III

(Förberedande akter)

EUROPEISKA CENTRALBANKEN

EUROPEISKA CENTRALBANKENS YTTRANDE

av den 4 juni 2021

om ett förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn

(CON/2021/20)

(2021/C 343/01)

Inledning och rättslig grund

Den 22, 23 och 29 december 2020 mottog Europeiska centralbanken (ECB) en begäran från Europeiska unionens råd respektive Europaparlamentet om ett yttrande över ett förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014 ([1]) (nedan kallad *förslaget till förordning*) och förslaget till direktiv om ändring av direktiv 2006/43/EG, 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 och (EU) 2016/2341 ([2]) (nedan kallat *förslaget till ändringsdirektiv* och, tillsammans med förslaget till förordning, *förslagen till rättsakter*).

ECB:s behörighet att avge ett yttrande grundas på artiklarna 127.4 och 282.5 i fördraget om Europeiska unionens funktionssätt eftersom förslagen till rättsakter innehåller bestämmelser som berör ECB:s behörighetsområden, särskilt att utforma och genomföra den monetära politiken, främja väl fungerande betalningssystem, medverka till de behöriga myndigheternas smidiga genomförande av riktlinjerna för det finansiella systemets stabilitet samt ECB:s uppgifter i fråga om tillsyn över kreditinstitut i enlighet med artikel 127.2 första och fjärde strecksatsen och artikel 127.5 och 127.6 i fördraget. I enlighet med artikel 17.5 första meningen i arbetsordningen för Europeiska centralbanken har detta yttrande antagits av ECB-rådet.

1. Allmänna kommentarer

1.1 ECB välkomnar förslaget till förordning som syftar till att öka finanssektorns cybersäkerhet och operativa motståndskraft. ECB välkomnar särskilt att förslaget till förordning syftar till att undanröja hinder för upprättandet av den inre marknaden för finansiella tjänster och förbättra dess funktion genom att se till att de tillämpliga bestämmelserna för riskhantering, rapportering, testning inom IKT-området och IKT-risker i samband med tredje parter är harmoniserade. Vidare välkomnar ECB att förslaget till förordning syftar till att rationalisera och harmonisera överlappande lagstadgade krav eller tillsynsförväntningar som finansiella enheter för närvarande omfattas av enligt unionsrätten.

1.2 Vad gäller finansiella enheter som har identifierats som leverantörer av samhällsviktiga tjänster ([3]) förstår ECB det som att förslaget till förordning utgör sektorsspecifik lagstiftning (*lex specialis*) i den mening som avses i artikel 1.7 i Europaparlamentets och rådets direktiv (EU) 2016/1148 ([4]) (nedan kallat *direktivet om nätverks- och informationssystem*); detta innebär att kraven enligt förslaget till förordning i princip ska ha företräde framför direktivet om nätverks- och informationssystem. I praktiken ska finansiella enheter som har identifierats som leverantörer av samhällsviktiga tjänster ([5]) bland annat rapportera incidenter enligt förslaget till förordning och

([1]) COM (2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Se artikel 1.2 i förslaget till förordning.
([4]) 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).
([5]) Se artikel 5 i direktivet om nätverks- och informationssystem.

inte enligt direktivet om nätverks- och informationssystem. ECB välkomnar att finansiella enheter omfattas av färre potentiella överlappande krav i fråga om incidentrapportering, men samspelet mellan förslaget till förordning och direktivet om nätverks- och informationssystem bör övervägas ytterligare. Enligt förslaget till förordning kan t.ex. en tredjepartsleverantör av IKT-tjänster ([6]) omfattas av rekommendationer som har utfärdats av den ledande tillsynsmyndigheten ([7]). Samtidigt kan samma tredjepartsleverantör av IKT-tjänster klassificeras som leverantör av samhällsviktiga tjänster enligt direktivet om nätverks- och informationssystem och omfattas av bindande instruktioner som har utfärdats av den behöriga myndigheten ([8]). Detta kan innebära att tredjepartsleverantörer av IKT-tjänster omfattas av motstridiga rekommendationer utfärdade enligt förslaget till förordning och bindande instruktioner utfärdade enligt direktivet om nätverks- och informationssystem. ECB föreslår att unionens lagstiftande organ ytterligare ska överväga om det förekommer inkonsekvenser mellan förslaget till förordning och direktivet om nätverks- och informationssystem som kan motverka harmoniseringen och minskningen av överlappande och motstridiga krav för finansiella enheter.

1.3 Som ECB tolkar förslaget till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 ([9]) (nedan kallat *förslaget till det andra direktivet om nätverks- och informationssystem*) kommer ”tillbud” ([10]) att omfattas av rapporteringskrav ([11]). I skäl 39 i förslaget till det andra direktivet om nätverks- och informationssystem hänvisas visserligen till innebörden av termen ”tillbud”, men det är oklart om avsikten är att kräva att tillbud ska rapporteras av de finansiella enheter som anges i artikel 2 i förslaget till förordning. I detta avseende, och med tanke på att tillbud kan identifieras först sedan de har inträffat, skulle ECB välkomna att bli underrättad om betydande tillbud i rimlig tid, så som för närvarande är fallet för cyberincidenter. ECB föreslår en ökad samordning mellan förslaget till förordning och förslaget till det andra direktivet om nätverks- och informationssystem, så att det klargörs exakt vilka uppgifter som varje finansiell enhet ska rapportera enligt dessa separata, men sammanhängande unionsrättsakter. Samtidigt skulle ”tillbud” behöva definieras och bestämmelser som klargör deras betydelse behöva utarbetas.

1.4 ECB välkomnar att finansiella enheter uppmuntras till frivilligt utbyte av underrättelser om cyberhot i syfte att förbättra och stärka sin ställning i fråga om cyberresiliens. ECB har för egen del bistått med det marknadsdrivna initiativet för informationsutbyte av underrättelser om cyberhot (CIISI-EU) och har tillhandahållit allmänt tillgängliga modeller för hur ett sådant initiativ kan byggas upp och främjas ([12]).

1.5 ECB stöder de behöriga myndigheternas samarbete i fråga om förslaget till förordning samt de europeiska tillsynsmyndigheterna och enheterna för hantering av IT-säkerhetsincidenter (Computer Security Incident Response Teams, CSIRT-enheter) ([13]). Det är viktigt att utbyta information för att säkerställa unionens operativa motståndskraft, eftersom myndigheternas informationsutbyte och samarbete kan bidra till att förhindra IT-attacker och bidra till att minska spridningen av IKT-hot. Det bör eftersträvas att det råder en samsyn kring IKT-relaterade risker och säkerställas att dessa risker bedöms på ett enhetligt sätt i hela EU. Det är ytterst viktigt att de behöriga myndigheterna utbyter information med den gemensamma kontaktpunkten ([14]) och de nationella CSIRT-enheterna ([15]) enbart om det finns tydligt fastställda mekanismer för klassificering och informationsutbyte samt lämpliga skyddsåtgärder för att säkerställa konfidentialitet.

1.6 Slutligen skulle ECB välkomna att det införs regler om personuppgifter och datalagring i enlighet med förslaget till förordning. Lagringsperiodens längd bör fastställas med hänsyn till de behöriga myndigheternas utredning, kontroll, begäran om information, kommunikation, offentliggörande, utvärdering, verifiering, bedömning och utarbetande av övervaknings- eller tillsynsplaner som de kan

([6]) Se artikel 3.15 i förslaget till förordning.
([7]) Se artikel 31.1 d i förslaget till förordning.
([8]) Se artikel 15.3 i direktivet om nätverks- och informationssystem.
([9]) COM(2020) 823 final.
([10]) Händelser som potentiellt skulle ha kunnat orsaka skada, men som framgångsrikt hindrades från att utvecklas fullt ut; se skäl 39 i det andra direktivet om nätverks- och informationssystem.
([11]) Se artikel 11 i det andra direktivet om nätverks- och informationssystem.
([12]) Cyber threat Intelligence Information Sharing Initiative (CIISI-EU), finns på ECB:s webbplats www.ecb.europa.eu.
([13]) Se artikel 42 i förslaget till förordning.
([14]) Se artikel 8.3 i direktivet om nätverks- och informationssystem.
([15]) Se även artiklarna 11, 26 och 27 i det andra direktivet om nätverks- och informationssystem.

behöva utföra som del av sina förpliktelser och skyldigheter enligt förslaget till förordning. I detta avseende skulle en lagringsperiod på 15 år vara lämplig. Denna datalagringsperiod skulle kunna förkortas eller förlängas, beroende på omständigheterna. I detta avseende föreslår ECB att unionens lagstiftande organ även ska beakta principen om uppgiftsminimering samt behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ([16]) när de utarbetar den relevanta bestämmelsen om personuppgifter och datalagring.

2. **Specifika kommentarer om tillsyn samt clearing och avveckling av värdepapper**

2.1 *ECBS och Eurosystemets tillsynsbefogenheter*

2.1.1 I fördraget och stadgan för Europeiska centralbankssystemet och Europeiska centralbanken. (nedan kallad *ECBS-stadgan*) föreskrivs att Eurosystemet ska övervaka clearing- och betalningssystemen, vilket är nära kopplat till dess grundläggande penningpolitiska uppgifter. Av artikel 127.2 fjärde strecksatsen i fördraget samt artikel 3.1 i ECBS-stadgan framgår att en annan grundläggande uppgift för Europeiska centralbankssystemet (ECBS) är att främja väl fungerande betalningssystem. När denna grundläggande uppgift utförs får ECB och de nationella centralbankerna ställa anordningar till förfogande och ECB får utfärda förordningar för att säkerställa effektiva och sunda clearing- och betalningssystem inom unionen och i förbindelser med tredje land ([17]). I enlighet med sin övervakande roll antog ECB Europeiska centralbankens förordning (EU) nr 795/2014 (ECB/2014/28) (nedan kallad *SIPS-förordningen*) ([18]). Genom SIPS-förordningen genomförs, i föreskrivande form, de principer för finansmarknadens infrastrukturer som upprättades i april 2012 av kommittén för betalnings- och avvecklingssystem (PSSC) och International Organization of Securities Commissions (Iosco) ([19]). Dessa principer är rättsligt bindande och omfattar systemviktiga betalningssystem såväl för större betalningar som för massbetalningar, oavsett om de utförs av en nationell centralbank i Eurosystemet eller av en privat enhet. I Eurosystemets tillsynsram ([20]) anges att betalningsinstrument utgör en ”integrerad del av betalningssystemen” och de inkluderas därmed i tillsynen. Tillsynsramen för betalningsinstrument genomgår för närvarande en översyn ([21]). Enligt denna ram definieras ett betalningsinstrument (t. ex. ett kort, en överföring, en autogirering, en överföring av elektroniska pengar och en digital betalningstoken ([22])) som personlig(a) anordning(ar) och/eller rutiner som betaltjänstanvändaren och betaltjänstleverantören har träffat avtal om och som används av betaltjänstanvändaren för att initiera en betalningsorder ([23]).

2.1.2 Mot denna bakgrund välkomnar ECB att systemoperatörer enligt definitionen i artikel 2 p i Europaparlamentets och rådets direktiv 98/26/EG ([24]), betalningssystem (även de som drivs av centralbanker), betalningsordningar och betalningsarrangemang undantas från tillämpningsområdet för förslaget till förordning, med tanke på

([16]) Se artiklarna 4 b och 13 i 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).

([17]) Se artikel 22 i ECBS-stadgan.

([18]) Europeiska centralbankens förordning (EU) nr 795/2014 av den 3 juli 2014 om krav på övervakning av systemviktiga betalningssystem (ECB/2014/28) (EUT L 217, 23.7.2014, s. 16).

([19]) Finns på webbplatsen för Banken för internationell betalningsutjämning, www.bis.org.

([20]) Eurosystemets tillsynsram, reviderad version (juli 2016), finns på ECB:s webbplats www.ecb.europa.eu.

([21]) Se Eurosystemets reviderade och konsoliderade tillsynsram för elektroniska betalningsinstrument, betalningsordningar och betalningsarrangemang (PISA-ramverket), finns på ECB:s webbplats www.ecb.europa.eu.

([22]) En digital betalningstoken är en digital värderepresentation som har bakomliggande fordringar eller tillgångar som bokförs på annat håll och gör det möjligt att överföra värde mellan slutanvändarna. Beroende på den underliggande utformningen för digitala betalningstoken kan värde överföras utan att detta nödvändigtvis behöver involvera en central tredje part och/eller betalningskonton.

([23]) Överföring av värde: ”Åtgärd som initieras av betalaren eller på dennes vägnar eller av betalningsmottagaren och som består i överföring av medel eller digitala betalningstoken, placering eller uttag av medel till/på/från ett användarkonto, oberoende av eventuella underliggande förpliktelser mellan betalaren och betalningsmottagaren. Överföringen kan omfatta en eller flera betaltjänstleverantörer.” Denna definition av ”överföring av värde” enligt PISA-ramverket skiljer sig dessutom från det som definieras som överföring av ”medel” enligt 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). Såsom ”betalningsinstrument” definieras i det direktivet kan ”överföring av värde” enbart avse överföring av ”medel”. Enligt det direktivet omfattar ”medel” inte digitala betalningstoken om inte dessa token kan klassificeras som elektroniska pengar (eller mer hypotetiskt som kontotillgodohavanden).

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

tillämpningen av ovannämnda tillsynsram. Av dessa skäl bör ECBS behörigheter enligt fördraget och Eurosystemets behörigheter enligt SIPS-förordningen tydligt anges i skälen och i förslaget till förordning.

2.1.3 På samma sätt välkomnar ECB att de tredjepartsleverantörer av IKT-tjänster som omfattas av tillsynsmekanismer som har inrättats till stöd för uppgifter som avses i artikel 127.2 i fördraget ([25]) enligt förslaget till förordning ska undantas från tillsynsramen. I samband med detta skulle ECB vilja understryka att centralbanker inom ECBS som agerar i egenskap av monetära myndigheter ([26]) och Eurosystemet när det tillhandahåller tjänster via Target2, Target2-Securites (T2S) ([27]) och Target Instant Payment Settlement (TIPS) ([28]) inte ingår i tillämpningsområdet för förslaget till förordning och inte heller kan anses utgöra tredjepartsleverantörer av IKT-tjänster, vilket innebär att de skulle kunna klassificeras som kritiska tredjepartsleverantörer av IKT-tjänster vad gäller förslaget till förordning. Eurosystemet utövar tillsyn över T2S i samband med sitt uppdrag att säkerställa effektiva och sunda clearing- och betalningssystem. Esma har vidare klargjort att T2S inte är en kritisk tjänsteleverantör ([29]) i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 909/2014 ([30]) (nedan kallad *förordningen om värdepapperscentraler*). För T2S säkerställs organisatorisk och operativ säkerhet, effektivitet och motståndskraft inte genom förordningen om värdepapperscentraler utan genom den tillämpliga rättsliga, regleringstekniska och operativa ramen samt överenskomna styrningsarrangemang eller T2S.

2.1.4 Eurosystemets tillsynsram ([31]) omfattar dessutom kritiska tjänsteleverantörer såsom Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT är ett aktiebolag med säte i Belgien som erbjuder säkra meddelandetjänster internationellt. Nationale Bank van België/Banque Nationale de Belgique är ledande tillsynsmyndighet för SWIFT och utövar enligt en samarbetsöverenskommelse tillsyn över SWIFT i samarbete med andra centralbanker i G10-länderna, inbegripet ECB. G10-ländernas tillsynsmyndigheter är införstådda med att tillsynsfokus ska ligga på SWIFT:s operativa risk, eftersom detta bedöms vara den riskkategori som i första hand skulle kunna leda till att SWIFT utgör en systemrisk för det finansiella systemet i unionen. I detta avseende har den gemensamma tillsynsgruppen för SWIFT utarbetat en uppsättning principer och förväntningar på hög nivå i fråga om SWIFT, t.ex. riskidentifiering och riskhantering, informationens säkerhet, tillförlitlighet och motståndskraft samt teknikplanering och användarkommunikation. G10-ländernas tillsynsmyndigheter förväntar sig att SWIFT ska följa Guidance on cyber resilience ([32]) (ej översatt till svenska) från kommittén för betalnings- och marknadsinfrastruktur (CPMI) och styrelsen för International Organization of Securities Commissions (Iosco) samt andra internationella IKT-säkerhetsstandarder som sammantaget överträffar de krav som anges i förslaget till förordning.

2.1.5 Om SWIFT och eventuellt andra tjänsteleverantörer som omfattas av Eurosystemets tillsynsram skulle tillhandahålla tjänster som inte omfattas av artikel 127.2 i fördraget, är det inte säkert att de skulle omfattas av förslaget till förordning i egenskap av tredjepartsleverantörer av IKT-tjänster. ECB är därför mycket positiv till att tjänsteleverantörer som redan omfattas av Eurosystemets tillsynsram, vilket bland annat inkluderar SWIFT, utesluts från tillsynsramens tillämpningsområde enligt förslaget till förordning.

([25]) Se artikel 28.5 i förslaget till förordning.

([26]) Se punkt 1.3 i Europeiska centralbanken yttrande av 19 februari 2021 om ett förslag till förordning om marknader för kryptotillgångar och om ändring av direktiv (EU) 2019/1937 (CON/2021/4). Alla ECB:s yttranden publiceras i EUR-Lex.

([27]) Se bilaga IIa till Europeiska centralbankens riktlinje ECB/2012/27 av den 5 december 2012 om ett transeuropeiskt automatiserat system för bruttoavveckling av betalningar i realtid (TARGET2) (EUT L 30, 30.1.2013, s. 1). Europeiska centralbankens riktlinje ECB/2012/13 av den 18 juli 2012 om TARGET2-Securities (EUT L 215, 11.8.2012, s. 19) och Europeiska centralbankens beslut ECB/2011/20 av den 16 november 2011 om detaljerade regler och förfaranden för att genomföra de kriterier enligt vilka värdepapperscentraler ges tillträde till de tjänster som TARGET2-Securities erbjuder (EUT L 319, 2.12.2011, s. 117). Se även ramavtalet för T2S och det kollektiva avtalet.

([28]) Se bilaga IIb till riktlinje ECB/2012/27.

([29]) Se artikel 30.5 i 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) och artikel 68 i kommissionens delegerade förordning (EU) 2017/392 av den 11 november 2016 om komplettering av Europaparlamentets och rådets förordning (EU) nr 909/2014 med avseende på tekniska tillsynsstandarder för auktorisationskrav, tillsynskrav och operativa krav för värdepapperscentraler (EUT L 65, 10.3.2017, s. 48).

([30]) 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).

([31]) Eurosystemets tillsynsram, reviderad version (juli 2016), finns på ECB:s webbplats www.ecb.europa.eu.

([32]) Finns på webbplatsen för Banken för internationell betalningsutjämning, www.bis.org.

2.2 *ECBS befogenheter vad gäller avveckling av värdepapper*

2.2.1 Värdepapperscentraler är noga reglerad finansmarknadsinfrastruktur som övervakas av olika myndigheter i enlighet med förordningen om värdepapperscentraler, som uppställer krav för avvecklingen av finansiella instrument samt regler för värdepapperscentralers organisation och uppförande. Värdepapperscentralerna bör dessutom beakta CPMI-Ioscos *Guidance on cyber resilience* (ej översatt till svenska) som har operationaliserats genom *Cyber resilience oversight expectations for financial market infrastructures* (december 2018) ([33]) . Utöver de tillsynsbefogenheter som tilldelats de nationella behöriga myndigheterna enligt förordningen om värdepapperscentraler, agerar ECBS-medlemmarna som ”relevanta myndigheter”, i sin egenskap av övervakningsmyndighet för värdepappersavvecklingssystem som drivs av värdepapperscentraler, som centralbanker ger ut de mest relevanta valutorna i vilka avveckling sker och som centralbanker i vars räkenskaper kontantdelen av transaktionerna avvecklas ([34]). I detta hänseende anges i skäl 8 i förordningen om värdepapperscentraler att den förordningen inte påverkar ECB:s och de nationella centralbankernas ansvar att säkerställa effektiva och sunda clearing- och betalningssystem inom unionen och i förbindelser med andra länder. I skäl 8 anges också att förordningen om värdepapperscentraler inte bör hindra ECBS-medlemmarna från att få tillgång till information som är relevant för utförandet av deras uppgifter ([35]), inbegripet tillsyn över värdepapperscentraler och annan finansmarknadsinfrastruktur ([36]).

2.2.2 ECBS-medlemmarna fungerar dessutom ofta som avvecklingsagenter för kontantdelen av värdepapperstransaktioner och Eurosystemet erbjuder avvecklingstjänster via T2S till värdepapperscentraler. Eurosystemets övervakning av T2S är kopplad till dess uppdrag att säkerställa effektiva och sunda clearing- och betalningssystem, medan de behöriga och relevanta myndigheterna för värdepapperscentraler strävar efter att säkerställa att de fungerar smidigt, att avvecklingen är säker och effektiv samt att finansmarknaderna inom respektive jurisdiktioner fungerar väl.

2.2.3 Enligt förslaget till förordning ([37]) ska centralbankerna i ECBS inte vara med och utarbeta tekniska standarder där IKT-risker specificeras. I förslaget till förordning ([38]) anges också att relevanta myndigheter inte ska underrättas om IKT-relaterade incidenter. En centralbank i ECBS bör involveras i motsvarande utsträckning som för närvarande sker enligt förordningen om värdepapperscentraler och de relevanta myndigheterna bör underrättas om IKT-relaterade incidenter. Eurosystemet är relevant myndighet för alla värdepapperscentraler i euroområdet samt för flera andra värdepapperscentraler i EU. Centralbankerna i ECBS skulle behöva bli underrättade om IKT-relaterade incidenter som är relevanta för utförandet av deras uppgifter, inklusive tillsyn över värdepapperscentraler och annan finansmarknadsinfrastruktur. Värdepapperscentralerna exponeras mot risker, däribland IKT-risker, som kan utgöra hota välfungerande värdepapperscentraler. IKT-risker är därför viktiga för de relevanta myndigheterna, som bör få en fullständig och detaljerad översikt över dessa risker för att kunna bedöma dem och påverka värdepapperscentralernas riskhanteringsstrategi. Kraven för IKT-risker bör inte vara mindre restriktiva i förslaget till förordning än vad de är i förordningen om värdepapperscentraler och aktuella tekniska tillsynsstandarder inom detta område.

2.2.4 Unionens lagstiftande organ bör dessutom klargöra samspelet mellan förslaget till förordning ([39]) och de tekniska tillsynsstandarder som kompletterar förordningen om värdepapperscentraler. Det är framför allt oklart om en värdepapperscentral ska undantas från skyldigheten att ha ett sekundärt driftställe om dess tredjepartsleverantör av IKT-tjänster har ett sådant driftställe ([40]). Om värdepapperscentraler undantas från

([33]) Finns på ECB:s webbplats www.ecb.europa.eu.

([34]) Se artikel 12 i förordning (EU) nr 909/2014.

([35]) Se även artikel 13 och artiklarna 17.4 och 22.6 i förordning (EU) nr 909/2014.

([36]) Se punkt 7.3 i Europeiska centralbankens yttrande av den 6 april 2017 om identifiering av kritiska infrastrukturer för IT-säkerhet (CON/2017/10), punkt 7.2 i Europeiska centralbankens yttrande av den 8 november 2018 om att utse samhällsviktiga tjänster och leverantörer av samhällsviktiga tjänster inom ramen för säkerhet i nätverks- och informationssystem (CON/2018/47), punkt 3.5.2 i Europeiska centralbankens yttrande av den 2 maj 2019 om säkerhet i nätverks- och informationssystem (CON/2019/17) och punkt 3.5.2 i Europeiska centralbankens yttrande av den 11 november 2019 om säkerhet i nätverks- och informationssystem (CON/2019/38) (inget av dessa yttranden finns översatta till svenska).

([37]) Se artikel 54.5 i förslaget till förordning och artikel 45.7 i förordning (EU) nr 909/2014.

([38]) Se artikel 54.4 i förslaget till förordning och artikel 45.6 i förordning (EU) nr 909/2014.

([39]) Se artikel 11.5 i förslaget till förordning.

([40]) Se artikel 78.3 i kommissionens delegerade förordning (EU) 2017/392 av den 11 november 2016 om komplettering av Europaparlamentets och rådets förordning (EU) nr 909/2014 med avseende på tekniska tillsynsstandarder för auktorisationskrav, tillsynskrav och operativa krav för värdepapperscentraler (EUT L 65, 10.3.2017, s. 48).

skyldigheten att ha ett sekundärt driftställe, blir det oklart vilket rättsligt värde ett sådant krav skulle ha. I förslaget till förordning ([41]) hänvisas också till ett mål för återställningstid samt till punktmål för återställning för varje funktion ([42]), medan det i relevanta tekniska tillsynsstandarder görs åtskillnad mellan kritiska funktioner ([43]) och kritisk verksamhet ([44]) vad gäller den återställningstid som fastställts för värdepapperscentralernas kritiska verksamhet. Här behöver unionens lagstiftande organ ytterligare förtydliga och överväga samspelet mellan förslaget till förordning och de tekniska tillsynsstandarder som kompletterar förordningen om värdepapperscentraler för att avvärja risken för motstridiga krav. Slutligen bör det förtydligas att de undantag som enligt förordningen om värdepapperscentraler ska gälla för värdepapperscentraler som drivs av vissa offentliga organ ([45]) ska utökas enligt förslaget till förordning.

2.3 *ECBS befogenheter vad gäller clearing av värdepapper*

2.3.1 ECBS centralbanker har anförtrotts tillsynsbefogenheter vad gäller centrala motparter. I detta avseende samarbetar Eurosystemets nationella centralbanker ofta med de relevanta nationella behöriga myndigheterna i de centrala motparternas övervakande funktioner och tillsynsfunktioner och deltar i respektive central motparts kollegium, som har upprättats i enlighet med Europaparlamentets och rådets förordning (EU) nr 648/2012 ([46]) (nedan kallad *Emir-förordningen*). De relevanta medlemmarna i Eurosystemet ([47]) deltar i Emir-kollegier i sin tillsynsfunktion och företräder Eurosystemet i egenskap av utgivande centralbank för centrala motparter där euron är en av de valutor som är mest relevanta för clearade finansiella instrument (samt för centrala motparter utanför euroområdet som clearar en betydande del av de finansiella instrumenten i euro). ECB är utgivande centralbank för centrala motparter utanför euroområdet.

2.3.2 Enligt förslaget till förordning ([48]) ska centralbankerna i ECBS inte vara med och utarbeta tekniska standarder där IKT-risker specificeras. Förslaget till förordning ([49]) innehåller inte heller några hänvisningar till Emir-förordningens krav på ett mål för återställningstid samt till punktmål för återställning för varje funktion ([50]). Det föreslagna regelverkets krav avseende IKT-risker bör inte vara mindre restriktiva än de nuvarande kraven. Det är därför viktigt att fastställa tydliga mål för återställningstid och punktmål för att ha en sund ram för kontinuitetshantering. Särskilda mål för återställningstid och punktmål ska upprätthållas även enligt CPMI-Ioscos *Principles for Financial Market Infrastructures* ([51]). Emir-förordningens nuvarande bestämmelse bör bibehållas och förslaget till förordning anpassas. Centralbankerna i ECBS bör vara delaktiga i arbetet med att ta fram sekundärlagstiftning, och unionens lagstiftande organ bör ytterligare förtydliga och överväga samspelet mellan förslaget till förordning och de kompletterande tekniska tillsynsstandarderna för att avvärja risken för motstridiga eller överlappande krav.

3. **Specifika kommentarer om tillsynsaspekter**

3.1 Genom rådets förordning (EU) nr 1024/2013 ([52]) (nedan kallad *SSM-förordningen*) tilldelas ECB specifika tillsynsuppgifter för kreditinstitut inom euroområdet och görs ansvarig för att den gemensamma tillsynsmekanismen (SSM) fungerar på ett effektivt och enhetligt sätt. Inom ramen för detta fördelas tillsynsuppgifterna mellan ECB och de deltagande nationella behöriga myndigheterna. Framför allt har ECB till uppgift att tilldela och återkalla auktorisationer för samtliga kreditinstitut. ECB har bland annat också till uppgift att säkerställa efterlevnad av relevant unionslagstiftning som föreskriver tillsynskrav för kreditinstitut, inbegripet kravet att ha robust företagsstyrning, såsom sunda riskhanteringsprocesser och interna kontrollmekanismer ([53]). För detta ändamål ges ECB alla tillsynsbefogenheter att ingripa i institutens verksamhet som den behöver för att utföra sina uppgifter. ECB

([41]) Se artikel 11.6 i förslaget till förordning.
([42]) Se artikel 3.17 i förslaget till förordning.
([43]) Se artikel 76.2 d och e i kommissionens delegerade förordning (EU) 2017/392.
([44]) Se artikel 78.2 och 78.3 i kommissionens delegerade förordning (EU) 2017/392.
([45]) Se artikel 1.4 i förordning (EU) nr 909/2014.
([46]) 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).
([47]) Se artikel 18 2 g och h i Emir-förordningen.
([48]) Se artikel 53.2 b och 53.3 i förslaget till förordning och artikel 34.3 i Emir-förordningen.
([49]) Se artikel 53.2 a i förslaget till förordning.
([50]) Se artikel 34 i Emir-förordningen.
([51]) Se CPMI-Ioscos principer för finansmarknadens infrastrukturer (Principles for Financial Market Infrastructures) som finns på webbplatsen för Banken för internationell betalningsutjämning www.bis.org.
([52]) 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).
([53]) Se artiklarna 4.1 e och 6.4 i förordning (EU) nr 1024/2013.

och de relevanta nationella behöriga myndigheterna är sålunda behöriga myndigheter som utövar särskilda tillsynsbefogenheter enligt Europaparlamentets och rådets förordning 2013/575/EU ([54]) (nedan kallad *kapitalkravsförordningen*) och Europaparlamentets och rådets direktiv 2013/36/EU ([55]) (nedan kallat *kapitalkravsdirektivet*).

3.2 I förslaget till förordning anges att det enhetliga regelverket och tillsynssystemet bör vidareutvecklas så att det omfattar digital operativ motståndskraft och IKT-säkerhet, genom att mandaten utökas för de finansiella tillsynsmyndigheter som har i uppdrag att övervaka och skydda den finansiella stabiliteten och marknadsintegriteten ([56]). Syftet är att främja en heltäckande IKT-ram eller ram för operativa risker genom harmonisering av viktiga krav på digital operativ motståndskraft för alla finansiella enheter ([57]). Förslaget till förordning syftar först och främst till att konsolidera och uppgradera de IKT-riskkrav som hittills har behandlats separat i olika unionsrättsakter ([58]).

3.3 IKT-riskkraven för den finansiella sektorn är för närvarande utspridda över ett antal olika unionsrättsakter, däribland kapitalkravsdirektivet, och icke-bindande instrument (t.ex. EBA:s riktlinjer) och är heterogena och ibland ofullständiga. I vissa fall har IKT-risken enbart tagits upp implicit, som en del av operativ risk, och i andra fall har den inte tagits upp alls. Det bör åtgärdas genom att förslaget till förordning och dessa rättsakter samordnas. Förslaget till ändringsdirektiv innehåller ett antal förslag till ändringar som förefaller nödvändiga för att öka rättssäkerheten och konsekvensen när de olika kraven på digital operativ motståndskraft ska tillämpas. I de ändringar av kapitalkravsdirektivet som nu har lagts fram i förslaget till ändringsdirektiv ([59]) hänvisas dock enbart till bestämmelser om beredskaps- och kontinuitetsplaner ([60]), då de enligt uppgift utgör en implicit grund för IKT-riskhantering.

3.4 Enligt förslaget till förordning ([61]) ska finansiella enheter, inbegripet kreditinstitut, ha interna styrnings- och kontrollramar som säkerställer en effektiv och ansvarsfull hantering av alla IKT-risker. I förslaget till förordning ([62]) fastställs hur de angivna kraven ska tillämpas på individuell och konsoliderad nivå, men utan tillräcklig samordning med den sektorsspecifika lagstiftning som det hänvisas till. I förslaget till förordning ([63]) anges slutligen att utan att detta påverkar tillämpningen av de bestämmelser om tillsynsramen för kritiska tredjepartsleverantörer av IKT-tjänster som avses i förslaget till förordning ([64]), ska efterlevnaden av de skyldigheter som fastställs i förslaget vad gäller kreditinstitut säkerställas av den behöriga myndighet som har utsetts i enlighet med artikel 4 i kapitalkravsdirektivet, utan att det påverkar de särskilda uppgifter som ECB tilldelas genom SSM-förordningen.

3.5 Mot bakgrund av ovanstående tolkar ECB det som att syftet med förslaget till förordning vad gäller kreditinstitut, med undantag för de bestämmelser i förslaget till förordning som avser tillsynsramen för kritiska tredjepartsleverantörer av IKT-tjänster ([65]), är att föreskriva en tillsynsorienterad intern styrningsram för IKT-riskhantering som kommer att integreras i den allmänna interna styrningsramen enligt kapitalkravsdirektivet. Med tanke på det föreslagna regelverkets tillsynsfokus kommer de behöriga myndigheter som har tillsynsansvar för efterlevnaden av de skyldigheter som fastställs i det föreslagna regelverket, inbegripet ECB, att vara de myndigheter som ansvarar för banktillsyn enligt SSM-förordningen.

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

([55]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, 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).

([56]) Se skäl 8 i förslaget till förordning.

([57]) Se skäl 11 i förslaget till förordning.

([58]) Se skäl 12 i förslaget till förordning.

([59]) Se skäl 4 och 5 i förslaget till ändringsdirektiv.

([60]) Se artikel 85 i kapitalkravsdirektivet.

([61]) Se artikel 4.1 i förslaget till förordning.

([62]) Se artikel 25.3.4 i förslaget till förordning.

([63]) Se artikel 41 i förslaget till förordning.

([64]) Se kapitel V avsnitt II i förslaget till förordning.

([65]) Se kapitel V avsnitt II i förslaget till förordning.

3.6 Unionens lagstiftande organ kan därför vilja överväga följande förslag för att få ökad tydlighet och samordning mellan förslaget till förordning och kapitalkravsdirektivet. För det första: kraven i förslaget till förordning kan bedömas vara av explicit tillsynskaraktär, vilket bland annat har skett i förordningen om värdepapperscentraler ([66]). För det andra: lydelsen i skälen i förslaget till ändringsdirektiv ([67]) skulle kunna föranleda en utvidgad tolkning, eftersom kraven i förslaget till förordning täcker in mer än enbart beredskaps- och kontinuitetsplaner. IKT-riskhanteringsåtgärder faller totalt sett under det mer allmänna tillämpningsområdet för en robust företagsstyrning enligt artikel 74 i kapitalkravsdirektivet ([68]). För det tredje: förslaget till förordning ([69]) bör ändras så att det i skälen erinras om ECB:s behörighet i fråga om tillsyn över kreditinstitut enligt fördraget och SSM-förordningen. För det fjärde: hänvisningen till tillämpning av krav fastställda på individuell och konsoliderad nivå ([70]) bör ses över med tanke på att undergruppsnivå och konsoliderad nivå inte definieras i förslaget till förordning, och vissa typer av förmedlare inte omfattas av konsoliderad tillsyn enligt den relevanta lagstiftningen (t.ex. betalningsinstitut). Tillämpningsnivån för de krav som anges i förslaget till förordning bör dessutom grundas enbart på den lagstiftning som gäller för respektive kategori av finansiell enhet. Vad gäller kreditinstitut finns ett tydligt samband mellan kapitalkravsdirektivet och förslaget till förordning, och de krav som anges i förslaget till förordning skulle därmed tillämpas automatiskt på individuell nivå, undergruppsnivå eller konsoliderad nivå ([71]), beroende på situationen. Unionens lagstiftande organ skulle slutligen kunna överväga att tillhandahålla övergångsbestämmelser för att hantera perioden från det att förslaget till förordning träder i kraft till dess att de tekniska tillsynsstandarderna gör det, med tanke på att vissa förmedlare, däribland kreditinstitut, redan omfattas av IKT-riskregler som gäller för vissa sektorer och som är mer ingående än de allmänna bestämmelserna i förslaget till förordning.

3.7 ECB har enligt SSM-förordningen anförtrotts uppgiften att säkerställa kreditinstitutens efterlevnad av unionslagstiftningens krav på att kreditinstitut ska ha effektiva riskhanteringsprocesser och interna kontrollmekanismer ([72]). Detta innebär att ECB ska se till att kreditinstitut tillämpar riktlinjer och processer för att utvärdera och hantera sin exponering för operativ risk, även i fråga om modellrisk, samt för att täcka extrema händelser med stor inverkan på institutets verksamhet. Kreditinstitut ska ange vad som utgör operativ risk vid tillämpningen av dessa riktlinjer och processer ([73]).

3.8 I juli 2017 antog ECB-rådet SSM-ramverket för rapportering av cyberincidenter (nedan kallat *ramverket*), utifrån ett utkast till förslag från tillsynsnämnden i enlighet med artiklarna 26.8 och 6.2 i SSM-förordningen och artikel 21.1 i Europeiska centralbankens förordning (EU) nr 468/2014 (ECB/2014/17) ([74]). Ramverket omfattar en bindande informationsbegäran (enskilda beslut riktade till kreditinstitut) och/eller rapportering på grundval av artikel 10 i SSM-förordningen ([75]). Vissa länder har redan en process för incidentrapportering med krav på att kreditinstitut ska rapportera alla betydande cyberincidenter till sina nationella behöriga myndigheter. I dessa länder kommer betydande kreditinstitut att fortsätta rapportera incidenter till de nationella behöriga myndigheterna, som därefter rapporterar vidare till ECB för dessa enheter under tillsyn. Ovannämnda beslut riktas därför även till dessa

([66]) Se rubriken ”Stabilitetskrav” i kapitel II, avsnitt 4 i förordningen om värdepapperscentraler.

([67]) Se skäl 4 i förslaget till ändringsdirektiv.

([68]) Artikel 85 i direktiv 2013/36/EU utgör bara en specificering. Se i detta avseende även s. 4, 11 och 37 i Europeiska bankmyndighetens riktlinjer för hantering av IKT-risker och säkerhetsrisker av den 29 november 2019 (nedan kallade *EBA:s riktlinjer*), där den allmänna rättsliga grunden uttryckligen anges som artikel 74 i direktiv 2013/36/EU.

([69]) Se artikel 41.1 i förslaget till förordning.

([70]) Se artikel 25.3 och 25.4 i förslaget till förordning.

([71]) Se även artikel 109 i kapitalkravsdirektivet.

([72]) Se artikel 4.1 e i SSM-förordningen.

([73]) Se artikel 85 i kapitalkravsdirektivet.

([74]) Europeiska centralbankens förordning (EU) nr 468/2014 av den 16 april 2014 om upprättande av ramen för samarbete inom den gemensamma tillsynsmekanismen mellan Europeiska centralbanken och nationella behöriga myndigheter samt med nationella utsedda myndigheter (ramförordning om den gemensamma tillsynsmekanismen [SSM]) (ECB/2014/17) (EUT L 141, 14.5.2014, s. 1).

([75]) Framför allt måste cyberincidenter (upptäckta fall av eventuellt informationssäkerhetsintrång, både avsiktliga och oavsiktliga) rapporteras in till ECB om minst ett av följande villkor är uppfyllt: 1) den eventuella ekonomiska effekten uppgår till 5 miljoner euro eller 0,1 procent av kärnprimärkapitalet, 2) incidenten är offentligt rapporterad eller skadar anseendet, 3) incidenten har eskalerats till IT-ansvarig chef utöver den vanliga rapporteringen, 4) banken har anmält incidenten till en CERT-/CSIRT-enhet, säkerhetsmyndighet eller polisen, 5) en katastrof- eller kontinuitetsplan har satts i verket eller en IT-skadeanmälan har skickats in till ett försäkringsbolag, 6) lag- eller regelbrott har begåtts, 7) banken använder interna kriterier och expertbedömningar (systempåverkan möjlig) och beslutar att informera ECB.

nationella myndigheter för att med stöd av ramverket vidarebefordra denna information till ECB. ECB stöder unionens lagstiftande organ i deras strävan att främja harmonisering och rationalisering, bland annat vad gäller regler och skyldigheter avseende kreditinstitutens incidentrapportering. ECB är därför beredd att vid behov ändra (och eventuellt upphäva) ramverket, inför ett slutligt antagande av förslaget till förordning.

4. Specifika kommentarer om IKT-riskhantering, incidentrapportering, testning av operativ motståndskraft samt IKT-tredjepartsrisk

4.1 *IKT-riskhantering*

4.1.1 ECB välkomnar att det enligt förslaget till förordning ska införas en stabil och heltäckande IKT-riskhanteringsram som omfattar CPMI-IOSCO:s *Guidance on cyber resilience* och som i hög grad är i linje med bästa praxis, inklusive Eurosystemets *Cyber Resilience Oversight Expectations for FMIs*.

4.1.2 ECB stöder tanken att finansiella enheter ska göra en riskbedömning vid varje ”större förändring” av nätverks- och informationssystemets infrastruktur ([76]). Förslaget till förordning innehåller dock ingen definition av ”större förändring”, vilket ger de finansiella enheter ett oönskat utrymme att göra olika tolkningar, vilket i förlängningen skulle kunna försvåra harmoniseringsmålen med förslaget till förordning. För rättssäkerhetens skull kan unionens lagstiftande organ vilja överväga att införa en definition av ”större förändring” i förslaget till förordning.

4.1.3 ECB stöder i princip tanken att andra finansiella enheter än mikroföretag ska rapportera relevanta kostnader och förluster som orsakas av IKT-avbrott och IKT-relaterade incidenter till de behöriga myndigheterna ([77]). Men för att säkerställa systemets övergripande effektivitet och undvika alltför många rapporter för behöriga myndigheter och finansiella enheter kan det vara en idé för unionens lagstiftande organ att införa relevanta tröskelvärden, eventuellt av kvantitativ art.

4.1.4 ECB ser det som fullt möjligt att de finansiella enheterna, efter godkännande av behöriga myndigheter, får delegera uppgiften att kontrollera efterlevnaden av IKT-riskhanteringskraven till koncerninterna eller externa företag ([78]). Samtidigt är det viktigt att unionens lagstiftande organ förtydligar hur de behöriga myndigheternas godkännande skulle beviljas i de fall då en finansiell enhet har flera behöriga myndigheter. Detta skulle kunna inträffa om en finansiell enhet är ett kreditinstitut, en leverantör av tjänster för kryptotillgångar och/eller en betaltjänstleverantör. Vad gäller den identifiering och klassificering som finansiella enheter ska utföra enligt förslaget till förordning ([79]) anser ECB slutligen att förslaget till förordning även bör omfatta ett krav på att finansiella enheter ska beakta tillgångars kritikalitet (dvs. om de stöder kritiska funktioner) när tillgångar klassificeras.

4.2 *Incidentrapportering*

4.2.1 ECB välkomnar att förslaget till förordning syftar till att harmonisera förutsättningarna för rapportering av IKT-incidenter inom unionen samt att arbeta för en centraliserad rapportering av större IKT-relaterade incidenter ([80]). Om det införs harmoniserade regler för att rapportera större IKT-relaterade incidenter ([81]) till relevanta behöriga myndigheter, skulle detta i princip innebära att rapporteringsbördan rationaliseras och harmoniseras för finansiella enheter, inbegripet kreditinstitut. Behöriga myndigheter skulle gynnas av att tillämpningsområdet för incidenter utökas och omfattar mer än de cyberrelaterade incidenter som för närvarande täcks av det befintliga regelverket ([82]). Ett framtida antagande av förslaget till förordning skulle innebära att befintliga regelverk, däribland SSM-ramverket för rapportering av cyberincidenter, skulle behöva ses över och eventuellt upphävas. Men om alla regelverk ska rationaliseras och samordnas fullt ut är det helt avgörande att tillämpningsområdet för incidentrapporteringsbestämmelserna i förslaget till förordning, inbegripet samtliga relevanta definitioner, tröskelvärden och rapporteringsparametrar, är helt i linje med relevanta regelverk. Det är framför allt av yttersta vikt att säkerställa att förslaget till

([76]) Se artikel 7.3 i förslaget till förordning.
([77]) Se artikel 10.9 i förslaget till förordning.
([78]) Se artikel 5.10 i förslaget till förordning.
([79]) Se artikel 7 i förslaget till förordning.
([80]) Se artikel 19 i förslaget till förordning.
([81]) Se artiklarna 3.7, 17 och 18 i förslaget till förordning.
([82]) Se t.ex. ramverket.

förordning är i linje med Europaparlamentets och rådets direktiv (EU) 2015/2366 ([83]) (nedan kallat *PSD2*) och EBA:s riktlinjer för rapportering vid allvarliga incidenter (nedan kallat *EBA:s riktlinjer*). Förslaget till ändringsdirektiv ([84]) innehåller ändringar till PSD2 vad gäller avgränsningen av incidentrapporteringen mellan förslaget till förordning och PSD2. Dessa ändringar skulle främst påverka betaltjänstleverantörer, som även kan vara auktoriserade som kreditinstitut, samt behöriga myndigheter. Det finns en otydlighet när det gäller incidentrapporteringsprocessen samt en potentiell överlappning mellan vissa av de incidenter som behöver rapporteras enligt både förslaget till förordning och EBA:s riktlinjer.

4.2.2 Med de rapporteringsprocesser för större incidenter som anges i förslaget till förordning ([85]), PSD2 och motsvarande EBA-riktlinjer skulle betaltjänstleverantörer behöva lämna en incidentrapport till respektive behörig myndighet så snart incidenten har klassificerats. I de första rapporterna anges nämligen inte incidentens art, orsak eller vilket funktionsområde som påverkas av incidenten och detta är något betaltjänstleverantörer kanske kan fastställa först längre fram, när det finns mer ingående information om incidenten. Detta innebär att de första incidentrapporterna kan lämnas både enligt förslaget till förordning och EBA:s riktlinjer. Betaltjänstleverantörer kan också välja en enda rapporteringsram och korrigera sina inlämnade rapporter längre fram. Samma osäkerhet (t.ex. vad gäller grundorsaken till en incident) kan även förekomma i del- och slutrapporter. Även detta skulle kunna innebära att rapporter lämnas in parallellt till de myndigheter som är behöriga enligt förslaget till förordning respektive PSD2.

4.2.3 Vissa incidenter som kan klassificeras som IKT-relaterade incidenter kan även påverka andra områden och skulle därmed behöva rapporteras enligt EBA:s riktlinjer. Detta kan t.ex. förekomma om en incident har påverkan i ett IKT-perspektiv, men samtidigt har direkt påverkan på tillhandahållandet av betalningstjänster och/eller har påverkat funktionsområden eller kanaler som inte omfattar IKT. I vissa fall är det kanske inte heller möjligt att skilja mellan operativa och IKT-relaterade incidenter. Enligt förslaget till förordning skulle dessutom en finansiell enhet som är både betydande kreditinstitut och betaltjänstleverantör behöva rapportera samma IKT-relaterade incident två gånger, eftersom enheten omfattas av två behöriga myndigheter. Mot denna bakgrund behöver förslaget till förordning förtydligas när det gäller hur samspelet mellan PSD2 och EBA:s riktlinjer är tänkt att fungera i praktiken. För en harmonisering och rationalisering av rapporteringskraven är det framför allt viktigt att unionens lagstiftande organ beaktar de frågor som ännu kvarstår vad gäller dubbelrapportering samt att det förtydligas om förslaget till förordning respektive PSD2 och EBA:s riktlinjer kommer att existera parallellt eller om det ska finnas en enda uppsättning incidentrapporteringskrav.

4.2.4. I förslaget till förordning införs kravet att behöriga myndigheter ([86]) ska bekräfta mottagandet av anmälan när de har mottagit en rapport och så snart som möjligt lämna all nödvändig återkoppling eller vägledning till den finansiella enheten, särskilt för att diskutera avhjälpande åtgärder på enhetsnivå eller sätt att minimera de negativa effekterna inom alla olika sektorer. Detta skulle innebära att de behöriga myndigheterna är aktivt delaktiga i arbetet med att hantera och avhjälpa incidenter samtidigt som de bedömer hur en enhet under tillsyn har hanterat kritiska incidenter. ECB understryker att det klart och tydligt bör anges att det uteslutande är den finansiella enheten som har ansvar och ägarskap för avhjälpandet och konsekvenserna av en incident. ECB skulle därför föreslå att återkopplingen och vägledningen begränsas till tillsyn på hög nivå. För att kunna ge mer omfattande återkoppling skulle det behövas en kategori av specialister med mycket ingående teknisk kunskap som kanske normalt inte ingår i tillsynsmyndigheternas rekryteringsbas.

4.3 *Testning av digital operativ motståndskraft*

4.3.1 ECB välkomnar kraven i förslaget till förordning ([87]) om att alla finansiella enheter ska testa sin digitala operativa motståndskraft samt att alla institut behöver ha ett eget testningsprogram Förslaget till förordning ([88]) innehåller en beskrivning av olika kategorier av tester som ska vara vägledande för de finansiella enheterna. Det är inte helt uppenbart vilken kategori av tester det handlar om och vissa tester, t.ex. kompatibilitetstester, frågeformulär eller scenariobaserade tester, kan dessutom tolkas på olika sätt av europeiska tillsynsmyndigheter, behöriga myndigheter

([83]) 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).
([84]) Se artikel 7.9 i förslaget till ändringsdirektiv.
([85]) Se artikel 17.3 i förslaget till förordning.
([86]) Se artikel 20 i förslaget till förordning.
([87]) Se artiklarna 21 och 22 i förslaget till förordning.
([88]) Se artikel 22.1 i förslaget till förordning.

eller finansiella enheter. Det finns dessutom ingen vägledning om hur ofta varje test ska genomföras. Ett tänkbart tillvägagångssätt skulle kunna vara att generiska testningskrav anges i förslaget till förordning, medan olika typer av tester beskrivs mer ingående i tekniska tillsyns- och genomförandestandarder.

4.3.2 Hotstyrd penetrationstestning (threat-led penetration testing, TLPT) är ett kraftfullt verktyg för att testa säkerhetsförsvar och beredskap. ECB uppmuntrar därför finansiella enheter att använda TLPT. Med detta verktyg testas inte enbart tekniska åtgärder, utan även personal och processer. Resultaten från dessa tester kan leda till att den högsta ledningen på de testade enheterna blir betydligt mer säkerhetsmedveten. Det europeiska ramverket för hotunderrättelsebaserade, etiska red teaming-insatser (European Framework for Threat Intelligence Based Ethical Red-teaming (TIBER-EU) ([89]) och andra TLPT-verktyg utanför unionen är de instrument som enheter i första hand kan använda för att på egen hand bedöma, testa, träna och stärka sin ställning och försvarsförmåga i fråga om cyberresiliens.

4.3.3 I de flesta medlemsstater där TIBER-EU har införts är övervakande myndigheter och tillsynsmyndigheter inte aktivt delaktiga i arbetet med att genomföra ett lokalanpassat TIBER-XX-program, och TIBER-cyberteamet (TCT) agerar nästan alltid oberoende i förhållande till dessa funktioner. De avancerade tester som anges i förslaget till förordning ([90]), i form av TLPT, bör därför genomföras som ett verktyg för att stärka det finansiella ekosystemet och öka den finansiella stabiliteten och inte som ett rent tillsynsverktyg. Det finns heller inget behov av att utveckla en ny avancerad ram för testning av cyberresiliens, eftersom medlemsstaterna redan i stor utsträckning har infört TIBER-EU, som för närvarande är den enda ramen i EU av den här kategorin.

4.3.4 Kraven på testare bör inte anges i artikeldelen i förslaget till förordning, eftersom den TLPT-relaterade sektorn fortfarande är under utveckling och angivna specifika krav kan hämma innovation. För att säkerställa en hög grad av oberoende i samband med testning anser dock ECB att de finansiella enheterna inte bör anställa eller kontraktera testare som är anställda eller kontrakterade av finansiella enheter i samma grupp eller av finansiella enheter som på annat sätt ägs och/eller kontrolleras av de finansiella enheter som ska testas.

4.3.5 För att minska risken för fragmentering och säkerställa harmonisering bör det i förslaget till förordning förordas en specifik TLPT-ram som ska tillämpas på den finansiella sektorn i hela unionen. Fragmentering kan leda till ökade kostnader och högre krav på tekniska, operativa och finansiella resurser, både för behöriga myndigheter och för finansinstitut. Dessa ökade kostnader och krav kan i förlängningen få negativa konsekvenser för det ömsesidiga erkännandet av tester. Avsaknaden av harmonisering och de problem det kan leda till i fråga om ömsesidigt erkännande är särskilt problematiska för finansiella enheter, som kan ha flera olika tillstånd och/eller bedriva verksamhet i flera av unionens jurisdiktioner. De tekniska tillsyns- och genomförandestandarder som enligt förslaget till förordning, ska utarbetas för TLPT bör vara i linje med TIBER-EU. ECB välkomnar vidare möjligheten att i samarbete med de europeiska tillsynsmyndigheterna vara med och utarbeta dessa tekniska tillsyns- och genomförandestandarder.

4.3.6 Om de behöriga myndigheterna blir aktivt delaktiga i testerna skulle detta kunna leda till en intressekonflikt med deras andra funktion, dvs. att bedöma den finansiella enhetens ram för testning. Mot denna bakgrund föreslår ECB att behöriga myndigheters eventuella skyldigheter att validera dokument och utfärda intyg för ett TLPT-test ska strykas från förslaget till förordning.

4.4 IKT-tredjepartsrisk

4.4.1 ECB välkomnar att det införs en heltäckande uppsättning centrala principer och en stabil tillsynsram för att identifiera och hantera IKT-risker som härrör från tredjepartsleverantörer av IKT-tjänster, oavsett om de hör till samma grupp finansiella enheter eller ej. För att uppnå att IKT-risker identifieras och hanteras på ett effektivt sätt är det viktigt att bland annat kritiska tredjepartsleverantörer av IKT-tjänster identifieras och klassificeras korrekt. Det är i och för sig positivt att det införs delegerade akter ([91]) som kompletterar de kriterier som ska användas för klassificering ([92]), men ECB ska höras innan dessa delegerade akter antas.

([89]) Finns på ECB:s webbplats www.ecb.europa.eu.
([90]) Artiklarna 23 och 24 i förslaget till förordning.
([91]) Se artikel 28.3 i förslaget till förordning.
([92]) Se artikel 28.2 i förslaget till förordning.

4.4.2 Vad gäller tillsynsramens struktur ([93]) behöver det förtydligas ytterligare vilken funktion den gemensamma kommittén ska ha. ECB är positiv till att ingå i tillsynsforumet som observatör, eftersom detta innebär att ECB får samma tillgång till dokumentation och information som medlemmar med rösträtt ([94]). ECB vill uppmärksamma unionens lagstiftande organ på att ECB, i sin roll som observatör, skulle bidra till arbetet i tillsynsforumet både som utgivande centralbank med ansvar för tillsyn över marknadsinfrastruktur och som tillsynsmyndighet för kreditinstitut. ECB noterar vidare att vid sidan av sin roll som observatör i tillsynsforumet skulle ECB även ingå i den gemensamma undersökningsgruppen i egenskap av behörig myndighet. Här skulle unionens lagstiftande organ ytterligare kunna överväga de gemensamma undersökningsgruppernas sammansättning ([95]) för att säkerställa att relevanta behöriga myndigheter får lämplig viktning. ECB anser även att maxantalet deltagare i de gemensamma undersökningsgrupperna bör höjas, med tanke på IKT-tredjepartstjänsternas kritikalitet, komplexitet och omfattning.

4.4.3 ECB noterar att enligt förslaget till förordning får den ledande tillsynsmyndigheten förhindra att kritiska tredjepartsleverantörer av IKT-tjänsters ingår ytterligare underleverantörsavtal om i) den planerade underleverantören är en tredjepartsleverantör av IKT-tjänster eller en IKT-underleverantör som är etablerad i ett tredjeland och ii) underentreprenaden avser en kritisk eller viktig funktion hos den finansiella enheten. ECB vill understryka att dessa befogenheter enbart kan utövas av den ledande tillsynsmyndigheter i samband med underleverantörsavtal där en kritisk tredjepartsleverantör av IKT-tjänster lägger ut en kritisk eller viktig funktion på underentreprenad till en separat rättslig enhet som är etablerad i ett tredjeland. ECB tolkar det som att den ledande tillsynsmyndigheten inte har jämförbara befogenheter för att förhindra en kritisk tredjepartsleverantör av IKT-tjänster från att utkontraktera kritiska eller viktiga funktioner hos den finansiella enheten till faciliteter som denna tjänsteleverantör har i ett tredjeland. I ett operativt perspektiv skulle detta t.ex. kunna röra sig om att kritiska data och/eller kritisk information kan lagras eller behandlas av faciliteter utanför Europeiska ekonomiska samarbetsområdet (EEA). I så fall har inte den ledande tillsynsmyndigheten befogenheter att på lämpligt sätt ge de behöriga myndigheterna tillgång till all information, alla lokaler samt all infrastruktur och personal som är av relevans för att den finansiella enheten ska kunna utföra alla kritiska eller viktiga funktioner. För att säkerställa att de behöriga myndigheterna kan utföra sina uppgifter obehindrat föreslår ECB att den ledande tillsynsmyndigheten ska få befogenhet att även begränsa möjligheten för kritiska tredjepartsleverantörer av IKT-tjänster att använda faciliteter utanför EES. Denna befogenhet skulle kunna utövas i de särskilda fall då det inte finns några sådana administrativa arrangemang med tredjeländers myndigheter som anges i förslaget till förordning ([96]) eller om företrädare för kritiska tredjepartsleverantörer av IKT-tjänster inte med stöd av det relevanta tredjelandets ramverk på ett tillfredsställande sätt kan garantera den tillgång till information, lokaler, infrastruktur och personal som behövs för att utföra tillsynsuppgifter.

4.4.4 Kravet på att behöriga myndigheter ska följa upp den ledande tillsynsmyndighetens rekommendationer ([97]) riskerar att bli ineffektivt, eftersom behöriga myndigheter kanske inte har hela bilden av de risker som genereras av varje kritisk tredjepartsleverantör av IKT-tjänster. Om de kritiska tredjepartsleverantörerna inte agerar enligt rekommendationerna kan dessutom de behöriga myndigheterna behöva vidta åtgärder mot de finansiella enheter som står under deras tillsyn. Enligt förslaget till förordning ([98]) får de behöriga myndigheterna kräva att finansiella enheter under tillsyn tillfälligt avbryter användningen av en kritisk tredjepartstjänst eller avslutar utestående avtal med kritiska tredjepartsleverantörer. Det är svårt att omvandla den planerade uppföljningsprocessen till konkreta åtgärder. Det är framför allt oklart om en finansiell enhet under tillsyn kommer att ha förutsättningar att tillfälligt avbryta eller avsluta ett avtal med en kritisk tredjepartsleverantör av IKT-tjänster. Den kritiska tredjepartsleverantören av IKT-tjänster kan nämligen vara en betydande leverantör för den finansiella enheten eller det kan komma att orsaka den finansiella enheten avtalsmässiga eller andra kostnader och skador om avtalet tillfälligt avbryts eller avslutas. Detta tillvägagångssätt främjar inte tillsynskonvergens, eftersom de behöriga myndigheterna kan tolka samma rekommendation på olika sätt. I förlängningen skulle detta kunna motverka den planerade harmoniseringen och den konsekventa strategin när kritisk IKT-tredjepartsrisk övervakas på unionsnivå. Mot denna bakgrund kan unionens lagstiftande organ vilja överväga att tilldela de lagstadgade tillsynsmyndigheterna särskilda verkställandebefogenheter gentemot kritiska tredjepartsleverantörer av IKT-tjänster, med tanke på de begränsningar som infördes genom *Meroni*-doktrinen, som visserligen har dämpats genom EU-domstolens dom i Esma-målet ([99]).

([93]) Se artikel 29 i förslaget till förordning.
([94]) Se artikel 29.3 i förslaget till förordning.
([95]) Se artikel 35 i förslaget till förordning.
([96]) Se artikel 39.1 i förslaget till förordning.
([97]) Se artiklarna 29.4 och 37 i förslaget till förordning.
([98]) Se artikel 37.3 i förslaget till förordning.
([99]) Se domstolens dom (stora avdelningen) av den 22 januari 2014, Förenade konungariket Storbritannien och Nordirland mot Europaparlamentet och Europeiska unionens råd avseende förordning (EU) nr 236/2012 – mål C-270/12.

I de fall där ECB rekommenderar att förslaget till förordning ska ändras anges de specifika förslagen i ett separat tekniskt arbetsdokument som åtföljs av en förklaring. Det tekniska arbetsdokumentet finns på engelska på i EUR-Lex.

Utfärdat i Frankfurt am Main den 4 juni 2021.

Christine LAGARDE
ECB:s ordförande