskilt cyberangrepp, och analysera vilken inverkan de kan förmodas ha på den digitala operativa motståndskraften.

2. Finansiella entiteter ska införa efterhandsöversyner av IKT-relaterade incidenter efter det att en allvarlig IKT-relaterad incident medför ett avbrott i kärnverksamheten, så att orsakerna till avbrotten kan analyseras och nödvändiga förbättringar av IKT-verksamheten eller i den IKT-kontinuitetspolicy som avses i artikel 11 identifieras.

Andra finansiella entiteter än mikroföretag ska på begäran till de behöriga myndigheterna meddela vilka ändringar som genomfördes efter de efterhandsöversyner av IKT-relaterade incidenter som avses i första stycket.

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, om så är lämpligt,

c) incidenteskaleringens effektivitet inom den finansiella entiteten,

d) effektiviteten i intern och extern kommunikation.

3. Lärdomar av den testning av digital operativ motståndskraft som har utförts i enlighet med artiklarna 26 och 27 och av verkliga IKT-relaterade incidenter, särskilt cyberangrepp, samt utmaningar i samband med aktivering av IKT-kontinuitetsplaner och åtgärds- och återställningsplaner avseende IKT och relevant information som har utväxlats med motparter och bedömts under tillsynsgranskningar, ska införlivas fortlöpande i IKT-riskbedömningsprocessen. Dessa resultat ska utgöra en grund för lämpliga översyner av relevanta delar i den IKT-riskhanteringsram som avses i artikel 6.1.

4. Finansiella entiteter ska övervaka effektiviteten i genomförandet av den strategi för digital operativ motståndskraft som anges i artikel 6.8. De ska kartlägga IKT-riskens utveckling över tid, analysera IKT-relaterade incidenters frekvens, typ, omfattning och utveckling, särskilt cyberangrepp och deras mönster, i syfte att förstå graden av IKT-riskexponering, särskilt när det gäller kritiska eller viktiga funktioner, och öka den finansiella entitetens cybermognad och cyberberedskap.

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

6. Finansiella entiteter ska utarbeta program för medvetenhet om IKT-säkerhet och utbildning om digital operativ motståndskraft som obligatoriska moduler i sina personalutbildningsprogram. Dessa program och utbildningar ska gälla för alla anställda och personer i ledande ställning, och deras komplexitet ska motsvara behörigheten för personens roll. När så är lämpligt ska finansiella entiteter också inkludera tredjepartsleverantörer av IKT-tjänster i sina relevanta utbildningar, i enlighet med artikel 30.2 i.

7. Andra finansiella entiteter än mikroföretag 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 bekämpa nuvarande eller nya former av cyberangrepp.

Artikel 14

Kommunikation

1. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter ha kriskommunikationsplaner som gör det möjligt att på ett ansvarsfullt sätt informera kunder och motparter samt allmänheten om åtminstone allvarliga IKT-relaterade incidenter eller sårbarheter, beroende på vad som är lämpligt.

2. Som en del av IKT-riskhanteringsramen ska finansiella entiteter genomföra kommunikationsstrategier för intern 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 personalen med ansvar för åtgärder och återställande, och personal som behöver information.

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

Artikel 15

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

De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa), utarbeta gemensamma förslag till tekniska standarder för tillsyn i syfte att

a) närmare specificera delar som ska ingå i de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i syfte att säkerställa säkerheten i nätverk, möjliggöra lämpliga skyddsåtgärder mot intrång och missbruk av uppgifter, bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet, inbegripet krypteringsmetoder, och garantera en korrekt och snabb dataöverföring utan allvarliga avbrott och onödiga dröjsmål,

b) utveckla ytterligare komponenter i den hantering av kontroll av åtkomsträttigheter som avses i artikel 9.4 c och tillhörande personalpolitik där det specificeras åtkomsträttigheter, förfaranden för beviljande och återkallande av rättigheter, övervakning av onormalt beteende i förhållande till IKT-risk genom lämpliga indikatorer, inbegripet mönster för nätanvändning, tidpunkter, it-verksamhet och okänd utrustning,

c) vidareutveckla de mekanismer som anges i artikel 10.1 för att möjliggöra en snabb upptäckt av onormal verksamhet och de kriterier som fastställs i artikel 10.2 som utlöser processer för upptäckt och hantering av IKT-relaterade incidenter,

d) närmare specificera komponenterna i den IKT-kontinuitetspolicy som avses i artikel 11.1,

e) närmare specificera de tester av IKT-kontinuitetsplaner som avses i artikel 11.6 för att säkerställa att det vid sådan testning tas tillräckligt stor hänsyn 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,

f) närmare specificera komponenterna i de åtgärds- och återställningsplaner avseende IKT som avses i artikel 11.3,

g) närmare specificera innehållet i och formatet för den rapport om översynen av IKT-riskhanteringsramen som avses i artikel 6.5.

När de europeiska tillsynsmyndigheterna utarbetar dessa förslag till tekniska standarder för tillsyn ska de beakta den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser, samtidigt som vederbörlig hänsyn tas till eventuella särdrag som härrör från den särskilda karaktären på verksamheten i olika sektorer för finansiella tjänster.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 januari 2024.

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 1094/2010 och (EU) nr 1095/2010.

Artikel 16

Förenklad IKT-riskhanteringsram

1. Artiklarna 5–15 i denna förordning ska inte tillämpas på små och icke-sammanlänkade värdepappersföretag, betalningsinstitut undantagna enligt direktiv (EU) 2015/2366, institut undantagna enligt direktiv 2013/36/EU och för vilka medlemsstaterna har beslutat att inte tillämpa den möjlighet som anges i artikel 2.4 i denna förordning; institut för elektroniska pengar undantagna enligt direktiv 2009/110/EG och små tjänstepensionsinstitut.

Utan att det påverkar tillämpningen av första stycket ska de enheter som förtecknas i första stycket

a) inrätta och upprätthålla en sund och dokumenterad IKT-riskhanteringsram som specificerar de mekanismer och åtgärder som syftar till att ge en snabb, effektiv och heltäckande hantering av IKT-risk, inbegripet vad gäller skyddet av relevanta fysiska komponenter och infrastrukturer,

b) kontinuerligt övervaka alla IKT-systems säkerhet och funktion,

c) minimera effekterna av IKT-risk genom användningen av sunda, motståndskraftiga och uppdaterade IKT-system, IKT-protokoll och IKT-verktyg som lämpar sig för att stödja utförandet av verksamheten och tillhandahållandet av tjänster och på ett tillräckligt sätt skydda konfidentialitet, tillgänglighet, integritet eller äkthet hos datan i nätverks- och informationssystemen,

d) göra det möjligt att snabbt identifiera och upptäcka IKT-risk och avvikelser i nätverks- och informationssystemen och att snabbt hantera IKT-relaterade incidenter,

e) identifiera de viktigaste beroendena av tredjepartsleverantörer av IKT-tjänster,

f) säkerställa kontinuiteten för kritiska eller viktiga funktioner genom kontinuitetsplaner och åtgärds- och återställnings-åtgärder, vilket bland annat innefattar säkerhetskopiering och återskapande,

g) regelbundet testa de planer och åtgärder som avses i led f, samt effektiviteten i de kontroller som genomförts i enlighet med leden a och c,

h) i enlighet med vad som är lämpligt genomföra relevanta operativa slutsatser som härrör från de test som avses i led g och från efteranalyser av incidenter i IKT-riskbedömningsprocessen, och utifrån behoven och IKT-riskprofilen utarbeta program för medvetenhet om IKT-säkerhet och utbildning om digital operativ motståndskraft för personal och ledning.

2. Den IKT-riskhanteringsram som avses i punkt 1 andra stycket a, ska dokumenteras och ses över regelbundet och vid uppkomsten av allvarliga IKT-relaterade incidenter, i enlighet med tillsynsinstruktionerna. Ramen ska förbättras fortlöpande baserat på erfarenheterna från genomförande och övervakning. En rapport om översynen av IKT-riskhanteringsramen ska överlämnas till den behöriga myndigheten på dess begäran.

3. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med Enisa, utarbeta gemensamma förslag till tekniska standarder för tillsyn i syfte att

a) närmare specificera vilka komponenter som ska ingå i den IKT-riskhanteringsram som avses i punkt 1 andra stycket a,

b) närmare specificera komponenterna i förhållande till system, protokoll och verktyg för att minimera effekterna av IKT-risk som avses i punkt 1 andra stycket c, i syfte att säkerställa säkerheten i nätverken, möjliggöra lämpliga skyddsåtgärder mot intrång och missbruk av data och bevara datans tillgänglighet, äkthet, integritet och konfidentialitet,

c) närmare specificera komponenterna i de IKT-kontinuitetsplaner som avses i punkt 1 andra stycket f,

d) närmare specificera reglerna för testningen av kontinuitetsplanerna och säkerställa att de kontroller som avses i punkt 1 andra stycket g är effektiva, och säkerställa att det vid sådan testning tas tillräckligt stor hänsyn till scenarier där kvaliteten på tillhandahållandet av en kritisk eller viktig funktion försämras till en oacceptabel nivå eller tillhandahållandet avbryts,

e) närmare specificera innehållet i och formatet för den rapport om översynen av IKT-riskhanteringsramen som avses i punkt 2.

När de europeiska tillsynsmyndigheterna utarbetar dessa förslag till tekniska standarder för tillsyn ska de ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 januari 2024.

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 1094/2010 och (EU) nr 1095/2010.

KAPITEL III

Hantering av, klassificering av och rapportering om IKT-relaterade incidenter

Artikel 17

Process för hantering av IKT-relaterade incidenter

1. Finansiella entiteter ska fastställa, inrätta och genomföra en process för hantering av IKT-relaterade incidenter för att upptäcka, hantera och rapportera IKT-relaterade incidenter.

2. Finansiella entiteter ska registrera alla IKT-relaterade incidenter och betydande cyberhot. Finansiella entiteter ska inrätta lämpliga förfaranden och processer för att säkerställa en konsekvent och integrerad övervakning, hantering och uppföljning av IKT-relaterade incidenter, för att säkerställa att grundorsakerna identifieras, dokumenteras och åtgärdas i syfte att förhindra att sådana incidenter inträffar.

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

a) införa indikatorer för tidig varning,

b) innehålla fastställda förfaranden för att identifiera, spåra, logga, kategorisera och klassificera IKT-relaterade incidenter enligt deras prioritetsordning och allvar och enligt de berörda tjänsternas kritikalitet i enlighet med de kriterier som fastställs i artikel 18.1,

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

d) innehålla planer för kommunikation till personal, externa berörda parter och medier i enlighet med artikel 14 och för anmälan till kunder, för interna eskaleringsförfaranden, inbegripet IKT-relaterade kundklagomål, samt för tillhandahållande av information till finansiella entiteter som fungerar som motparter, beroende på vad som är lämpligt,

e) säkerställa att åtminstone allvarliga IKT-relaterade incidenter rapporteras till relevant senior ledning och att ledningsorganet informeras om åtminstone allvarliga IKT-relaterade incidenter, med en förklaring av effekter, åtgärder och ytterligare kontroller som ska fastställas till följd av sådana IKT-relaterade incidenter,

f) 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 18

Klassificering av IKT-relaterade incidenter och cyberhot

1. Finansiella entiteter ska klassificera IKT-relaterade incidenter och fastställa deras inverkan baserat på följande kriterier:

a) Antalet och/eller betydelsen av kunder eller finansiella motparter som påverkas, och i tillämpliga fall, mängden eller antalet transaktioner som påverkas 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, vad gäller tillgänglighet, äkthet, integritet eller konfidentialitet vad gäller datan

e) De berörda tjänsternas kritikalitet, inbegripet den finansiella entitetens transaktioner och verksamhet.

f) De ekonomiska effekterna, särskilt direkta och indirekta kostnader och förluster, av den IKT-relaterade incidenten i absoluta och relativa tal.

2. Finansiella entiteter ska klassificera cyberhot som betydande baserat på de hotade tjänsternas kritikalitet, inbegripet den finansiella entitetens transaktioner och verksamhet, antalet och/eller betydelsen av kunder eller finansiella motparter som hotas och den geografiska spridningen av de hotade områdena.

3. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med 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 allvarliga IKT-relaterade incidenter eller, i tillämpliga fall, allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, som omfattas av rapporteringsskyldigheten i artikel 19.1.

b) De kriterier som de behöriga myndigheterna ska tillämpa för att bedöma allvarliga IKT-relaterade incidenters eller, i tillämpliga fall, allvarliga betalningsrelaterade operativa incidenters eller säkerhetsincidenters relevans för de relevanta behöriga myndigheterna i andra medlemsstater och de detaljer i rapporter om allvarliga IKT-relaterade incidenter eller, i tillämpliga fall, allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter som ska delas med andra behöriga myndigheter enligt artikel 19.6 och 19.7.

c) De kriterier som anges i punkt 2 i denna artikel, inbegripet höga väsentlighetströsklar för att fastställa betydande cyberhot.

4. När de europeiska tillsynsmyndigheterna utarbetar de gemensamma förslag till tekniska standarder för tillsyn som avses i punkt 3 i denna artikel ska de ta hänsyn till kriterierna i artikel 4.2 samt internationella standarder, riktlinjer och specifikationer som har utarbetats och offentliggjorts av Enisa, inbegripet, när så är lämpligt, specifikationer för andra ekonomiska sektorer. Vid tillämpningen av kriterierna i artikel 4.2 ska de europeiska tillsynsmyndigheterna vederbörligen beakta behovet av att mikroföretag och små och medelstora företag mobiliserar tillräckliga resurser och tillräcklig kapacitet för att säkerställa att IKT-relaterade incidenter hanteras snabbt.

De europeiska tillsynsmyndigheterna ska överlämna dessa gemensamma förslag till tekniska standarder för tillsyn till kommissionen senast den 17 januari 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i punkt 3 i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 19

Rapportering av allvarliga IKT-relaterade incidenter och frivillig anmälan av betydande cyberhot

1. Finansiella entiteter ska rapportera allvarliga IKT-relaterade incidenter till den relevanta behöriga myndighet som avses i artikel 46 i enlighet med punkt 4 i den här artikeln.

Om en finansiell entitet är föremål för tillsyn av mer än en sådan nationell behörig myndighet som avses i artikel 46 ska medlemsstaterna utse en enda behörig myndighet till relevant behörig myndighet med ansvar för att utföra de funktioner och skyldigheter som föreskrivs i denna artikel.

Kreditinstitut som klassificeras som betydande i enlighet med artikel 6.4 i förordning (EU) nr 1024/2013 ska rapportera allvarliga IKT-relaterade incidenter till den relevanta nationella behöriga myndighet som utsetts i enlighet med artikel 4 i direktiv 2013/36/EU, och myndigheten ska omedelbart översända den rapporten till ECB.

Vid tillämpning av första stycket ska finansiella entiteter, efter att ha samlat in och analyserat all relevant information, utarbeta den första anmälan och de rapporter som avses i punkt 4 i denna artikel med hjälp av de mallar som avses i artikel 20 och överlämna dem till den behöriga myndigheten. Om det visar sig vara tekniskt omöjligt att överföra den första anmälan med hjälp av mallen ska finansiella entiteter anmäla till den behöriga myndigheten på annat vis.

Den första anmälan och de rapporter som avses i punkt 4 ska innehålla all information som är nödvändig för att den behöriga myndigheten ska kunna fastställa betydelsen av den allvarliga IKT-relaterade incidenten och bedöma eventuella gränsöverskridande konsekvenser.

Utan att det påverkar den finansiella entitetens rapportering enligt första stycket till den relevanta behöriga myndigheten får medlemsstaterna även besluta att vissa eller alla finansiella entiteter dessutom till den första anmälan och de rapporter som avses i punkt 4 i denna artikel ska använda de mallar som avses i artikel 20 när de överlämnar anmälan och rapporterna till de behöriga myndigheterna eller de CSIRT-enheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555.

2. Finansiella entiteter får på frivillig basis rapportera betydande cyberhot till den relevanta behöriga myndigheten, när de anser att hotet är relevant för det finansiella systemet, tjänsteanvändarna eller kunderna. Den relevanta behöriga myndigheten får lämna sådan information till de andra relevanta myndigheter som avses i punkt 6.

Kreditinstitut som klassificeras som betydande i enlighet med artikel 6.4 i förordning (EU) nr 1024/2013 får på frivillig basis rapportera betydande cyberhot till den relevanta nationella behöriga myndighet som utsetts i enlighet med artikel 4 i direktiv 2013/36/EU, och myndigheten ska omedelbart översända den anmälan till ECB.

Medlemsstaterna får fastställa att de finansiella entiteter som rapporterar på frivillig basis i enlighet med första stycket också får vidarebefordra den anmälan till de CSIRT-enheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555.

3. Om en allvarlig IKT-relaterad incident inträffar och påverkar kunders ekonomiska intressen ska finansiella entiteter utan onödigt dröjsmål så snart de blir medvetna om den informera sina kunder om den allvarliga IKT-relaterade incidenten och om de åtgärder som har vidtagits för att mildra de negativa effekterna av en sådan incident.

I händelse av ett betydande cyberhot ska finansiella entiteter, i tillämpliga fall, informera de kunder som kan påverkas om alla lämpliga skyddsåtgärder som de sistnämnda kan överväga att vidta.

4. Finansiella entiteter ska, inom de tidsfrister som ska fastställas i enlighet med artikel 20 första stycket a ii, lämna följande till den relevanta behöriga myndigheten:

a) En första anmälan.

b) En delrapport efter den första anmälan som avses i led a, så snart statusen för den ursprungliga incidenten har förändrats avsevärt eller hanteringen av den allvarliga IKT-relaterade incidenten har förändrats på grund av ny tillgänglig information, när så är lämpligt 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, och när de faktiska påverkanssiffrorna finns tillgängliga för att ersätta uppskattningar.

5. Finansiella entiteter får i enlighet med unionsrätten och nationell rätt på området utkontraktera rapporteringsskyldigheterna enligt denna artikel till en tredjepartsleverantör av tjänster. Vid sådan utkontraktering bär den finansiella entiteten det fulla ansvaret för efterlevnaden av incidentrapporteringskraven.

6. Efter mottagandet av den första anmälan och av varje rapport som avses i punkt 4 ska den behöriga myndigheten skyndsamt lämna närmare uppgifter om den allvarliga IKT-relaterade incidenten till följande mottagare, i tillämpliga fall på grundval av deras respektive behörigheter:

a) EBA, Esma eller Eiopa,

b) ECB när det gäller de finansiella entiteter som avses i artikel 2.1 a, b och d,

c) de behöriga myndigheter, de gemensamma kontaktpunkter eller de CSIRT-enheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555,

d) de resolutionsmyndigheter som avses i artikel 3 i direktiv 2014/59/EU och den gemensamma resolutionsnämnden när det gäller sådana enheter som avses i artikel 7.2 i Europaparlamentets och rådets förordning (EU) nr 806/2014 ([37]) och när det gäller sådana enheter och koncerner som avses i artikel 7.4 b och 7.5 i förordning (EU) nr 806/2014 om sådana detaljer gäller incidenter som utgör en risk för säkerställandet av kritiska funktioner i den mening som avses i artikel 2.1.35 i direktiv 2014/59/EU, och

e) andra relevanta offentliga myndigheter enligt nationell rätt.

7. Efter att ha mottagit information i enlighet med punkt 6 ska EBA, Esma eller Eiopa och ECB, i samråd med Enisa och i samarbete med den relevanta behöriga myndigheten, bedöma huruvida den allvarliga IKT-relaterade incidenten är relevant för behöriga myndigheter i andra medlemsstater. Efter denna bedömning ska EBA, Esma eller Eiopa så snart som möjligt underrätta de relevanta behöriga myndigheterna i andra medlemsstater i ärendet. ECB ska underrätta medlemmarna i Europeiska centralbankssystemet om frågor som är relevanta för betalningssystemet. Baserat på denna underrättelse ska de behöriga myndigheterna vid behov vidta alla nödvändiga åtgärder för att skydda det finansiella systemets omedelbara stabilitet.

([37]) Europaparlamentets och rådets förordning (EU) nr 806/2014 av den 15 juli 2014 om fastställande av enhetliga regler och ett enhetligt förfarande för resolution av kreditinstitut och vissa värdepappersföretag inom ramen för en gemensam resolutionsmekanism och en gemensam resolutionsfond och om ändring av förordning (EU) nr 1093/2010 (EUT L 225, 30.7.2014, s. 1).

8. Den anmälan som Esma ska göra enligt punkt 7 i denna artikel ska inte påverka den behöriga myndighetens skyldighet att skyndsamt översända uppgifterna om den allvarliga IKT-relaterade incidenten till den relevanta myndigheten i värdmedlemsstaten, om en värdepapperscentral har betydande gränsöverskridande verksamhet i värdmedlemsstaten, om den allvarliga IKT-relaterade incidenten sannolikt kommer att medföra allvarliga konsekvenser för finansmarknaderna i värdmedlemsstaten och om det finns samarbetsarrangemang mellan behöriga myndigheter som gäller tillsynen av finansiella entiteter.

Artikel 20

Harmonisering av rapporteringsinnehåll och mallar

De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med Enisa och ECB, utarbeta

a) gemensamma förslag till tekniska standarder för tillsyn för att

   i) fastställa innehållet i rapporterna om allvarliga IKT-relaterade incidenter, för att återspegla de kriterier som fastställts i artikel 18.1 och införliva ytterligare beståndsdelar, såsom detaljerna för att fastställa huruvida rapporteringen är relevant för andra medlemsstater och huruvida det utgör en allvarliga betalningsrelaterad operativ incident eller säkerhetsincident eller inte,

   ii) fastställa tidsfristerna för den första anmälan och för varje rapport som avses i artikel 19.4,

   iii) fastställa innehållet i anmälan om betydande cyberhot.

   Vid utarbetandet av dessa förslag till tekniska standarder för tillsyn ska de europeiska tillsynsmyndigheterna ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil samt karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser, särskilt för att säkerställa att olika tidsfrister för tillämpningen av detta stycke led a ii, beroende på vad som är lämpligt, kan återspegla de finansiella sektorernas särdrag, utan att det påverkar upprätthållandet av en enhetlig strategi för IKT-relaterad incidentrapportering enligt denna förordning och i direktiv (EU) 2022/2555. De europeiska tillsynsmyndigheterna ska, beroende på vad som är tillämpligt, lämna en motivering när de avviker från de metoder som tillämpas inom ramen för det direktivet.

b) gemensamma förslag till tekniska standarder för genomförande i syfte att fastställa standardformulär, mallar och förfaranden för finansiella entiteter för rapportering av en allvarlig IKT-relaterad incident eller anmälan av ett betydande cyberhot.

De europeiska tillsynsmyndigheterna ska överlämna de gemensamma förslag till tekniska standarder för tillsyn som avses i första stycket a och de gemensamma förslag till tekniska genomförandestandarder som avses i första stycket b till kommissionen senast den 17 juli 2024.

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

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

Artikel 21

Centralisering av rapportering av allvarliga 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 entiteters rapportering av allvarliga IKT-relaterade incidenter. Den gemensamma 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 gemensamma rapport som avses i punkt 1 ska innehålla minst följande:

a) Förutsättningar för att inrätta en gemensam EU-knutpunkt.

b) Fördelar, begränsningar och risker, inbegripet risker förknippade med hög koncentration av känslig information.

c) Nödvändig kapacitet för att säkerställa interoperabilitet med andra relevanta rapporteringssystem.

d) Inslag i den operativa förvaltningen.

e) Villkor för medlemskap.

f) Tekniska arrangemang för att finansiella entiteter och nationella behöriga myndigheter ska få tillgång till den gemensamma EU-knutpunkten.

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

3. De europeiska tillsynsmyndigheterna ska överlämna den rapport som avses i punkt 1 till Europaparlamentet, rådet och kommissionen senast den 17 januari 2025.

Artikel 22

Återkoppling från tillsynsmyndigheterna

1. Utan att det påverkar de tekniska uppgifterna, råden eller åtgärderna och efterföljande uppföljning, som i tillämpliga fall kan tillhandahållas i enlighet med nationell rätt, av CSIRT-enheterna enligt direktiv (EU) 2022/2555, ska den behöriga myndigheten, efter mottagandet av den första anmälan och av varje rapport som avses i artikel 19.4, bekräfta mottagandet och får, när så är möjligt, skyndsamt tillhandahålla relevant och proportionell återkoppling eller vägledning på hög nivå till den finansiella entiteten, särskilt genom att göra tillgänglig all eventuell relevant anonymiserad information och underrättelser om liknande hot, och får diskutera åtgärder som tillämpas på finansiell entitetsnivå, och sätt att minimera och mildra de negativa effekterna i den finansiella sektorn. Utan att det påverkar den återkoppling som mottagits från tillsynsmyndigheterna ska finansiella entiteter förbli fullt ansvariga för hanteringen av och konsekvenserna av IKT-relaterade incidenter som rapporteras enligt artikel 19.1.

2. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén årligen lämna anonymiserade och aggregerade rapporter om allvarliga IKT-relaterade incidenter, vars detaljer ska komma från behöriga myndigheter i enlighet med artikel 19.6, med angivande av åtminstone antalet allvarliga IKT-relaterade incidenter och deras art, inverkan på finansiella entiteters eller kunders verksamhet, vidtagna avhjälpande åtgärder och uppkomna kostnader.

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

Artikel 23

Betalningsrelaterade operativa incidenter eller säkerhetsincidenter som gäller kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar

De krav som fastställs i detta kapitel ska också tillämpas på betalningsrelaterade operativa incidenter eller säkerhetsincidenter och på allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, om de gäller kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar.

KAPITEL IV

Testning av digital operativ motståndskraft

Artikel 24

Allmänna krav för testning av digital operativ motståndskraft

1. För att bedöma beredskapen för hantering av IKT-relaterade incidenter, identifiera svagheter, brister och luckor i den digitala operativa motståndskraften och snabbt genomföra korrigerande åtgärder ska andra finansiella entiteter än mikroföretag, med hänsyn till de kriterier som fastställs i artikel 4.2, 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 6.

2. Programmet för testning av digital operativ motståndskraft ska omfatta en rad bedömningar, tester, metoder, praxis och verktyg som ska tillämpas i enlighet med artiklarna 25 och 26.

3. När andra finansiella entiteter än mikroföretag genomför det testprogram för digital operativ motståndskraft som avses i punkt 1 i denna artikel ska de följa en riskbaserad metod med hänsyn tagen till kriterierna i artikel 4.2 med vederbörligt beaktande av IKT-riskens utveckling, eventuella specifika risker som den berörda finansiella entiteten är eller kan bli exponerad för, kritikaliteten hos informationstillgångar och tillhandahållna tjänster samt varje annan faktor som den finansiella entiteten anser lämplig.

4. Andra finansiella entiteter än mikroföretag ska se till att testerna utförs av oberoende parter, oavsett om de är interna eller externa. När tester utförs av en intern testare ska finansiella entiteter avsätta tillräckliga resurser och säkerställa att intressekonflikter kan undvikas under testets utformning och genomförande.

5. Andra finansiella entiteter än mikroföretag ska fastställa förfaranden och strategier för prioritering, klassificering och åtgärdande av alla problem som visar sig under genomförandet av testerna och ska införa interna valideringsmetoder för att säkerställa att alla identifierade svagheter, brister eller luckor åtgärdas fullt ut.

6. Andra finansiella entiteter än mikroföretag ska säkerställa, åtminstone årligen, att lämpliga tester utförs på alla IKT-system och IKT-tillämpningar som stöder kritiska eller viktiga funktioner.

Artikel 25

Testning av IKT-verktyg och IKT-system

1. Det program för testning av digital operativ motståndskraft som avses i artikel 24 ska, i enlighet med kriterierna i artikel 4.2, innehålla bestämmelser om utförande av lämpliga tester, såsom sårbarhetsanalyser och skanningar, analyser av öppen källkod, nätverkssäkerhetsbedömningar, gapanalyser, fysiska säkerhetsgranskningar, frågeformulär och programvarulösningar för skanning, källkodsgranskningar när så är möjligt, scenariobaserade tester, kompatibilitetstester, prestandatester, tester ändpunkt till ändpunkt (end-to-end) och penetrationstester.

2. Värdepapperscentraler och centrala motparter ska utföra sårbarhetsbedömningar före eventuellt införande eller återinförande av nya eller befintliga tillämpningar och infrastrukturkomponenter, och IKT-tjänster som stöder den finansiella entitetens kritiska eller viktiga funktioner,.

3. Mikroföretag ska utföra de tester som avses i punkt 1 genom att kombinera en riskbaserad metod med strategisk planering av IKT-testning, genom att vederbörligen beakta behovet av att upprätthålla en balans mellan å ena sidan omfattningen av de resurser och den tid som ska avsättas för IKT-testning som föreskrivs i denna artikel och å andra sidan skyndsamheten, typen av risk, kritikaliteten hos informationstillgångarna och de tillhandahållna tjänsterna samt alla andra relevanta faktorer, inbegripet den finansiella entitetens förmåga att ta beräknade risker.

Artikel 26

Avancerad testning av IKT-verktyg, IKT-system och IKT-processer baserad på hotbildsstyrd penetrationstestning

1. Andra finansiella entiteter än de entiteter som avses i artikel 16.1 första stycket och mikroföretag, vilka har identifierats i enlighet med punkt 8 tredje stycket i den här artikeln ska minst vart tredje år genomföra avancerade tester med hjälp av hotbildsstyrd penetrationstestning. Baserat på den finansiella entitetens riskprofil och med beaktande av de operativa omständigheterna får den behöriga myndigheten vid behov begära att den finansiella entiteten minskar eller ökar denna frekvens.

2. Varje hotbildsstyrt penetrationstest ska omfatta flera eller alla av en finansiell entitets kritiska eller viktiga funktioner och ska utföras på produktionssystem i drift som stöder sådana funktioner.

Finansiella entiteter ska identifiera alla relevanta underliggande IKT-system, IKT-processer och IKT-tekniker som stöder kritiska eller viktiga funktioner och IKT-tjänster, inbegripet de som stöder de kritiska eller viktiga funktioner som har utkontrakterats eller kontrakterats till tredjepartsleverantörer av IKT-tjänster.

Finansiella entiteter ska bedöma vilka kritiska eller viktiga funktioner som behöver omfattas av den hotbildsstyrda penetrationstestningen. Resultatet av denna bedömning ska fastställa den exakta omfattningen av den hotbildsstyrda penetrationstestningen och ska valideras av de behöriga myndigheterna.

3. Om tredjepartsleverantörer av IKT-tjänster omfattas av den hotbildsstyrda penetrationstestningen ska den finansiella entiteten vidta nödvändiga åtgärder och skyddsåtgärder för att säkerställa att sådana tredjepartsleverantörer av IKT-tjänster deltar i den hotbildsstyrda penetrationstestningen och ska alltid ha fullt ansvar för att säkerställa att denna förordning efterlevs.

4. Utan att det påverkar tillämpningen av punkt 2 första och andra styckena får den finansiella entiteten och en tredjepartsleverantör av IKT-tjänster, om tredjepartsleverantörens deltagande i den hotbildsstyrda penetrationstestningen som avses i punkt 3 kan förväntas få negativ inverkan på kvaliteten eller säkerheten för de tjänster som tredjepartsleverantören av IKT-tjänster tillhandahåller till kunder som är entiteter som inte omfattas av denna förordning, eller för konfidentialiteten för data som är relaterade till sådana tjänster, skriftligen enas om att tredjepartsleverantören av IKT-tjänster ingår avtal med en extern testare i syfte att, under ledning av en utsedd finansiell entitet, genomföra en gemensam hotbildsstyrd penetrationstestning med flera finansiella entiteter (gemensam testning) till vilka tredjepartsleverantören av IKT-tjänster tillhandahåller IKT-tjänster.

Den gemensamma testningen ska omfatta det relevanta spektrum av IKT-tjänster som stöder kritiska eller viktiga funktioner som de finansiella entiteterna har ingått avtal om med respektive tredjepartsleverantör av IKT-tjänster. Den gemensamma testningen ska betraktas som hotbildsstyrd penetrationstestning utförd av de finansiella entiteter som deltar i den gemensamma testningen.

Antalet finansiella entiteter som deltar i den gemensamma testningen ska vederbörligen kalibreras med beaktande av de berörda tjänsternas komplexitet och typ.

5. De finansiella entiteterna ska, i samarbete med tredjepartsleverantörer av IKT-tjänster och andra berörda parter, inbegripet testarna men exklusive de behöriga myndigheterna, tillämpa effektiva riskhanteringskontroller för att minska riskerna för möjliga effekter på data, skador på tillgångar och avbrott i kritiska eller viktiga funktioner, tjänster eller transaktioner hos den finansiella entiteten själv, dess motpart eller den finansiella sektorn.

6. När testet har avslutats och efter det att rapporter och åtgärdsplaner har godkänts ska den finansiella entiteten och, i tillämpliga fall, de externa testarna förse den myndighet som utsetts i enlighet med punkt 9 eller 10 med en sammanfattning av de relevanta resultaten, åtgärdsplanerna och dokumentation som visar att den hotbildsstyrda penetrationstestningen har utförts i enlighet med kraven.

7. Myndigheter ska förse finansiella entiteter med ett intyg som bekräftar att testet genomfördes i enlighet med kraven, vilket ska framgå av dokumentationen, i syfte att möjliggöra ömsesidigt erkännande av hotbildsstyrd penetrationstestning mellan behöriga myndigheter. Den finansiella entiteten ska underrätta den relevanta behöriga myndigheten om intyget, sammanfattningen av de relevanta resultaten och åtgärdsplanerna.

Utan att det påverkar tillämpligheten av ett sådant intyg ska de finansiella entiteterna alltid ha det fulla ansvaret för effekterna av de tester som avses i punkt 4.

8. Finansiella entiteter ska anlita testare i syfte att genomföra hotbildsstyrd penetrationstestning i enlighet med artikel 27. Om finansiella entiteter använder interna testare för att genomföra hotbildsstyrd penetrationstestning ska de anlita externa testare vid vart tredje test.

De kreditinstitut som klassificeras som betydande i enlighet med artikel 6.4 i förordning (EU) nr 1024/2013 ska endast använda externa testare i enlighet med artikel 27.1 a–e.

De behöriga myndigheterna ska identifiera de finansiella entiteter som är skyldiga att genomföra hotbildsstyrd penetrationstestning med beaktande av kriterierna i artikel 4.2, baserat på en bedömning av följande:

a) Påverkansfaktorer, särskilt i vilken utsträckning de tjänster som tillhandahålls och den verksamhet som bedrivs av den finansiella entiteten påverkar den finansiella sektorn.

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

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

9. Medlemsstaterna får utse en enda offentlig myndighet inom finanssektorn som ska ansvara för frågor som rör hotbildsstyrd penetrationstestning inom den finansiella sektorn på nationell nivå och ska ge myndigheten alla befogenheter och uppgifter i detta syfte.

10. Om det inte har utsetts någon myndighet i enlighet med punkt 9 i denna artikel, och utan att det påverkar befogenheten att välja ut vilka finansiella entiteter som är skyldiga att utföra hotbildsstyrd penetrationstestning, får en behörig myndighet delegera vissa eller alla av de uppgifter som avses i denna artikel och artikel 27 till en annan nationell myndighet inom den finansiella sektorn.

11. De europeiska tillsynsmyndigheterna ska, i samförstånd med ECB, utarbeta gemensamma förslag till tekniska standarder för tillsyn i enlighet med TIBER-EU-ramen i syfte att närmare specificera

a) de kriterier som används för tillämpningen av punkt 8 andra stycket,

b) kraven och standarderna för användning av interna testare

c) kraven i fråga om

   i) omfattningen av den hotbildsstyrda penetrationstestning som avses i punkt 2,

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

   iii) testningens resultat och avslutnings- och åtgärdsfaser,

d) den typ av tillsynssamarbete och annat relevant samarbete som krävs för genomförandet av hotbildsstyrd penetrationstestning och för underlättande av det ömsesidiga erkännandet av sådan testning när det gäller finansiella entiteter 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.

När de europeiska tillsynsmyndigheterna utvecklar dessa förslag till tekniska standarder för tillsyn ska de ta vederbörlig hänsyn till eventuella särdrag som härrör från den särskilda karaktären på verksamheten i olika sektorer för finansiella tjänster.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 juli 2024.

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 1094/2010 och (EU) nr 1095/2010.

Artikel 27

Krav för testare vid utförandet av hotbildsstyrd penetrationstestning

1. Finansiella entiteter ska endast utföra sådana testare för att utföra hotbildsstyrd penetrationstestning som

a) är allra bäst lämpade och har högst anseende,

b) har teknisk och organisatorisk kapacitet och uppvisar särskild sakkunskap om underrättelser om hot, penetrationstestning och red-team-testning,

c) har certifierats av ett ackrediteringsorgan i en medlemsstat eller ansluter sig till formella uppförandekoder eller etiska ramar,

d) lämnar en oberoende försäkran eller en revisionsberättelse om sund riskhantering i samband med utförandet av hotbildsstyrd penetrationstestning, inbegripet relevant skydd av den finansiella entitetens konfidentiella information och ersättning för den finansiella entitetens affärsrisker,

e) har en relevant och heltäckande ansvarsförsäkring som omfattar risker för fel och försummelser i yrkesutövningen.

2. Vid användandet av interna testare ska finansiella entiteter säkerställa att, utöver villkoren i punkt 1, följande villkor är uppfyllda:

a) Sådan användning av dem har godkänts av den relevanta behöriga myndigheten eller av den enda offentliga myndighet som utsetts i enlighet med artikel 26.9 och 26.10.

b) Den relevanta behöriga myndigheten har verifierat att den finansiella entiteten har avsatt tillräckliga resurser och säkerställt att intressekonflikter kan undvikas under testets utformning och genomförande.

c) Leverantören av underrättelser om hot är extern i förhållande till den finansiella entiteten.

3. Finansiella entiteter ska se till att avtal som ingås med externa testare innehåller krav på en sund förvaltning av resultaten av den hotbildsstyrda penetrationstestningen och att all databehandling av dem, inbegripet generering, lagring, aggregering, utkast, rapportering, kommunikation eller förstörelse, inte skapar risker för den finansiella entiteten.

KAPITEL V

Hantering av IKT-tredjepartsrisker

Avsnitt I

Huvudprinciper för en sund hantering av IKT-tredjepartsrisker

Artikel 28

Allmänna principer

1. Finansiella entiteter ska hantera IKT-tredjepartsrisker som en integrerad del av IKT-risken inom sin IKT-riskhanteringsram som avses i artikel 6.1, och i enlighet med följande principer:

a) De finansiella entiteter som har ingått ett kontraktsmässigt arrangemang om användningen av IKT-tjänster för att bedriva sin affärsverksamhet ska alltid ha det fulla ansvaret för uppfyllandet och fullgörandet av alla skyldigheter enligt denna förordning och tillämplig rätt avseende finansiella tjänster.

b) Finansiella entiteters hantering av IKT-tredjepartsrisker ska genomföras med hänsyn till proportionalitetsprincipen, med beaktande av

i) IKT-relaterade beroendens karaktär, omfattning, komplexitet och betydelse,

ii) 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 kritikaliteten eller betydelsen av respektive tjänst, process eller funktion, och den potentiella inverkan på kontinuiteten och tillgängligheten hos finansiella tjänster och verksamheter, på individuell nivå och på koncernnivå.

2. Som en del av sin IKT-riskhanteringsram ska andra finansiella entiteter än de enheter som avses i artikel 16.1 första stycket och mikroföretag anta och regelbundet se över en strategi för IKT-tredjepartsrisk, med beaktande av den strategi för flera olika leverantörer som avses i artikel 6.9 i tillämpliga fall. Strategin för IKT-tredjepartsrisk ska omfatta riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster och ska tillämpas individuellt och, i förekommande fall, på undergrupps- och gruppnivå. Ledningsorganet ska, baserat på en bedömning av den finansiella entitetens allmänna riskprofil samt omfattningen av och komplexiteten i entitetens affärstjänster, regelbundet se över de risker som har identifierats vad gäller kontraktsmässiga arrangemang för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner.

3. Som en del av sin IKT-riskhanteringsram ska finansiella entiteter upprätthålla och uppdatera ett register med information på entitetsnivå, 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.

Finansiella entiteter 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 IKT-tjänster och funktioner som tillhandahålls.

Finansiella entiteter 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 entiteten.

Finansiella entiteter ska i god tid informera den behöriga myndigheten om eventuella planerade kontraktsmässiga arrangemang för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner samt när en funktion har blivit kritisk eller viktig.

4. Innan finansiella entiteter ingår ett kontraktsmässigt arrangemang om användning av IKT-tjänster ska de

a) bedöma om det kontraktsmässiga arrangemanget omfattar användningen av IKT-tjänster som stöder 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 kontraktsmässiga arrangemang kan bidra till att förstärka IKT-koncentrationsrisken enligt artikel 29,

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.

5. Finansiella entiteter får endast ingå kontraktsmässiga arrangemang med tredjepartsleverantörer av IKT-tjänster som uppfyller lämpliga standarder för informationssäkerhet. När dessa kontraktsmässiga arrangemang gäller kritiska eller viktiga funktioner ska finansiella entiteter, innan de ingår arrangemangen, vederbörligen beakta huruvida tredjepartsleverantörerna av IKT-tjänster använder de senaste och mest högkvalitativa standarderna för informationssäkerhet.

6. När finansiella entiteter utövar åtkomst-, inspektions- och revisionsrättigheter gentemot tredjepartsleverantören av IKT-tjänster ska de baserat på en riskbaserad metod på förhand fastställa frekvensen för revisioner och inspektioner samt de områden som ska granskas genom att följa allmänt accepterade revisionsstandarder i enlighet med eventuella tillsynsinstruktioner om användning och införlivande av sådana revisionsstandarder.

Om kontraktsmässiga arrangemang som ingås med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster medför hög teknisk komplexitet ska den finansiella entiteten kontrollera att revisorer, oavsett om de är interna eller externa eller ingår i en pool av revisorer, har lämpliga färdigheter och kunskaper för att effektivt kunna utföra de relevanta revisionerna och bedömningarna.

7. Finansiella entiteter ska se till att kontraktsmässiga arrangemang om användning av IKT-tjänster kan avslutas under någon av följande omständigheter:

a) Tredjepartsleverantören av IKT-tjänster bryter på ett betydande sätt 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-tredjepartsleverantören har påvisade svagheter vad gäller sin övergripande IKT-riskhantering och i synnerhet det sätt på vilket den säkerställer tillgänglighet, äkthet, integritet och konfidentialitet för data, oavsett om det är personuppgifter eller på annat sätt känsliga uppgifter eller icke-personuppgifter.

d) Om den behöriga myndigheten inte längre effektivt kan utöva tillsyn över den finansiella entiteten till följd av villkoren i eller omständigheter relaterade till respektive kontraktsmässiga arrangemang.

8. När det gäller IKT-tjänster som stöder kritiska eller viktiga funktioner ska finansiella entiteter införa exitstrategier. Exitstrategierna ska ta hänsyn till risker som kan uppstå hos tredjepartsleverantörerna av IKT-tjänster, i synnerhet eventuella fel hos dessa, försämring av kvaliteten på de IKT-tjänster som tillhandahålls, eventuella avbrott i verksamheten på grund av olämpligt eller misslyckat tillhandahållande av IKT-tjänster eller eventuella väsentliga risker som uppstår i samband med en lämplig och kontinuerlig användning av respektive IKT-tjänst, eller uppsägning av kontraktsmässiga arrangemang med tredjepartsleverantörer av IKT-tjänster under någon av de omständigheter som anges i punkt 7.

Finansiella entiteter 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 de tjänster som tillhandahålls kunder.

Exitplanerna ska vara heltäckande och dokumenterade och de ska, i enlighet med kriterierna i artikel 4.2, vara tillräckligt testade och ska regelbundet ses över.

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

Finansiella entiteter ska ha lämpliga beredskapsåtgärder på plats för att upprätthålla kontinuiteten i verksamheten vid uppkomst av de omständigheter som avses i första stycket.

9. 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 3, inbegripet uppgifter som är gemensamma för alla kontraktsmässiga arrangemang om användning av IKT-tjänster. De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för genomförande till kommissionen senast den 17 januari 2024.

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 1094/2010 och (EU) nr 1095/2010.

10. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för tillsyn för att närmare specificera det detaljerade innehållet i de riktlinjer som avses i punkt 2 i fråga om de kontraktsmässiga arrangemangen för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster.

När de europeiska tillsynsmyndigheterna utarbetar dessa förslag till tekniska standarder för tillsyn ska de ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser. De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 januari 2024.

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 1094/2010 och (EU) nr 1095/2010.

Artikel 29

Preliminär bedömning av IKT-koncentrationsrisker på entitetsnivå

1. När finansiella entiteter utför den identifiering och bedömning av risk som avses i artikel 28.4 c ska de även ta hänsyn till om det planerade ingåendet av ett kontraktsmässigt arrangemang avseende IKT-tjänster som stöder kritiska eller viktiga funktioner skulle leda till något av följande:

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

b) Flera kontraktsmässiga arrangemang gällande tillhandahållande av IKT-tjänster som stöder kritiska eller viktiga funktioner med samma tredjepartsleverantör av IKT-tjänster eller med nära anknutna tredjepartsleverantörer av IKT-tjänster.

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

Om de kontraktsmässiga arrangemangen gäller IKT-tjänster som stöder kritiska eller viktiga funktioner ska finansiella entiteter vederbörligen ta hänsyn till de insolvensrättsliga bestämmelser som skulle vara tillämpliga om IKT-tjänsteleverantören går i konkurs samt eventuella begränsningar som kan uppstå när det gäller skyndsam återställning av den finansiella entitetens data.

Om kontraktsmässiga arrangemang om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner ingås med en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland ska finansiella entiteter utöver de hänsynstaganden som avses i andra stycket även beakta överensstämmelsen med unionens dataskyddsregler och den faktiska efterlevnaden av rätten i det tredjelandet.

Om de kontraktsmässiga arrangemangen om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner medger underentreprenad, ska finansiella entiteter 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 entiteten i detta avseende.

Artikel 30

Viktiga avtalsbestämmelser

1. Rättigheterna och skyldigheterna för den finansiella entiteten och tredjepartsleverantören av IKT-tjänster ska vara tydligt fördelade och skriftligen angivna. Det fullständiga avtalet ska omfatta servicenivåavtalen och dokumenteras i ett skriftligt dokument som parterna ska ha tillgång till på papper eller i ett dokument med ett annat nedladdningsbart, varaktigt och tillgängligt format.

2. De kontraktsmässiga arrangemangen för användning av IKT-tjänster ska innehålla åtminstone följande delar:

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

b) De platser, nämligen regioner eller länder, där de funktioner och IKT-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 på förhand ska underrätta den finansiella entiteten om den planerar att ändra sådana platser.

c) Bestämmelser om tillgänglighet, äkthet, integritet och konfidentialitet vad gäller skydd av data, inbegripet personuppgifter.

d) Bestämmelser om säkerställande av åtkomst, återställande och återlämnande i ett lättillgängligt format av personuppgifter och andra uppgifter än personuppgifter som behandlas av den finansiella entiteten i händelse av insolvens, resolution eller nedläggning av verksamheten vad avser tredjepartsleverantören av IKT-tjänster, eller i händelse av uppsägning av de kontraktsmässiga arrangemangen.

e) Beskrivningar av servicenivå, inbegripet uppdateringar och revideringar av dessa.

f) Skyldigheten för tredjepartsleverantören av IKT-tjänster att tillhandahålla assistans till den finansiella entiteten utan extra kostnad, eller till en kostnad som fastställs på förhand, när en IKT-incident med anknytning till den IKT-tjänst som tillhandahålls den finansiella entiteten inträffar.

g) Skyldigheten för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut med de behöriga myndigheterna och resolutionsmyndigheterna för den finansiella entiteten, inbegripet personer som har utsetts av dem.

h) Uppsägningsrätt och tillhörande minsta uppsägningstid för uppsägning av det kontraktsmässiga arrangemanget, i enlighet med de behöriga myndigheternas och resolutionsmyndigheternas förväntningar.

i) Villkoren för deltagande av tredjepartsleverantörer av IKT-tjänster i finansiella entiteters program för medvetenhet om IKT-säkerhet och utbildning om digital operativ motståndskraft i enlighet med artikel 13.6.

3. De kontraktsmässiga arrangemangen om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner ska, utöver de delar som avses i punkt 2, innehålla åtminstone följande:

a) Beskrivningar av fullständig servicenivå, inklusive uppdateringar och revideringar av dessa, med exakta kvantitativa och kvalitativa prestationsmål inom de överenskomna servicenivåerna för att göra det möjligt för den finansiella entiteten att effektivt övervaka IKT-tjänster och göra det möjligt att utan onödigt dröjsmål vidta lämpliga korrigerande åtgärder när överenskomna servicenivåer inte uppnås.

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

c) 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 ger en lämplig säkerhetsnivå vid tillhandahållande av tjänster från den finansiella entitetens sida i enlighet med dess regelverk.

d) Skyldigheten för tredjepartsleverantören av IKT-tjänster att delta och fullt ut samarbeta i den finansiella entitetens hotbildsstyrda penetrationstestning enligt artiklarna 26 och 27.

e) Rätten att fortlöpande övervaka prestandan hos tredjepartsleverantören av IKT-tjänster, vilket omfattar följande:

i) Obegränsad rätt till tillgång till, inspektion och revision för den finansiella entiteten eller en utsedd tredjepart, och för den behöriga myndigheten, och rätt att ta kopior av relevant dokumentation på plats om de är kritiska för verksamheten hos tredjepartsleverantören av IKT-tjänster, vars faktiska utövande inte hindras eller begränsas av andra kontraktsmässiga arrangemang eller strategier för genomförande.

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

iii) Skyldigheten för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut under de inspektioner och revisioner på plats som utförs av de behöriga myndigheterna, den ledande tillsynsmyndigheten, den finansiella entiteten eller en utsedd tredjepart.

iv) Skyldigheten att tillhandahålla närmare uppgifter om omfattningen, de förfaranden som ska följas och frekvensen för sådana inspektioner och revisioner.

f) Exitstrategier, särskilt inrättande av en obligatorisk lämplig övergångsperiod

i) under vilken tredjepartsleverantören av IKT-tjänster kommer att fortsätta att tillhandahålla respektive funktioner eller IKT-tjänster i syfte att minska risken för avbrott hos den finansiella entiteten, eller säkerställa en effektiv resolution och omstrukturering av denna,

ii) som gör det möjligt för den finansiella entiteten att migrera till en annan tredjepartsleverantör av IKT-tjänster eller byta till interna lösningar som är förenliga med komplexiteten hos den tillhandahållna tjänsten.

Genom undantag från led e får tredjepartsleverantören av IKT-tjänster och en finansiell entitet som är ett mikroföretag komma överens om att den finansiella entitetens rätt till tillgång, inspektion och revision kan delegeras till en oberoende tredjepart som utsetts av tredjepartsleverantören av IKT-tjänster, och att den finansiella entiteten när som helst kan begära information och försäkran om IKT-tredjepartsleverantörens prestanda från den tredje parten.

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

5. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för tillsyn för att närmare specificera de delar som avses i punkt 2 a och som en finansiell entitet måste fastställa och bedöma när den lägger ut IKT-tjänster som stöder kritiska eller viktiga funktioner på underentreprenad.

När de europeiska tillsynsmyndigheterna utarbetar dessa förslag till tekniska standarder för tillsyn ska de ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 juli 2024.

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 1094/2010 och (EU) nr 1095/2010.

Avsnitt II

Tillsynsram för kritiska tredjepartsleverantörer av IKT-tjänster

Artikel 31

Klassificering av tredjepartsleverantörer av IKT-tjänster som kritiska

1. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och på rekommendation av det tillsynsforum som har inrättats enligt artikel 32.1,

a) klassificera tredjepartsleverantörer av IKT-tjänster som kritiska för finansiella entiteter, efter en bedömning som tar hänsyn till de kriterier som anges i punkt 2,

b) utse till ledande tillsynsmyndighet för varje kritisk tredjepartsleverantör av IKT-tjänster den europeiska tillsynsmyndighet som är ansvarig enligt förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 eller (EU) nr 1095/2010 för de finansiella entiteter som tillsammans har den största andelen av de totala tillgångarna av värdet av de totala tillgångarna hos alla finansiella entiteter som utnyttjar tjänster från den relevanta kritiska tredjepartsleverantören av IKT-tjänster, i enlighet med vad som framgår av summan av dessa finansiella entiteters enskilda balansräkningar.

2. Den klassificering som avses i punkt 1 a ska baseras på samtliga följande kriterier när det gäller IKT-tjänster som tillhandahålls av tredjepartsleverantören av IKT-tjänster:

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 entiteter och det totala värdet av tillgångarna hos de finansiella entiteter som den berörda tredjepartsleverantören av IKT-tjänster tillhandahåller tjänster till.

b) Påverkan på eller betydelsen för systemet av de finansiella entiteter 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 entiteter, inbegripet situationer där de globala systemviktiga instituten eller andra systemviktiga instituten tillhandahåller finansiella infrastrukturtjänster till andra finansiella entiteter.

c) Finansiella entiteters beroende av de tjänster som tillhandahålls av den berörda tredjepartsleverantören av IKT-tjänster i förhållande till kritiska eller viktiga funktioner hos de finansiella entiteter som i sista hand involverar samma tredjepartsleverantör av IKT-tjänster, oavsett om finansiella entiteter 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 när det gäller att helt eller delvis migrera relevanta data och arbetsbelastningar från den berörda tredjepartsleverantören av IKT-tjänster till en annan tredjepartsleverantör av IKT-tjänster, på grund av betydande finansiella kostnader, tidsåtgång eller andra resurser som migrationsprocessen kan medföra, eller på grund av ökad IKT-risk eller andra operativa risker som den finansiella entiteten kan utsättas för genom sådan migration.

3. Om tredjepartsleverantören av IKT-tjänster ingår i en koncern ska de kriterier som avses i punkt 2 beaktas vad avser de IKT-tjänster som koncernen som helhet tillhandahåller.

4. Kritiska tredjepartsleverantörer av IKT-tjänster som ingår i en koncern ska utse en juridisk person till samordningspunkt för att säkerställa lämplig representation och kommunikation med den ledande tillsynsmyndigheten.

5. Den ledande tillsynsmyndigheten ska underrätta tredjepartsleverantören av IKT-tjänster om resultatet av den bedömning som leder till den klassificering som avses i punkt 1 a. Inom sex veckor från dagen för anmälan får tredjepartsleverantören av IKT-tjänster lämna in ett motiverat uttalande till den ledande tillsynsmyndigheten med all relevant information för bedömningen. Den ledande tillsynsmyndigheten ska beakta det motiverade uttalandet och får begära att ytterligare information lämnas inom 30 kalenderdagar efter mottagandet av ett sådant uttalande.

Efter att ha klassificerat en tredjepartsleverantör av IKT-tjänster som kritisk ska de europeiska tillsynsmyndigheterna, genom den gemensamma kommittén, underrätta tredjepartsleverantören av IKT-tjänster om klassificeringen och från och med vilket datum tredjepartsleverantören faktiskt kommer att omfattas av tillsynsverksamhet. Detta startdatum ska inträffa senast en månad efter anmälan. Tredjepartsleverantören av IKT-tjänster ska underrätta de finansiella entiteter som den tillhandahåller tjänster om att den klassificeras som kritisk.

6. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 57 för att komplettera denna förordning genom att närmare specificera kriterierna i punkt 2 i den här artikeln senast den 17 juli 2024.

7. Den klassificering som avses i punkt 1 a får inte användas förrän kommissionen har antagit en delegerad akt i enlighet med punkt 6.

8. Den klassificering som avses i punkt 1 a får inte tillämpas på följande:

i) Finansiella entiteter som tillhandahåller IKT-tjänster till andra finansiella entiteter.

ii) 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.

iii) Koncerninterna IKT-tjänsteleverantörer.

iv) Tredjepartsleverantörer av IKT-tjänster som endast tillhandahåller IKT-tjänster i en medlemsstat till finansiella entiteter som endast är verksamma i den medlemsstaten.

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

10. Vid tillämpning av punkt 1 a ska de behöriga myndigheterna årligen och i aggregerad form översända de rapporter som avses i artikel 28.3 tredje stycket till det tillsynsforum som har inrättats enligt artikel 32. Tillsynsforumet ska bedöma finansiella entiteters IKT-beroende gentemot tredjepart baserat på den information som har mottagits från de behöriga myndigheterna.

11. De tredjepartsleverantörer av IKT-tjänster som inte ingår i den förteckning som avses i punkt 9 får begära att bli klassificerade som kritiska i enlighet med punkt 1 a.

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 klassificeras som kritisk 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.

12. Finansiella entiteter ska endast använda sig av de tjänster som en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland och som har klassificerats som kritisk i enlighet med punkt 1 a erbjuder om den har etablerat ett dotterföretag i unionen inom tolv månader efter klassificeringen.

13. Den kritiska tredjepartsleverantör av IKT-tjänster som avses i punkt 12 ska underrätta den ledande tillsynsmyndigheten om eventuella ändringar av ledningsstrukturen för det dotterföretag som är etablerat i unionen.

Artikel 32

Tillsynsramens struktur

1. Den gemensamma kommittén ska i enlighet med artikel 57.1 i förordningarna (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 31.1 b inom området för IKT-tredjepartsrisker i alla finansiella sektorer. Tillsynsforumet ska utarbeta utkast till gemensamma ståndpunkter och utkast till gemensamma akter från den gemensamma kommittén på detta område.

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

2. Tillsynsforumet ska årligen göra en gemensam bedömning av resultaten och slutsatserna av den tillsynsverksamhet som genomförts för alla kritiska tredjepartsleverantörer av IKT-tjänster och främja samordningsåtgärder för att öka finansiella entiteters 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 följande:

a) Ordförandena för de europeiska tillsynsmyndigheterna.

b) En företrädare på hög nivå för den tjänstgörande personalen på den relevanta behöriga myndighet som avses i artikel 46 i varje medlemsstat.

c) De verkställande direktörerna för varje europeisk tillsynsmyndighet och en företrädare för kommissionen, ESRB, ECB och Enisa som observatörer.

d) När så är lämpligt, ytterligare en företrädare från en behörig myndighet som avses i artikel 46 i varje medlemsstat som observatör.

e) I tillämpliga fall, en företrädare från de behöriga myndigheter som i enlighet med direktiv (EU) 2022/2555 har utsetts eller inrättats till ansvariga för tillsynen av en väsentlig eller viktig entitet om inte annat följer av det direktivet som har klassificerats som kritisk tredjepartsleverantör av IKT-tjänster som observatör.

Tillsynsforumet får, när så är lämpligt, rådfråga oberoende experter som utsetts i enlighet med punkt 6.

5. Varje medlemsstat ska utse den relevanta behöriga myndighet vars anställde ska vara den företrädare på hög nivå som avses i punkt 4 första stycket b, och ska informera den ledande tillsynsmyndigheten om detta.

De europeiska tillsynsmyndigheterna ska på sin webbplats offentliggöra förteckningen över de företrädare på hög nivå från den befintliga personalen vid den relevanta behöriga myndigheten som utsetts av medlemsstaterna.

6. De oberoende experter som avses i punkt 4 andra stycket ska utses av tillsynsforumet bland en pool av experter som väljs ut efter ett offentligt och transparent ansökningsförfarande.

De oberoende experterna ska utses baserat på sin sakkunskap om finansiell stabilitet, digital operativ motståndskraft och IKT-säkerhet. De ska handla oberoende och objektivt och uteslutande i hela unionens intresse och varken begära eller ta emot instruktioner från unionens institutioner eller organ, regeringen i någon medlemsstat eller något annat offentligt eller privat organ.

7. I enlighet med artikel 16 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 ska de europeiska tillsynsmyndigheterna senast den 17 juli 2024 vid tillämpningen av detta avsnitt utfärda riktlinjer för samarbetet mellan de europeiska tillsynsmyndigheterna och de behöriga myndigheterna som omfattar detaljerade förfaranden och villkor för fördelningen och utförandet av uppgifter mellan behöriga myndigheter och de europeiska tillsynsmyndigheterna och närmare uppgifter om det informationsutbyte som är nödvändiga för att de behöriga myndigheterna ska kunna säkerställa uppföljningen av de rekommendationer som riktas till kritiska tredjepartsleverantörer av IKT-tjänster enligt artikel 35.1 d.

8. De krav som fastställs i detta avsnitt ska inte påverka tillämpningen av direktiv (EU) 2022/2555 och andra unionsregler om tillsyn som är tillämpliga på leverantörer av molntjänster.

9. 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 om tillämpningen av detta avsnitt för Europaparlamentet, rådet och kommissionen.

Artikel 33

Den ledande tillsynsmyndighetens uppgifter

1. Den ledande tillsynsmyndigheten, som utsetts i enlighet med artikel 31.1 b, ska utöva tillsyn över de kritiska tredjepartsleverantörer av IKT-tjänster som den tilldelats och ska, när det gäller alla frågor som rör tillsynen, vara den huvudsakliga kontaktpunkten för dessa kritiska tredjepartsleverantörer av IKT-tjänster.

2. Vid tillämpning av punkt 1 ska den ledande tillsynsmyndigheten bedöma huruvida varje kritisk tredjepartsleverantör av IKT-tjänster har infört heltäckande, sunda och effektiva regler, förfaranden, mekanismer och arrangemang för att hantera den IKT-risk som den kan medföra för finansiella entiteter.

Den bedömning som avses i första stycket ska huvudsakligen inriktas på IKT-tjänster som tillhandahålls av den kritiska tredjepartsleverantör av IKT-tjänster som stöder finansiella entiteters kritiska eller viktiga funktioner. Om det är nödvändigt för att hantera alla relevanta risker ska den bedömningen även omfatta IKT-tjänster som stöder andra funktioner än de som är kritiska eller viktiga.

3. Den bedömning som avses i punkt 2 ska omfatta:

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 entiteter, samt förmåga att alltid upprätthålla höga standarder för tillgänglighet, äkthet, integritet eller konfidentialitet.

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

c) Riskhanteringsprocesser, inbegripet IKT-riskhanteringsstrategier, IKT-kontinuitetspolicy och åtgärds- och återställningsplaner avseende IKT.

d) Styrformer, inbegripet en organisationsstruktur med tydliga, transparenta och konsekventa regler för ansvar och ansvarsskyldighet som möjliggör en effektiv IKT-riskhantering.

e) Identifiering, övervakning och snabb rapportering av väsentliga IKT-relaterade incidenter till finansiella entiteter, hantering och avhjälpande av dessa incidenter, särskilt cyberangrepp.

f) Mekanismer för dataportabilitet, tillämpningsportabilitet och interoperabilitet, som säkerställer att finansiella entiteter 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 finansiella entiteter.

4. Baserat på den bedömning som avses i punkt 2, och i samordning med det gemensamma tillsynsnätverk som avses i artikel 34.1, ska den ledande tillsynsmyndigheten anta en tydlig, detaljerad och motiverad individuell tillsynsplan med en beskrivning av de årliga tillsynsmålen och de huvudsakliga tillsynsinsatser som planeras för varje kritisk tredjepartsleverantör av IKT-tjänster. Planen ska varje år meddelas den kritiska tredjepartsleverantören av IKT-tjänster.

Innan tillsynsplanen antas ska den ledande tillsynsmyndigheten överlämna utkastet till tillsynsplan till den kritiska tredjepartsleverantören av IKT-tjänster.

Vid mottagandet av utkastet till tillsynsplan får den kritiska tredjepartsleverantören av IKT-tjänster lämna in ett motiverat uttalande inom 15 kalenderdagar som dels styrker den förväntade inverkan på de kunder som är entiteter som faller utanför denna förordnings tillämpningsområde och dels, i förekommande fall, formulerar lösningar för att minska riskerna.

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

Artikel 34

Operativ samordning mellan ledande tillsynsmyndigheter

1. För att säkerställa ett konsekvent tillvägagångssätt för tillsynsverksamheten och i syfte att möjliggöra samordnade allmänna tillsynsstrategier och sammanhängande operativa tillvägagångssätt och arbetsmetoder, ska de tre ledande tillsynsmyndigheter som utsetts i enlighet med artikel 31.1 b inrätta ett gemensamt tillsynsnätverk för att sinsemellan samordna de förberedande faserna och samordna genomförandet av tillsynsverksamheten för de respektive kritiska tredjepartsleverantörer av IKT-tjänster som de granskar, samt inom ramen för eventuella åtgärder som kan behövas enligt artikel 42.

2. Vid tillämpning av punkt 1 ska de ledande tillsynsmyndigheterna utarbeta ett gemensamt tillsynsprotokoll som anger de detaljerade förfaranden som ska följas för den dagliga samordningen och för att säkerställa snabba utbyten och reaktioner. Protokollet ska regelbundet ses över för att återspegla de operativa behoven, särskilt utvecklingen av arrangemangen för den praktiska tillsynen.

3. De ledande tillsynsmyndigheterna får från fall till fall uppmana ECB och Enisa att tillhandahålla teknisk rådgivning, dela med sig av praktiska erfarenheter eller delta i specifika samordningsmöten för det gemensamma tillsynsnätverket.

Artikel 35

Den ledande tillsynsmyndighetens befogenheter

1. För att fullgöra de uppgifter som anges i detta avsnitt ska den ledande tillsynsmyndigheten vad gäller de kritiska tredjepartsleverantörerna av IKT-tjänster ha befogenhet att

a) begära all relevant information och dokumentation i enlighet med artikel 37,

b) genomföra allmänna utredningar och inspektioner i enlighet med artiklarna 38 respektive 39,

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

d) utfärda rekommendationer på de områden som avses i artikel 33.3, 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 entiteter,

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

   iii) om eventuell planerad underentreprenad, när den ledande tillsynsmyndigheten bedömer att ytterligare underentreprenad, inbegripet underentreprenadsavtal som de kritiska tredjepartsleverantörerna av IKT-tjänster planerar att ingå med tredjepartsleverantörer av IKT-tjänster eller med IKT-underleverantörer som är etablerade i ett tredjeland, kan utlösa risker för den finansiella entitetens tillhandahållande av tjänster eller risker för den finansiella stabiliteten, på grundval av granskningen av den information som samlas in i enlighet med artiklarna 37 och 38,

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

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

      — underentreprenaden avser kritiska eller viktiga funktioner hos den finansiella entiteten, och

— den ledande tillsynsmyndigheten anser att användningen av sådan underentreprenad utgör en klar och allvarlig risk för unionens finansiella stabilitet eller för finansiella entiteter, inbegripet finansiella entiteters förmåga att uppfylla tillsynskraven.

Vid tillämpning av led iv i detta led ska tredjepartsleverantörer av IKT-tjänster, med hjälp av den mall som avses i artikel 41.1 b, överföra informationen om underentreprenad till den ledande tillsynsmyndigheten.

2. Vid utövandet av de befogenheter som avses i denna artikel ska den ledande tillsynsmyndigheten

a) säkerställa regelbunden samordning inom det gemensamma tillsynsnätverket, och i synnerhet eftersträva konsekventa tillvägagångssätt, när så är lämpligt, vad gäller tillsynen av kritiska tredjepartsleverantörer av IKT-tjänster,

b) ta vederbörlig hänsyn till den ram som fastställs i direktiv (EU) 2022/2555 och vid behov samråda med de relevanta behöriga myndigheter som utsetts eller inrättats i enlighet med det direktivet, för att undvika överlappning av tekniska och organisatoriska åtgärder som skulle kunna tillämpas på kritiska tredjepartsleverantörer av IKT-tjänster enligt det direktivet,

c) sträva efter att i möjligaste mån minimera risken för avbrott i tjänster som kritiska tredjepartsleverantörer av IKT-tjänster tillhandahåller kunder som är entiteter som faller utanför denna förordnings tillämpningsområde.

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

Innan den ledande tillsynsmyndigheten utfärdar rekommendationer i enlighet med punkt 1 d ska den ge tredjepartsleverantören av IKT-tjänster möjlighet att inom 30 kalenderdagar tillhandahålla relevant information som dels styrker den förväntade inverkan på de kunder som är entiteter som faller utanför denna förordnings tillämpningsområde och dels, i förekommande fall, formulerar lösningar för att minska riskerna.

4. Den ledande tillsynsmyndigheten ska informera det gemensamma tillsynsnätverket om resultatet av utövandet av de befogenheter som avses i punkt 1 a och b. Den ledande tillsynsmyndigheten ska utan onödigt dröjsmål översända de rapporter som avses i punkt 1 c till det gemensamma tillsynsnätverket och till de behöriga myndigheterna för de finansiella entiteter som använder de IKT-tjänster som tillhandahålls av den kritiska tredjepartsleverantören av IKT-tjänster.

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

6. Den ledande tillsynsmyndigheten ska, vid helt eller delvis bristande efterlevnad av de åtgärder som ska vidtas enligt utövandet av befogenheterna i punkt 1 a, b och c och efter utgången av en period på minst 30 kalenderdagar från den dag då den kritiska tredjepartsleverantören av IKT-tjänster mottog anmälan om åtgärderna, anta ett beslut om föreläggande av vite för att tvinga den kritiska tredjepartsleverantören av IKT-tjänster att efterleva dessa åtgärder.

7. Det vite som avses i punkt 6 ska åläggas dagligen till dess att efterlevnad har uppnåtts och i högst sex månader efter det att beslutet om vite har anmälts till den kritiska tredjepartsleverantören av IKT-tjänster.

8. Vitesbeloppet, beräknat från det datum som anges i beslutet om föreläggande av vitet, ska vara upp till 1 % av den genomsnittliga globala omsättningen per dag för den kritiska tredjepartsleverantören av IKT-tjänster under det föregående räkenskapsåret. Den ledande tillsynsmyndigheten ska när den fastställer vitesbeloppet beakta följande kriterier för bristande efterlevnad av de åtgärder som avses i punkt 6:

a) Den bristande efterlevnadens allvarlighetsgrad och varaktighet.

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

c) Viljan hos tredjepartsleverantören av IKT-tjänster att samarbeta med den ledande tillsynsmyndigheten.

Vid tillämpning av första stycket ska den ledande tillsynsmyndigheten samråda inom det gemensamma tillsynsnätverket för att säkerställa en konsekvent strategi.

9. Vitet ska vara av administrativ karaktär och ska vara verkställbart. Verkställigheten ska följa de civilprocessrättsliga regler som gäller i den medlemsstat inom vars territorium inspektionerna 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.

10. Den ledande tillsynsmyndigheten 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 oproportionellt stor skada.

11. Innan ett vite åläggs enligt punkt 6 ska den ledande tillsynsmyndigheten ge företrädarna för den kritiska tredjepartsleverantör av IKT-tjänster som är föremål för förfarandet möjlighet att höras om de omständigheter som tillsynsmyndigheterna har påtalat, och den ska grunda sina beslut endast på omständigheter som den kritiska tredjepartsleverantören av IKT-tjänster som är föremål för förfarandet har haft möjlighet att yttra sig över.

Rätten till försvar för personer som är föremål för förfarandet ska iakttas fullt ut under förfarandet. Den kritiska tredjepartsleverantör av IKT-tjänster som är föremål för förfarandet 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 36

Den ledande tillsynsmyndighetens utövande av befogenheter utanför unionen

1. Om tillsynsmålen inte kan uppnås genom samverkan med det dotterföretag som har etablerats i enlighet med artikel 31.12 eller genom utövande av tillsynsverksamhet i lokaler som är belägna i unionen, får den ledande tillsynsmyndigheten utöva de befogenheter som anges i följande bestämmelser i alla lokaler som är belägna i ett tredjeland och som ägs eller på något sätt används av en kritisk tredjepartsleverantör av IKT-tjänster i syfte att tillhandahålla tjänster till finansiella entiteter i unionen i samband med dess affärsverksamhet, funktioner eller tjänster, inbegripet alla administrativa kontor, företagslokaler eller driftställen, anläggningar, mark, byggnader eller annan egendom:

a) I artikel 35.1 a.

b) I artikel 35.1 b, i enlighet med artikel 38.2 a, b och d, artikel 39.1 och 39.2 a.

De befogenheter som avses i första stycket får utövas om samtliga följande villkor är uppfyllda:

i) Den ledande tillsynsmyndigheten anser att en inspektion i ett tredjeland är nödvändig för att den fullt ut och på ett ändamålsenligt sätt ska kunna utföra sina uppgifter enligt denna förordning.

ii) Inspektionen i ett tredjeland har ett direkt samband med tillhandahållandet av IKT-tjänster till finansiella entiteter i unionen.

iii) Den berörda kritiska tredjepartsleverantören av IKT-tjänster samtycker till att en inspektion genomförs i ett tredjeland.

iv) Den relevanta myndigheten i det berörda tredjelandet har underrättats officiellt av den ledande tillsynsmyndigheten och har inte gjort några invändningar mot detta.

2. Utan att det påverkar unionsinstitutionernas och medlemsstaternas befogenheter ska EBA, Esma eller Eiopa vid tillämpningen av punkt 1 ingå arrangemang för administrativt samarbete med den relevanta myndigheten i det tredjelandet för att göra det möjligt för den ledande tillsynsmyndigheten och den grupp som den har utsett för uppdraget i det berörda tredjelandet att på ett smidigt sätt genomföra inspektioner i det tredjelandet. Dessa samarbetsarrangemang får inte medföra några rättsliga skyldigheter för unionen och dess medlemsstater eller hindra medlemsstaterna och deras behöriga myndigheter från att ingå bilaterala eller multilaterala arrangemang med dessa tredjeländer och deras relevanta myndigheter.

I dessa samarbetsarrangemang ska åtminstone följande anges:

a) Förfarandena för samordning av den tillsynsverksamhet som genomförs enligt denna förordning och all motsvarande övervakning av IKT-tredjepartsrisker i den finansiella sektorn som utövas av den relevanta myndigheten i det berörda tredjelandet, inbegripet uppgifter för översändande av den sistnämndas samtycke så att den ledande tillsynsmyndigheten och dess utsedda grupp kan genomföra allmänna utredningar och inspektioner på plats enligt punkt 1 första stycket på det territorium som omfattas av dess jurisdiktion.

b) Mekanismen för översändande av relevant information mellan EBA, Esma eller Eiopa och den relevanta myndigheten i det berörda tredjelandet, särskilt i samband med information som den ledande tillsynsmyndigheten kan begära enligt artikel 37.

c) Mekanismerna för omedelbar anmälan till EBA, Esma eller Eiopa från den relevanta myndigheten i det berörda tredjelandet av fall där en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland och har klassificerats som kritisk i enlighet med artikel 31.1 a anses ha åsidosatt de krav som den enligt det berörda tredjelandets tillämpliga rätt är skyldig att följa när den tillhandahåller tjänster till finansiella institut i det tredjelandet samt de avhjälpande åtgärder och sanktioner som tillämpas.

d) Regelbundet översändande av uppdateringar om utvecklingen på reglerings- eller tillsynsområdet när det gäller övervakningen av IKT-tredjepartsrisker för finansiella institut i det berörda tredjelandet.

e) Uppgifter som vid behov gör det möjligt för en företrädare för den relevanta myndigheten i det berörda tredjelandet att delta i de inspektioner som den ledande tillsynsmyndigheten och den utsedda gruppen genomför.

3. När den ledande tillsynsmyndigheten inte kan genomföra sådan tillsynsverksamhet utanför unionen som avses i punkterna 1 och 2, ska den ledande tillsynsmyndigheten

a) utöva sina befogenheter enligt artikel 35 på grundval av alla sakförhållanden som den känner till och dokument som den har tillgång till,

b) dokumentera och förklara eventuella konsekvenser av att den inte är i stånd att genomföra den planerade tillsynsverksamhet som avses i denna artikel.

De potentiella konsekvenser som avses i led b i denna punkt ska beaktas i den ledande tillsynsmyndighetens rekommendationer, som utfärdas enligt artikel 35.1 d.

Artikel 37

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 och operativa dokument, avtal, strategier, dokumentation, 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 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) 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 genom ett beslut 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 35.6 om den begärda informationen är ofullständig eller om informationen inte tillhandahålls inom den tidsfrist som anges i led d i den här punkten,

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

4. Företrädarna för de kritiska tredjepartsleverantörerna 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 översända en kopia av beslutet om tillhandahållande av information till de behöriga myndigheterna för de finansiella entiteter som använder berörd kritisk tredjepartsleverantörs IKT-tjänster och till det gemensamma tillsynsnätverket.

Artikel 38

Allmänna utredningar

1. För att fullgöra sina uppgifter enligt denna förordning får den ledande tillsynsmyndigheten, med bistånd av den gemensamma undersökningsgrupp som avses i artikel 40.1, vid behov genomföra utredningar av kritiska 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, dokumenterade förfaranden och allt annat material,

c) kalla till sig företrädare för den kritiska 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 35.6 om den dokumentation, de uppgifter, de dokumenterade 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 kritiska 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 35.6, 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 innan utredningen inleds underrätta de behöriga myndigheterna för de finansiella entiteter som använder de IKT-tjänster som tillhandahålls av den kritiska tredjepartsleverantören av IKT-tjänster om den planerade utredningen och namnge de bemyndigade personerna.

Den ledande tillsynsmyndigheten ska underrätta det gemensamma tillsynsnätverket om all information som översänds enligt första stycket.

Artikel 39

Inspektioner

1. För att utföra sina uppgifter enligt denna förordning får den ledande tillsynsmyndigheten, med bistånd av de gemensamma undersökningsgrupper som avses i artikel 40.1, inleda och genomföra alla nödvändiga inspektioner på plats i företagslokaler, på mark eller egendom som tillhör tredjepartsleverantörerna av IKT-tjänster, såsom huvudkontor, driftscentrum och sekundära lokaler, samt genomföra skrivbordsinspektioner.

Vid utövandet av de befogenheter som avses i första stycket ska den ledande tillsynsmyndigheten samråda med det gemensamma tillsynsnätverket.

2. Tjänstemän och andra personer som av den ledande tillsynsmyndigheten har bemyndigats att genomföra en inspektion på plats ska ha befogenhet att

a) bereda sig tillträde till företagslokaler, mark eller egendom och att

b) försegla sådana företagslokaler, räkenskaper eller affärshandlingar under den tid och i den utsträckning som krävs för inspektionen.

Tjänstemän och andra personer som har bemyndigats av den ledande tillsynsmyndigheten ska utöva sina befogenheter mot uppvisande av ett skriftligt tillstånd som anger inspektionens föremål och syften liksom de viten som föreskrivs i artikel 35.6 om företrädarna för de berörda kritiska tredjepartsleverantörerna av IKT-tjänster inte underkastar sig inspektionen.

3. Den ledande tillsynsmyndigheten ska i god tid innan inspektionen inleds informera de behöriga myndigheterna för de finansiella entiteter som använder denna tredjepartsleverantör av IKT-tjänster.

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

5. Före en planerad inspektion på plats ska den ledande tillsynsmyndigheten 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 inspektionen eller revisionen inte längre skulle vara effektiv.

6. Den kritiska tredjepartsleverantören av IKT-tjänster ska underkasta sig inspektioner på plats som har beordrats genom beslut av den ledande tillsynsmyndigheten. Beslutet ska ange föremålet för och syftet med inspektionen, fastställa den dag då inspektionen ska inledas och ange de viten som föreskrivs i artikel 35.6, 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 inspektion som har beordrats enligt denna artikel, ska den ledande tillsynsmyndigheten informera den kritiska tredjepartsleverantören av IKT-tjänster om konsekvenserna av att den motsätter sig kontrollen, inbegripet möjligheten för de berörda finansiella entiteternas behöriga myndigheter att kräva att de finansiella entiteterna säger upp de kontraktsmässiga arrangemang som har ingåtts med den kritiska tredjepartsleverantören av IKT-tjänster.

Artikel 40

Fortlöpande tillsyn

1. Vid tillsynsverksamhet, särskilt allmänna utredningar eller inspektioner ska den ledande tillsynsmyndigheten bistås av en gemensam 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

a) de europeiska tillsynsmyndigheterna,

b) de relevanta behöriga myndigheter som utövar tillsyn över de finansiella entiteter till vilka den kritiska tredjepartsleverantören av IKT-tjänster tillhandahåller IKT-tjänster,

c) den nationella behöriga myndighet som avses i artikel 32.4 e, på frivillig basis,

d) en nationell behörig myndighet från den medlemsstat där den kritiska tredjepartsleverantören av IKT-tjänster är etablerad, på frivillig basis.

Medlemmar i den gemensamma undersökningsgruppen ska ha sakkunskap om IKT-frågor och om operativa risker. Den gemensamma undersökningsgruppen ska samordnas av en utsedd anställd vid den ledande tillsynsmyndigheten (*den ledande tillsynsmyndighetens samordnare*).

3. Inom tre månader efter slutförandet av en utredning eller inspektion ska den ledande tillsynsmyndigheten, efter samråd med tillsynsforumet, anta rekommendationer som ska riktas till den kritiska tredjepartsleverantören av IKT-tjänster enligt de befogenheter som avses i artikel 35.

4. De rekommendationer som avses i punkt 3 ska omedelbart meddelas den kritiska tredjepartsleverantören av IKT-tjänster och de behöriga myndigheterna för de finansiella entiteter till vilka den tillhandahåller IKT-tjänster.

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

Artikel 41

Harmonisering av villkor som möjliggör genomförandet för tillsynsverksamheten

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 tredjepartsleverantör av IKT-tjänster i ansökan om frivillig begäran om att bli klassificerad som kritisk enligt artikel 31.11,

b) innehållet, strukturen och formatet avseende den information som tredjepartsleverantörerna av IKT-tjänster ska lämna in, offentliggöra eller rapportera enligt artikel 35.1, inbegripet mallen för tillhandahållande av information om underleverantörsavtal,

c) kriterierna för fastställande av den gemensamma undersökningsgruppens sammansättning, vilka säkerställer ett balanserat deltagande av personal från de europeiska tillsynsmyndigheterna och från de relevanta behöriga myndigheterna samt deras utseende, uppgifter och arbetsmetoder,

d) närmare uppgifter om de behöriga myndigheternas bedömning av de åtgärder som har vidtagits av kritiska tredjepartsleverantörer av IKT-tjänster på grundval av rekommendationerna från den ledande tillsynsmyndigheten enligt artikel 42.3.

2. De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 juli 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i punkt 1 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 42

Behöriga myndigheters uppföljning

1. Inom 60 kalenderdagar från mottagandet av de rekommendationer som har utfärdats av den ledande tillsynsmyndigheten enligt artikel 35.1 d ska kritiska tredjepartsleverantörer av IKT-tjänster antingen underrätta den ledande tillsynsmyndigheten om sin avsikt att följa rekommendationerna eller lämna en motiverad förklaring till varför de inte följer sådana rekommendationer. Den ledande tillsynsmyndigheten ska omedelbart vidarebefordra denna information till de berörda finansiella entiteternas behöriga myndigheter.

2. Den ledande tillsynsmyndigheten ska offentliggöra fall där en kritisk tredjepartsleverantör av IKT-tjänster underlåter att underrätta den ledande tillsynsmyndigheten i enlighet med punkt 1 eller där den förklaring som lämnats av den kritiska tredjepartsleverantören av IKT-tjänster inte bedöms vara tillräcklig. Den offentliggjorda informationen ska avslöja identiteten på den kritiska tredjepartsleverantören av IKT-tjänster samt information om typen och arten av den bristande efterlevnaden. Sådan information ska begränsas till vad som är relevant och proportionellt för att säkerställa allmänhetens medvetenhet, såvida inte ett sådant offentliggörande skulle kunna orsaka de berörda parterna oproportionellt stor skada eller allvarligt skulle kunna äventyra finansmarknadernas korrekta funktion och integritet eller stabiliteten i hela eller delar av unionens finansiella system.

Den ledande tillsynsmyndigheten ska underrätta tredjepartsleverantören av IKT-tjänster om detta offentliggörande.

3. De behöriga myndigheterna ska informera de berörda finansiella entiteterna om de risker som har identifierats i rekommendationerna till kritiska tredjepartsleverantörer av IKT-tjänster i enlighet med artikel 35.1 d.

Finansiella entiteter ska när de hanterar IKT-tredjepartsrisker ta hänsyn till de risker som avses i första stycket.

4. Om en behörig myndighet bedömer att en finansiell entitet i sin hantering av IKT-tredjepartsrisker inte tar hänsyn till eller i tillräcklig utsträckning hanterar de specifika risker som identifierats i rekommendationerna, ska den underrätta den finansiella entiteten om att det inom 60 kalenderdagar efter mottagandet av en sådan underrättelse kan fattas ett beslut enligt punkt 6 i avsaknad av lämpliga kontraktsmässiga arrangemang för hantering av sådana risker.

5. De behöriga myndigheterna får efter att ha mottagit de rapporter som avses i artikel 35.1 c, och innan de fattar ett beslut som avses i punkt 6 i den här artikeln, på frivillig basis samråda med de behöriga myndigheter som i enlighet med direktiv (EU) 2022/2555 har utsetts eller inrättats till ansvariga för tillsynen av en väsentlig eller viktig entitet om inte annat följer av det direktivet, som har klassificerats som kritisk tredjepartsleverantör av IKT-tjänster.

6. De behöriga myndigheterna får, som en sista utväg efter underrättelsen och i förekommande fall samrådet enligt punkterna 4 och 5 i denna artikel, i enlighet med artikel 50 fatta ett beslut om att finansiella entiteter tillfälligt, helt eller delvis, ska avbryta användningen eller införandet av en tjänst som tillhandahålls av den kritiska tredjepartsleverantörer av IKT-tjänster till dess att de risker som identifieras i rekommendationerna till kritiska tredjepartsleverantörer av IKT-tjänster har åtgärdats. Vid behov får de kräva att finansiella entiteter helt eller delvis ska avsluta de relevanta kontraktsmässiga arrangemang som har ingåtts med de kritiska tredjepartsleverantörerna av IKT-tjänster.

7. Om en kritisk tredjepartsleverantör av IKT-tjänster vägrar att godta rekommendationer baserat på en annan strategi än den som den ledande tillsynsmyndigheten rekommenderar och en sådan annan strategi kan inverka negativt på ett stort antal finansiella entiteter eller en betydande del av den finansiella sektorn, och enskilda varningar från de behöriga myndigheterna inte har lett till konsekventa strategier som minskar den potentiella risken för den finansiella stabiliteten, får den ledande tillsynsmyndigheten efter samråd med tillsynsforumet när så är lämpligt utfärda icke-bindande och icke-offentliga yttranden till behöriga myndigheter för att främja konsekventa och samstämmiga uppföljningsåtgärder avseende tillsyn.

8. Efter att ha mottagit de rapporter som avses i artikel 35.1 c ska de behöriga myndigheterna när de fattar ett beslut som avses i punkt 6 i den här artikeln 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 eller interna kontroller.

c) Huruvida ekonomisk brottslighet har underlättats eller orsakats av eller på annat sätt tillskrivs den bristande efterlevnaden.

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

e) Huruvida det tillfälliga upphävandet eller uppsägningen av de kontraktsmässiga arrangemangen hotar kontinuiteten i den finansiella entitetens affärsverksamhet trots den finansiella entitetens ansträngningar att undvika avbrott i tillhandahållandet av tjänster.

f) I tillämpliga fall, det yttrande som på frivillig basis har inhämtats i enlighet med punkt 5 i denna artikel från de behöriga myndigheter som i enlighet med direktiv (EU) 2022/2555 har utsetts eller inrättats till ansvariga för tillsynen av en väsentlig eller viktig entitet om inte annat följer av det direktivet, som har klassificerats som kritisk tredjepartsleverantör av IKT-tjänster.

De behöriga myndigheterna ska ge finansiella entiteter den tid som krävs för att de ska kunna anpassa sina kontraktsmässiga arrangemang med kritiska tredjepartsleverantörer av IKT-tjänster i syfte att undvika negativa effekter på den digitala operativa motståndskraften och för att de ska kunna införa sådana exitstrategier och övergångsplaner som avses i artikel 28.

9. Det beslut som avses i punkt 6 i denna artikel ska meddelas medlemmarna i det tillsynsforum som avses i artikel 32.4 a, b och c och det gemensamma tillsynsnätverket.

De kritiska tredjepartsleverantörer av IKT-tjänster som påverkas av de beslut som avses i punkt 6 ska samarbeta fullt ut med de berörda finansiella entiteterna, särskilt i samband med tillfälligt upphävande eller uppsägning av deras kontraktsmässiga arrangemang.

10. De behöriga myndigheterna ska regelbundet informera den ledande tillsynsmyndigheten om de metoder och åtgärder som de har vidtagit i sina tillsynsuppgifter när det gäller finansiella entiteter samt om de kontraktsmässiga arrangemang som finansiella entiteter har ingått om kritiska tredjepartsleverantörer av IKT-tjänster helt eller delvis inte har godtagit rekommendationerna till dem från den ledande tillsynsmyndigheten.

11. Den ledande tillsynsmyndigheten får på begäran lämna ytterligare klargöranden om de utfärdade rekommendationerna för att ge de behöriga myndigheterna vägledning i uppföljningsåtgärderna.

Artikel 43

Tillsynsavgifter

1. Den ledande tillsynsmyndigheten ska i enlighet med den delegerade akt som avses i punkt 2 i denna artikel från de kritiska tredjepartsleverantörerna av IKT-tjänster ta ut avgifter som till fullo täcker den ledande tillsynsmyndighetens 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 den gemensamma undersökningsgrupp som avses i artikel 40 samt kostnaderna för den rådgivning som tillhandahålls av de oberoende experter som avses i artikel 32.4 andra stycket i frågor som omfattas av direkt tillsynsverksamhet.

Det avgiftsbelopp som tas ut av en kritisk tredjepartsleverantör av IKT-tjänster ska täcka alla kostnader för fullgörandet av de uppgifter som anges i detta avsnitt och stå i proportion till leverantörens omsättning.

2. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 57 för att komplettera denna förordning genom att senast den 17 juli 2024 fastställa avgiftsbeloppen och hur de ska betalas.

Artikel 44

Internationellt samarbete

1. Utan att det påverkar tillämpningen av artikel 36 får EBA, Esma och Eiopa, i enlighet med artikel 33 i förordningarna (EU) nr 1093/2010, (EU) nr 1095/2010 och (EU) nr 1094/2010, 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 och den inre marknadens funktion.

KAPITEL VI

Arrangemang för informationsutbyte

Artikel 45

Arrangemang för utbyte av information och underrättelser om cyberhot

1. Finansiella entiteter 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 finansiella entiteters digitala operativa motståndskraft, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra cyberhotens spridningsförmåga, varvid försvarsförmåga, metoder för att upptäcka hot, begränsningsstrategier eller åtgärds- och återställningsfaser stöds,

b) äger rum inom betrodda grupper av finansiella entiteter,

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 i enlighet med förordning (EU) 2016/679 och riktlinjer för konkurrenspolitiken.

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 på vilket sätt dessa kan knytas till arrangemangen för informationsutbyte, om deltagandet av tredjepartsleverantörer av IKT-tjänster och om operativa delar, inbegripet användningen av särskilda it-plattformar.

3. Finansiella entiteter 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 så har skett.

KAPITEL VII

Behöriga myndigheter

Artikel 46

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 denna förordning säkerställas av följande behöriga myndigheter i enlighet med de befogenheter som tilldelats genom respektive rättsakt:

a) För kreditinstitut och för institut undantagna enligt direktiv 2013/36/EU: den behöriga myndighet som har utsetts i enlighet med artikel 4 i det direktivet. För kreditinstitut som har klassificerats som betydande i enlighet med artikel 6.4 i förordning (EU) nr 1024/2013: ECB i enlighet med de befogenheter och uppgifter som har tilldelats genom den förordningen.

b) För betalningsinstitut, inbegripet betalningsinstitut undantagna enligt direktiv (EU) 2015/2366, institut för elektroniska pengar, inbegripet de som är undantagna enligt direktiv 2009/110/EG, och leverantörer av kontoinformationstjänster som avses i artikel 33.1 i direktiv (EU) 2015/2366: den behöriga myndighet som har utsetts i enlighet med artikel 22 i direktiv (EU) 2015/2366.

c) För värdepappersföretag: den behöriga myndighet som har utsetts i enlighet med artikel 4 i Europaparlamentets och rådets direktiv (EU) 2019/2034 ([38]).

d) För leverantörer av kryptotillgångstjänster som har auktoriserats enligt förordningen om kryptotillgångar och emittenter av tillgångsanknutna token: den behöriga myndighet som har utsetts i enlighet med de relevanta bestämmelserna i den förordningen.

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

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

g) För handelsplatser och leverantörer av datarapporteringstjänster: den behöriga myndighet som har utsetts i enlighet med artikel 67 i direktiv 2014/65/EU och den behöriga myndigheten enligt definitionen i artikel 2.1.18 i förordning (EU) nr 600/2014.

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

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

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

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

l) 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.

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

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

o) För administratörer av kritiska referensvärden: den behöriga myndighet som har utsetts i enlighet med artiklarna 40 och 41 i förordning (EU) 2016/1011.

([38]) Europaparlamentets och rådets direktiv (EU) 2019/2034 av den 27 november 2019 om tillsyn av värdepappersföretag och om ändring av direktiven 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU och 2014/65/EU (EUT L 314, 5.12.2019, s. 64).

p) För leverantörer av gräsrotsfinansieringstjänster: den behöriga myndighet som har utsetts i enlighet med artikel 29 i förordning (EU) 2020/1503.

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

Artikel 47

Samarbete med strukturer och myndigheter som har inrättats genom direktiv (EU) 2022/2555

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 14 i direktiv (EU) 2022/2555 får de europeiska tillsynsmyndigheterna och de behöriga myndigheterna delta i samarbetsgruppens verksamhet i frågor som rör deras tillsynsverksamhet i samband med finansiella entiteter. De europeiska tillsynsmyndigheterna och de behöriga myndigheterna får begära att bli inbjudna att delta i samarbetsgruppens verksamhet i väsentliga eller viktiga frågor som rör entiteter om inte annat följer av direktiv (EU) 2022/2555 och som har klassificerats som kritiska tredjepartsleverantörer av IKT-tjänster enligt artikel 31 i denna förordning.

2. De behöriga myndigheterna får när så är lämpligt samråda och utbyta information med den gemensamma kontaktpunkten och de CSIRT-enheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555.

3. De behöriga myndigheterna får när så är lämpligt begära relevant teknisk rådgivning och tekniskt stöd från de behöriga myndigheter som har utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555 och ingå samarbetsarrangemang som gör det möjligt att inrätta effektiva och snabba samordningsmekanismer.

4. De arrangemang som avses i punkt 3 i denna artikel kan bland annat ange förfarandena för samordning av tillsynsverksamheten i samband med väsentliga eller viktiga entiteter om inte annat följer av] direktiv (EU) 2022/2555 och som har klassificerats som kritiska tredjepartsleverantörer av IKT-tjänster enligt artikel 31 i denna förordning, bl.a. för genomförande av utredningar och inspektioner på plats i enlighet med nationell rätt och för mekanismer för informationsutbyte mellan de behöriga myndigheterna enligt denna förordning och de behöriga myndigheter som har utsetts eller inrättats i enlighet med det direktivet, inbegripet tillgång till information som de senare myndigheterna har begärt.

Artikel 48

Samarbete mellan myndigheter

1. De behöriga myndigheterna ska ha ett nära samarbete sinsemellan och, i tillämpliga fall, med den ledande tillsynsmyndigheten.

2. De behöriga myndigheterna och den ledande tillsynsmyndigheten ska i god tid ömsesidigt utbyta all relevant information om kritiska tredjepartsleverantörer av IKT-tjänster som är nödvändig för att de ska kunna utföra sina respektive uppgifter enligt denna förordning, särskilt om identifierade risker, strategier och åtgärder som vidtas som en del av den ledande tillsynsmyndighetens tillsynsuppgifter.

Artikel 49

Övningar, kommunikation och samarbete mellan finansiella sektorer

1. De europeiska tillsynsmyndigheterna får, genom den gemensamma kommittén och i samarbete med behöriga myndigheter, resolutionsmyndigheter som avses i artikel 3 i direktiv 2014/59/EU, ECB, Gemensamma resolutionsnämnden, när det gäller information som rör entiteter som omfattas av tillämpningsområdet för förordning (EU) nr 806/2014, ESRB och Enisa, när så är lämpligt, 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 cyberangrepp i syfte att utveckla kommunikationskanaler och gradvis möjliggöra en effektiv samordnad reaktion på unionsnivå i händelse av en allvarlig 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. De behöriga myndigheterna, de europeiska tillsynsmyndigheterna och ECB ska ha ett nära samarbete och utbyta information för att fullgöra sina uppgifter enligt artiklarna 47–54. De ska nära samordna sin tillsyn för att identifiera och åtgärda överträdelser av denna förordning, utarbeta och främja bästa praxis, underlätta samarbete, främja en konsekvent tolkning och tillhandahålla bedömningar över jurisdiktionsgränserna om det uppstår meningsskiljaktigheter.

Artikel 50

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 följande befogenheter:

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 inspektioner på plats, som ska omfatta men inte vara begränsade till att

   i) kalla till sig företrädare för finansiella entiteter och be dem om muntliga eller skriftliga förklaringar angående sakförhållanden eller dokument som rör föremålet för och syftet med utredningen samt nedteckna svaren,

   ii) höra vilken annan fysisk eller juridisk person som helst som går med på att höras i syfte att samla in information om föremålet för utredningen.

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

3. Utan att det påverkar medlemsstaternas rätt att ålägga straffrättsliga påföljder i enlighet med artikel 52 ska medlemsstaterna fastställa regler om lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av denna förordning och säkerställa 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 vilket det krävs att den fysiska eller juridiska personen upphör med det agerande som strider mot denna förordning 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 vilken typ av åtgärd som helst, även av ekonomisk art, för att säkerställa att finansiella entiteter 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, inbegripet offentliga uttalanden, med uppgift om den fysiska eller juridiska personens identitet och överträdelsens art.

5. Om 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 rätt är ansvariga för överträdelsen.

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

Artikel 51

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 50 i enlighet med sina nationella rättsliga ramar, när så är lämpligt, på något av följande sätt:

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 50, ta hänsyn till i vilken utsträckning överträdelsen är avsiktlig eller beror på försummelse och till 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 styrkan hos 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 den fysiska eller juridiska 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 52

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 53

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 den 17 januari 2025. Medlemsstaterna ska utan onödigt dröjsmål underrätta kommissionen, Esma, EBA och Eiopa om eventuella ändringar av dessa.

Artikel 54

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 och personuppgifter är oproportionellt, inbegripet riskerna när det gäller skyddet av personuppgifter, kan hota stabiliteten på de finansiella marknaderna eller äventyra en pågående brottsutredning eller, i den mån detta kan bestämmas, vålla den berörda personen oproportionell skada, ska den behöriga myndigheten vidta någon av följande åtgärder i fråga om beslutet om att ålägga en administrativ sanktion:

a) Skjuta upp offentliggörandet av beslutet 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 om offentliggörandet inte 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 efterföljande 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 endast under den tidsperiod som är nödvändig vid tillämpning av denna artikel. Denna period får inte överstiga fem år efter offentliggörandet.

Artikel 55

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 tillämpas för alla personer som arbetar eller har arbetat för de behöriga myndigheterna enligt 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, inbegripet informationsutbyte mellan behöriga myndigheter enligt denna förordning och behöriga myndigheter som har utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555, får inte lämnas ut till någon annan person eller myndighet utom när detta föreskrivs i unionsrätt eller nationell rätt.

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.

Artikel 56

Dataskydd

1. De europeiska tillsynsmyndigheterna och de behöriga myndigheterna får endast behandla personuppgifter om det är nödvändigt för att de ska kunna fullgöra sina respektive skyldigheter och uppgifter enligt denna förordning, särskilt när det gäller utredning, inspektion, begäran om information, kommunikation, offentliggörande, utvärdering, verifiering, bedömning och utarbetande av tillsynsplaner. Personuppgifterna ska behandlas i enlighet med förordning (EU) 2016/679 eller förordning (EU) 2018/1725, beroende på vilken som är tillämplig.

2. Utom där annat föreskrivs i andra sektorsspecifika rättsakter ska de personuppgifter som avses i punkt 1 lagras till dess att de tillämpliga tillsynsuppgifterna fullgjorts och under alla omständigheter i högst 15 år, utom i fall av pågående domstolsförfaranden som kräver ytterligare lagring av sådana uppgifter.

KAPITEL VIII

Delegerade akter

Artikel 57

Utövande av delegeringen

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 31.6 och 43.2 ska ges till kommissionen för en period på fem år från och med den 17 januari 2024. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

3. Den delegering av befogenhet som avses i artiklarna 31.6 och 43.2 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 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 av den 13 april 2016 om bättre lagstiftning.

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

6. En delegerad akt som antas enligt artiklarna 31.6 och 43.2 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på tre 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 tre månader på Europaparlamentets eller rådets initiativ.

KAPITEL IX

Övergångs- och slutbestämmelser

Avsnitt I

Artikel 58

Översynsklausul

1. Senast den 17 januari 2028 ska kommissionen, efter samråd med de europeiska tillsynsmyndigheterna och ESRB, när så är lämpligt, genomföra en översyn och överlämna en rapport till Europaparlamentet och rådet, när så är lämpligt åtföljd av ett lagstiftningsförslag. Översynen ska minst omfatta följande:

a) Kriterierna för att klassificera tredjepartsleverantörer av IKT-tjänster som kritiska i enlighet med artikel 31.2.

b) Den frivilliga karaktären hos den anmälan av betydande cyberhot som avses i artikel 19.

c) Den ordning som avses i artikel 31.12 och de befogenheter för den ledande tillsynsmyndigheten som föreskrivs i artikel 35.1 d iv första strecksatsen, i syfte att utvärdera om dessa bestämmelser är ändamålsenliga för att säkerställa en effektiv tillsyn av kritiska tredjepartsleverantörer av IKT-tjänster som är etablerade i ett tredjeland och om det är nödvändigt att etablera ett dotterföretag i unionen.

   Vid tillämpning av första stycket i detta led ska översynen omfatta en analys av den ordning som avses i artikel 31.12, inbegripet vad gäller åtkomst för finansiella entiteter i unionen till tjänster från tredjeländer och tillgång till sådana tjänster på marknaden i unionen, och den ska ta hänsyn till den fortsatta utvecklingen på marknaderna för de tjänster som omfattas av denna förordning, finansiella entiteters och de finansiella tillsynsmyndigheternas praktiska erfarenheter av tillämpningen respektive tillsynen av den ordningen samt all relevant utveckling inom reglering och tillsyn som äger rum på internationell nivå.

d) Lämpligheten i att i tillämpningsområdet för denna förordning inkludera sådana finansiella entiteter som avses i artikel 2.3 e som använder automatiska försäljningssystem, mot bakgrund av den framtida marknadsutvecklingen när det gäller användningen av sådana system.

e) Det gemensamma tillsynsnätverkets funktion och ändamålsenlighet när det gäller att stödja konsekvens i tillsynen och effektivitet i informationsutbytet inom tillsynsramen.

2. I samband med översynen av direktiv (EU) 2015/2366 ska kommissionen bedöma behovet av ökad cyberresiliens i betalningssystem och betalningshantering och lämpligheten i att utvidga tillämpningsområdet för denna förordning till att även omfatta betalningssystemsoperatörer och enheter som deltar i betalningshantering. Mot bakgrund av denna bedömning ska kommissionen, som en del av översynen av direktiv (EU) 2015/2366, lägga fram en rapport för Europaparlamentet och rådet senast den 17 juli 2023.

Baserat på den översynsrapporten och efter samråd med de europeiska tillsynsmyndigheterna, ECB och ESRB får kommissionen, när så är lämpligt och som en del av det lagstiftningsförslag som den får anta i enlighet med artikel 108 andra stycket i direktiv (EU) 2015/2366, lägga fram ett förslag för att säkerställa att alla betalningssystemsoperatörer och entiteter som deltar i betalningshantering är föremål för lämplig tillsyn, samtidigt som hänsyn tas till den befintliga tillsynen av centralbanken.

3. Senast den 17 januari 2026 ska kommissionen, efter samråd med de europeiska tillsynsmyndigheterna och kommittén för europeiska tillsynsorgan för revisorer, genomföra en översyn och överlämna en rapport till Europaparlamentet och rådet, vid behov åtföljd av ett lagstiftningsförslag, om huruvida det är lämpligt att stärka kraven för lagstadgade revisorer och revisionsföretag när det gäller digital operativ motståndskraft genom att inkludera lagstadgade revisorer och revisionsföretag i tillämpningsområdet för denna förordning eller genom att ändra Europaparlamentets och rådets direktiv 2006/43/EG ([39]).

Avsnitt II

Ändringar

Artikel 59

Ändringar av förordning (EG) nr 1060/2009

Förordning (EG) nr 1060/2009 ska ändras på följande sätt:

1. I bilaga I avsnitt A punkt 4 ska 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) 2022/2554 (*).

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1)."

2. I bilaga III ska punkt 12 ersättas med följande:

"12. Ett kreditvärderingsinstitut bryter mot artikel 6.2, jämförd med bilaga I avsnitt A punkt 4, om det inte tillämpar sunda förfaranden för förvaltning eller redovisning eller inte har mekanismer för internkontroll eller effektiva riskbedömningsmetoder samt effektiva kontroll- eller skyddssystem för förvaltningen av sina IKT-system i enlighet med förordning (EU) 2022/2554, eller om det inte tillämpar eller upprätthåller beslutsförfaranden och organisationsstrukturer enligt vad som krävs i den punkten."

Artikel 60

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) 2022/2554 (*).

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022. s. 1)."

([39]) Europaparlamentets och rådets direktiv 2006/43/EG av den 17 maj 2006 om lagstadgad revision av årsbokslut och sammanställd redovisning och om ändring av rådets direktiv 78/660/EEG och 83/349/EEG samt om upphävande av rådets direktiv 84/253/EEG (EUT L 157, 9.6.2006, s. 87).

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-kontinuitetspolicy och åtgärds- och återställningsplaner avseende IKT som har upprättats och genomförts i enlighet med förordning (EU) 2022/2554, för att säkerställa verksamheten, snabbt återuppta den och fullgöra den centrala motpartens skyldigheter.”

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

”3. 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-kontinuitetspolicy och IKT-katastrofplanerna.”

3. I artikel 56.3 ska 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) 2022/2554.

2. Ett transaktionsregister ska utforma, tillämpa och upprätthålla tillräckliga riktlinjer för kontinuerlig verksamhet och en katastrofplan, inbegripet IKT-kontinuitetspolicy och åtgärds- och återställningsplaner avseende IKT som har upprättats i enlighet med förordning (EU) 2022/2554, för att säkerställa verksamheten, snabbt kunna återuppta den och fullgöra transaktionsregistrets skyldigheter.”

5. I artikel 80 ska punkt 1 utgå.

6. I bilaga I ska avsnitt II ändras på följande sätt:

a) Leden a och b ska ersättas med följande:

”a) Ett transaktionsregister bryter mot artikel 79.1 om det inte identifierar operativa riskkällor eller inte minimerar dessa risker genom att utveckla lämpliga system, kontroller och förfaranden, inbegripet IKT-system som förvaltas i enlighet med förordning (EU) 2022/2554.

b) Ett transaktionsregister bryter mot artikel 79.2 om det inte utformar, tillämpar eller upprätthåller en lämplig strategiplan för kontinuerlig verksamhet och en katastrofplan som har upprättats i enlighet med förordning (EU) 2022/2554, för att säkerställa verksamheten, snabbt kunna återuppta den och fullgöra transaktionsregistrets skyldigheter.”

b) Led c ska utgå.

7. Bilaga III ska ändras på följande sätt:

a) Avsnitt II ska ändras på följande sätt:

i) Led c ska ersättas med följande:

”c) En central motpart i kategori 2 överträder artikel 26.3 om den inte upprätthåller en organisationsstruktur som säkerställer en kontinuerlig och väl fungerande verksamhet och tillhandahållande av tjänster, eller om den inte använder lämpliga och proportionella system, resurser eller förfaranden, inbegripet IKT-system som förvaltas i enlighet med förordning (EU) 2022/2554.”

ii) Led f ska utgå.

b) I avsnitt III ska led a ersättas med följande:

”a) En central motpart i kategori 2 överträder artikel 34.1 om den inte utformar, genomför eller upprätthåller lämpliga riktlinjer för kontinuerlig verksamhet och en åtgärds- och återställningsplan som har upprättats i enlighet med förordning (EU) 2022/2554, för att säkerställa verksamheten, snabbt kunna återuppta den och fullgöra den centrala motpartens skyldigheter, vilket åtminstone ger möjlighet att återställa alla transaktioner till vad de var vid tidpunkten för störningen, så att den centrala motpartens verksamhet är fortsatt säker och den kan fullfölja avvecklingen vid fastställt datum.”

Artikel 61

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-processer och IKT-strategier som har inrättats och förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*), 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) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).”

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-kontinuitetspolicy och åtgärds- och återställningsplaner avseende IKT som har inrättats i enlighet med förordning (EU) 2022/2554, 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 föreskrivs i artikel 12.5 och 12.7 i förordning (EU) 2022/2554.”

4. Punkt 6 ska ersättas med följande:

”6. 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-risk.”

5. I punkt 7 ska första stycket ersättas med följande:

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

Artikel 62

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 ersättas med följande:

   ”4. APA ska uppfylla de krav avseende säkerhet i nätverks- och informationssystem som fastställs i Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

   (*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).”

   b) Punkt 8 c ska ersättas med följande:

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

2. Artikel 27h ska ändras på följande sätt:

   a) Punkt 5 ska ersättas med följande:

   ”5. CTP ska uppfylla de krav avseende säkerhet i nätverks- och informationssystem som fastställs i förordning (EU) 2022/2554.”

   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 ersättas med följande:

   ”3. ARM ska uppfylla de krav avseende säkerhet i nätverks- och informationssystem som fastställs i förordning (EU) 2022/2554.”

   b) Punkt 5 b ska ersättas med följande:

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

Artikel 63

Ändringar av förordning (EU) 2016/1011

I artikel 6 i förordning (EU) 2016/1011 ska följande punkt läggas till:

”6. För kritiska referensvärden ska administratören tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för internkontroll och effektiva riskbedömningsmetoder samt effektiva kontroll- och skyddssystem för förvaltningen av IKT-system i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

(*) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1).”

Artikel 64

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 17 januari 2025.

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

Utfärdad i Strasbourg den 14 december 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	M. BEK
Ordförande	*Ordförande*