III

(Forberedende retsakter)

DEN EUROPÆISKE CENTRALBANK

DEN EUROPÆISKE CENTRALBANKS UDTALELSE

af 4. juni 2021

om et forslag til Europa-Parlamentets og Rådets forordning om digital operationel modstandsdygtighed i den finansielle sektor

(CON/2021/20)

(2021/C 343/01)

Indledning og retsgrundlag

Den Europæiske Centralbank (ECB) modtog den 22., 23. og 29. december 2020 anmodninger fra henholdsvis Rådet for Den Europæiske Union og Europa-Parlamentet om en udtalelse om et forslag til Europa-Parlamentets og Rådets forordning om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012 og (EU) nr. 600/2014 ([1]) (herefter »forordningsforslaget«) og et forslag til et direktiv om ændring af direktiv 2006/43/EF, 2009/65/EF, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 ([2]) (herefter »det foreslåede ændringsdirektiv«, sammen med »forordningsforslaget« »lovforslagene«).

ECB's kompetence til at afgive udtalelse er baseret på artikel 127, stk. 4, og artikel 282, stk. 5, i traktaten om Den Europæiske Unions funktionsmåde, da lovforslagene indeholder bestemmelser, der henhører under ECB's kompetenceområder, navnlig formulering og gennemførelse af den monetære politik, fremme af betalingssystemernes smidige funktion, bidrag til en smidig gennemførelse af de kompetente myndigheders politikker vedrørende det finansielle markedssystems stabilitet og ECB's opgaver vedrørende tilsyn med kreditinstitutter i henhold til traktatens artikel 127, stk. 2, første og fjerde led, artikel 127, stk. 5, og artikel 127, stk. 6. I overensstemmelse med artikel 17.5, første punktum, i forretningsordenen for Den Europæiske Centralbank er denne udtalelse vedtaget af ECB's Styrelsesråd.

1. Generelle bemærkninger

1.1 ECB glæder sig over den foreslåede forordning, der har til formål at øge cybersikkerheden og den operationelle modstandsdygtighed i den finansielle sektor. ECB glæder sig navnlig over forordningsforslaget formålet om at fjerne hindringer for og forbedre oprettelsen og funktionen af det indre marked for finansielle tjenesteydelser ved at harmonisere de regler, der gælder inden for risikostyring i forbindelse med informations- og kommunikationsteknologi (ICT), indberetning, test og IKT-tredjepartsrisici. ECB glæder sig desuden over forordningsforslagets formål om at strømline og harmonisere eventuelle sammenfaldende reguleringsmæssige krav eller tilsynsmæssige forventninger, som de finansielle enheder i øjeblikket er underlagt i henhold til EU-lovgivningen.

1.2 ECB forstår det således, at forordningsforslaget hvad angår finansielle enheder, der er identificeret som operatører af væsentlige tjenester ([3]), udgør sektorspecifik lovgivning (lex specialis) i overensstemmelse med betydningen i artikel 1, stk. 7, i Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 ([4]) (herefter NIS-direktivet). Det medfører, at kravene i forordningsforslaget i princippet har forrang over NIS-direktivet. I praksis vil finansielle enheder, der er identificeret som operatører af væsentlige tjenester ([5]), bl.a. indberette

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Jf. forordningsforslagets artikel 1, stk. 2.
([4]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).
([5]) Jf. NIS-direktivets artikel 5.

hændelser i overensstemmelse med forordningsforslaget i stedet for NIS-direktivet. Selv om ECB glæder sig over reduktionen af potentielle sammenfaldende krav til de finansielle enheder i forbindelse med indberetningen af hændelser, bør der tages yderligere hensyn til samspillet mellem den forordningsforslaget og NIS-direktivet. For eksempel kan en IKT-tredjepartstjenesteyder ([6]) være underlagt henstillinger udstedt af den hovedansvarlige for overvågningen ([7]). Samtidig kan den samme udbyder af IKT-tjenester klassificeres som operatør af væsentlige tjenester i henhold til NIS-direktivet og være underlagt bindende instrukser fra den kompetente myndighed ([8]). I sådanne tilfælde kan IKT-tredjepartstjenesteudbyderen være underlagt modstridende henstillinger udstedt i henhold til den forordningsforslaget og bindende instrukser udstedt i henhold til NIS-direktivet. ECB foreslår, at Unionens lovgivende organer overvejer yderligere potentielle uoverensstemmelser mellem den foreslåede forordning og NIS-direktivet, som kan hæmme harmoniseringen og reduktionen af sammenfaldende og modstridende krav til de finansielle enheder.

1.3 ECB forstår det også således, at i henhold til forslaget til Europa-Parlamentets og Rådets direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 ([9]) (herefter »det foreslåede NIS2-direktiv«), vil »nærvedhændelser« ([10]) blive underlagt indberetningsforpligtelser ([11]). Mens betragtning 39 til det foreslåede NIS2-direktiv henviser til betydningen af udtrykket »nærvedhændelser«, er det uklart, om det er hensigten at kræve, at nærvedhændelser indberettes af de finansielle enheder, der fremgår af forordningsforslagets artikel 2. I den forbindelse og under hensyn til, at nærvedhændelser først kan identificeres som sådanne, efter at de er indtruffet, vil ECB gerne modtage rettidig underretning om væsentlige nærvedhændelser, sådan som det i øjeblikket er tilfældet for cyberhændelser. ECB foreslår mere koordinering mellem den forordningsforslaget og det foreslåede NIS2-direktiv for at præcisere det nøjagtige omfang af den indberetning, som en given finansiel enhed kan være underlagt i henhold til disse to særskilte, men forbundne EU-retsakter. Samtidig er det nødvendigt at definere »nærvedhændelser«, og der skal udvikles bestemmelser, der præciserer deres betydning.

1.4 ECB glæder sig over, at finansielle enheder tilskyndes til frivilligt at udveksle oplysninger om cybertrusler med hinanden for at forbedre og styrke deres cyberrobusthedsstillinger. ECB har selv assisteret med det markedsdrevne Cyber threat Intelligence Information Sharing Initiative (CIISI-EU) og har gjort planerne tilgængelige for alle med henblik på at opbygge og fremme sådan et initiativ ([12]).

1.5 ECB støtter samarbejdet mellem de kompetente myndigheder med henblik på den forordningsforslaget, de europæiske tilsynsmyndigheder og computersikkerhedsberedskabsteamene (CSIRTS) ([13]). Det er vigtigt at udveksle oplysninger for at sikre Unionens operationelle modstandsdygtighed, da informationsudveksling og samarbejde mellem myndighederne kan bidrage til at forebygge cyberangreb og bidrage til at mindske spredningen af IKT-trusler. En fælles forståelse af IKT-relaterede risici bør fremmes, og der bør sikres en konsekvent vurdering af sådanne risici i hele Unionen. Det er yderst vigtigt, at de kompetente myndigheder ([14]) kun udveksler oplysninger med kontaktpunktet ([15]) og de nationale CSIRTS, når der findes klart fastlagte klassificerings- og informationsudvekslingsmekanismer, kombineret med passende sikkerhedsforanstaltninger for at sikre fortrolighed.

1.6 Endelig ser ECB gerne, at der i forordningsforslaget indføres regler om personoplysninger og datalagring. Lagringsperiodens længde bør tage hensyn til den undersøgelse, inspektion, anmodning om oplysninger, meddelelse, offentliggørelse, evaluering, verifikation, vurdering og udarbejdelse af overvågnings- eller tilsynsplaner, som de kompetente myndigheder kan være nødt til at gennemføre som led i deres respektive forpligtelser og opgaver i henhold til forordningsforslaget. I den forbindelse vil en lagringsperiode på 15 år være tilstrækkelig. Denne datalagringsperiode kan forkortes eller forlænges, hvis det påkræves i specifikke

([6]) Jf. forordningsforslagets artikel 3, stk. 15.
([7]) Jf. forordningsforslagets artikel 31, stk. 1, litra d).
([8]) Jf. NIS-direktivets artikel 15, stk. 3.
([9]) COM(2020) 823 final.
([10]) Begivenheder, der potentielt kunne have forvoldt skade, men hvor det lykkedes at forhindre, at de indtraf fuldt ud, jf. betragtning 39 til NIS2-direktivet.
([11]) Jf. NIS2-direktivets artikel 11.
([12]) Cyber threat Intelligence Information Sharing Initiative (CIISI-EU) tilgængelig på ECB's websted www.ecb.europa.eu.
([13]) Jf. artikel 42 i den foreslåede forordning.
([14]) Jf. også artikel 11, 26 og 27 i NIS2-direktivet.
([15]) Jf. NIS-direktivets artikel 8, stk. 3.

tilfælde. I den forbindelse foreslår ECB, at Unionens lovgivende organer i deres formulering af den relevante bestemmelse om personoplysninger og datalagring også tager hensyn til princippet om dataminimering samt yderligere behandling med henblik på arkivering i almenhedens interesse, videnskabelige eller historiske forskningsformål eller statistiske formål ([16]).

2. **Specifikke bemærkninger om overvågning og clearing og afvikling af værdipapirer**

2.1 *ESCB's og Eurosystemets overvågningskompetencer*

2.1.1 Traktaten og statutten for Det Europæiske System af Centralbanker og Den Europæiske Centralbank (herefter »ESCB-statutten«) indeholder bestemmelser om Eurosystemets overvågning af clearing- og betalingssystemer i tæt tilknytning til dens grundlæggende pengepolitiske opgaver. I henhold til traktatens artikel 127, stk. 2, fjerde led, som afspejlet i ESCB-statuttens artikel 3.1, er en af de grundlæggende opgaver, der skal udføres af Det Europæiske System af Centralbanker (ESCB), at fremme betalingssystemernes smidige funktion. Med henblik på at sikre effektive og pålidelige clearing- og betalingssystemer inden for Unionen og over for tredjelande kan ECB og de nationale centralbanker tilbyde faciliteter, og ECB kan udstede forordninger for at udføre denne grundlæggende opgave ([17]). ECB vedtog i henhold til sin overvågningsrolle Den Europæiske Centralbanks forordning (EU) No 795/2014 (herefter »SIPS-forordningen«) ([18]). SIPS-forordningen gennemfører i præskriptiv form principperne for finansielle markedsinfrastrukturer fra april 2012, som er udstedt af Komitéen for Betalings- og Afviklingssystemer og Den Internationale Børstilsynsorganisation ([19]), og som er juridisk bindende og omfatter både store betalingssystemer og detailbetalingssystemer af systemisk betydning, som drives af enten en centralbank i Eurosystemet eller en privat enhed. Eurosystemets overvågningsramme ([20]) identificerer betalingsinstrumenter som en »integreret del af betalingssystemerne« og inkluderer således disse inden for rammerne af overvågningen. Rammen for tilsyn med betalingsinstrumenter er i øjeblikket ved at blive revideret ([21]). I henhold til den ramme defineres et betalingsinstrument (f.eks. et kort, en kreditoverførsel, direkte debitering, overførsel af e-penge og digitalt betalingstoken ([22])) som en personaliseret anordning (eller en række anordninger) og/eller række af procedurer, som brugeren af betalingstjenesten og udbyderen af betalingstjenesten anvendte for at initiere en værdioverførsel ([23]).

2.1.2 I lyset af ovenstående glæder ECB sig over udelukkelsen af systemoperatører som defineret i artikel 2, litra p), i Europa-Parlamentets og Rådets direktiv 98/26/EF ([24]), betalingssystemer (herunder de, der drives af centralbanker), betalingsordninger og betalingsordninger med henblik på anvendelsen af ovennævnte

([16]) Jf. artikel 4, litra b), og artikel 13 i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

([17]) Jf. ESCB-statuttens artikel 22.

([18]) Den Europæiske Centralbanks forordning (EU) nr. 795/2014 af 3. juli 2014 om overvågningskrav for systemisk vigtige betalingssystemer (ECB/2014/28) (EUT L 217 af 23.7.2014, s. 16).

([19]) Findes på Den Internationale Betalingsbanks websted www.bis.org.

([20]) Eurosystemets overvågningsramme, revideret udgave (juli 2016), som findes på ECB's websted www.ecb.europa.eu.

([21]) Jf. den reviderede og konsoliderede ramme for eurosystemets overvågning af elektroniske betalingsinstrumenter, -ordninger og -aftaler af oktober 2020 (PISA-rammen), som findes på ECB's websted www.ecb.europa.eu.

([22]) En digital betalingstoken er en digital gengivelse af værdi med sikkerhed i fordringer eller aktiver, der er registreret andetsteds, og som muliggør værdioverførsel mellem slutbrugere. Afhængigt af det underliggende design kan digitale betalingtokens forudse en værdioverførsel uden nødvendigvis at involvere en central tredjepart og/eller anvende betalingskonti.

([23]) »Værdioverførsel«: »Handling, der iværksættes af betaleren eller på betalerens eller betalingsmodtagerens vegne med henblik på at overføre midler eller digitale betalingstokens eller indsætte eller hæve kontanter på/fra en brugerkonto uanset eventuelle underliggende forpligtelser mellem betaleren og betalingsmodtageren. Overførslen kan involvere en enkelt eller flere betalingstjenesteudbydere.« Denne definition af »værdioverførsel« i henhold til PISA-rammen afviger fra definitionen af »overførsel af midler« i Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35). En »værdioverførsel« i forbindelse med et »betalingsinstrument« som defineret i det pågældende direktiv kan kun omhandle en overførsel af »midler«. I henhold til direktivet omfatter »midler« ikke digitale betalingtokens, medmindre tokens kan klassificeres som elektroniske penge (eller mere hypotetisk som kontopenge).

([24]) Europa-Parlamentets og Rådets direktiv 98/26/EF af 19. maj 1998 om endelig afregning i betalingssystemer og værdipapirafviklingssystemer (EFT L 166 af 11.6.1998, s. 45).

overvågningsrammer fra forordningsforslagets anvendelsesområde. Af disse årsager bør ESCB's beføjelser i henhold til traktaten og Eurosystemets beføjelser i henhold til forordningen om overvågningskrav for systemisk vigtige betalingssystemer klart præciseres i betragtningerne til forordningsforslaget.

2.1.3 På samme måde glæder ECB sig over udelukkelsen fra anvendelsen af den overvågningsramme, der er fastsat i den forordningsforslaget, af IKT-tredjepartstjenesteudbydere, der er underlagt overvågningsrammer, som er oprettet med henblik på at støtte de opgaver, der er omhandlet i traktatens artikel 127, stk. 2 ([25]). I den forbindelse vil ECB gerne understrege, at ESCB-centralbanker, der handler i deres monetære kapacitet ([26]), og Eurosystemet, når de leverer tjenesteydelser via TARGET2, TARGET2-Securites (T2S) ([27]) og TARGET Instant Payment Settlement (TIPS) ([28]), ikke er omfattet af forordningsforslagets anvendelsesområde, og at de heller ikke kan betragtes som udbydere af IKT-tjenester og dermed potentielt klassificeres som udbydere af kritiske IKT-tjenester med henblik på forordningsforslaget. Eurosystemet fører tilsyn med T2S i forbindelse med sit mandat til at sikre effektive og pålidelige clearing- og betalingssystemer ESMA har desuden præciseret, at T2S ikke er en udbyder af kritiske tjenesteydelser ([29]) som omhandlet i Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 ([30]) (herefter »CSD-forordningen«). Som følge heraf sikres T2S' organisatoriske og operationelle sikkerhed, effektivitet og robusthed gennem de gældende retlige, reguleringsmæssige og operationelle rammer og aftalte ledelsesordninger eller T2S i modsætning til via CSD-forordningen.

2.1.4 Eurosystemets overvågningsramme ([31]) omfatter desuden udbydere af kritiske tjenester som Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT er et aktieelskab med begrænset ansvar, der er etableret i Belgien, og som leverer sikre betalingstjenester på internationalt plan. Nationale Bank van België/Banque Nationale de Belgique fungerer som hovedansvarlig for SWIFT og fører på grundlag af en samarbejdsbaseret tilsynsordning tilsyn med SWIFT i samarbejde med de øvrige G10-centralbanker, herunder ECB. G10-overvågerne anerkender, at det primære fokus for tilsynet er SWIFT's operationelle risiko, da dette anses for at være den primære risikokategori, hvorigennem SWIFT kan udgøre en systemisk risiko for det finansielle system i Unionen. SWIFT's Cooperative Oversight Group har i den forbindelse udviklet en række specifikke principper og forventninger på højt niveau, der gælder for SWIFT, såsom risikoidentifikation og -styring, informationssikkerhed, pålidelighed og robusthed, teknologiplanlægning og kommunikation med brugerne. G10-overvågerne forventer, at SWIFT tilslutter sig Udvalget om Betalings- og Markedsinfrastrukturer (CPMI) og Den Internationale Børstilsynsorganisations (IOSCO's) vejledning om cyberrobusthed ([32]) samt andre internationale standarder for IKT-sikkerhed, som samlet set overstiger kravene i forordningsforslaget.

2.1.5 Man kan ikke være sikker på, at SWIFT og muligvis andre tjenesteudbydere, der er underlagt Eurosystemets overvågningsramme, kan blive omfattet af forordningsforslaget som udbydere af IKT-tjenester, hvis de leverer tjenester, der ikke er omfattet af traktatens artikel 127, stk. 2. ECB glæder sig derfor meget over, at tjenesteudbydere, der allerede er underlagt Eurosystemets tilsynspolitiske rammer, herunder, men ikke begrænset til SWIFT, udelukkes fra anvendelsesområdet for den overvågningsramme, der er fastsat i forordningsforslaget.

([25]) Jf. forordningsforslagets artikel 28, stk. 5.

([26]) Jf. afsnit 1.3 i Den Europæiske Centralbanks udtalelse af 19. februar 2021 om et forslag til forordning om markeder for kryptoaktiver og om ændring af direktiv (EU) 2019/1937 (CON/2021/4). Alle ECB's udtalelser offentliggøres i EUR-Lex.

([27]) Jf. bilag IIa til Den Europæiske Centralbanks retningslinje ECB/2012/27 af 5. december 2012 om TARGET2 (Trans-European Automated Real-time Gross settlement Express Transfer system) (EUT L 30 af 30.1.2013, s. 1). Retningslinje ECB/2012/13; Den Europæiske Centralbanks retningslinje af 18. juli 2012 om TARGET2-Securities (EUT L 215 af 11.8.2012, s. 19), Den Europæiske Centralbanks afgørelse ECB/2011/20 af 16. november 2011 om fastsættelse af de nærmere regler og procedurer for gennemførelse af kriterierne for værdipapircentralers adgang til TARGET2-Securities tjenesteydelser (EUT L 319 af 2.12.2011, s. 117). Jf. også T2S-rammeaftalen og den kollektive overenskomst.

([28]) Jf. bilag IIb til retningslinje ECB/2012/27.

([29]) Jf. artikel 30, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler samt om ændring af direktiv 98/26/EF og 2014/65/EU samt forordning (EU) nr. 236/2012 (EUT L 257 af 28.8.2014, s. 1) og artikel 68 i Kommissionens delegerede forordning (EU) 2017/392 af 11. november 2016 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 for så vidt angår reguleringsmæssige tekniske standarder for krav vedrørende tilladelse, tilsyn og drift i forbindelse med værdipapircentraler (EUT L 65 af 10.3.2017, s. 48).

([30]) Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler samt om ændring af direktiv 98/26/EF og 2014/65/EU samt forordning (EU) nr. 236/2012 (EUT L 257 af 28.8.2014, s. 1).

([31]) Eurosystemets overvågningsramme, revideret udgave (juli 2016), som findes på ECB's websted www.ecb.europa.eu.

([32]) Findes på Den Internationale Betalingsbanks websted www.bis.org.

2.2 *ESCB's beføjelser inden for værdipapirafvikling*

2.2.1 Centrale værdipapircentraler (CSD'er) er finansielle markedsinfrastrukturer (FMI'er), som er strengt reguleret og underlagt tilsyn af forskellige myndigheder i henhold til CSD-forordningen, som fastsætter krav til afvikling af finansielle instrumenter samt regler om CSD'ers organisation og adfærd. Derudover bør CSD'erne notere sig CPMI-IOSCO's vejledning om cyberrobusthed, som er realiseret ved Overvågningsforventningerne til cyberrobusthed for finansielle infrastrukturer (december 2018) ([33]) . Ud over de tilsynskompetencer, der er tillagt de kompetente nationale myndigheder i henhold til CSD-forordningen, fungerer medlemmerne af ESCB som »relevante myndigheder« i deres egenskab af tilsynsførende for værdipapirafviklingssystemer, der drives af CSD'er, som centralbanker der udsteder de mest relevante valutaer, hvor afviklingen finder sted, og som centralbanker over hvis regnskaber kontantdelen af transaktionerne afvikles ([34]). I den forbindelse fremgår det af betragtning 8 i CSD-forordningen, at forordningen ikke berører det ansvar, som påhviler ECB og de nationale centralbanker, for at sikre effektive og solide clearing- og betalingssystemer inden for Unionen og i forhold til andre lande. Det fremgår endvidere af betragtning 8, at CSD-forordningen ikke bør forhindre ESCB-medlemmers adgang til oplysninger, der er relevante for udførelsen af deres opgaver ([35]), herunder deres tilsyn med CSD'er og andre FMI'er ([36]).

2.2.2 Desuden fungerer medlemmerne af ESCB ofte som afviklingsagenter for kontantdelen af værdipapirtransaktioner, og Eurosystemet tilbyder afviklingstjenester via T2S til værdipapircentralerne. Eurosystemets overvågning af T2S er forbundet med dets mandat til at sikre effektive og solide clearing- og betalingssystemer, mens CSD'ernes kompetente og relevante myndigheder har til formål at sikre, at de fungerer gnidningsløst, at afviklingen er sikker og effektiv, og at de finansielle markeder fungerer korrekt i deres respektive jurisdiktioner.

2.2.3 I henhold til forordningsforslaget ([37]) er ESCB-centralbanker ikke involveret i udarbejdelsen af tekniske standarder hvad angår præciseringen af IKT-risici. Tilsvarende underrettes de relevante myndigheder i henhold til forordningsforslaget ([38]) ikke om nogen IKT-relaterede hændelser. ESCB-centralbankerne bør opretholde samme grad af involvering som i øjeblikket i henhold til CSD-forordningen, og de relevante myndigheder bør underrettes om IKT-relaterede hændelser. Eurosystemet er den relevante myndighed for alle værdipapircentraler i euroområdet og for flere andre CSD'er i EU. ESCB-centralbankerne vil skulle underrettes om IKT-relaterede hændelser, der er relevante for udførelsen af deres opgaver, herunder tilsynet med CSD'er og andre FMI'er. De risici, som CSD'erne er udsat for, herunder IKT-risici, har mulighed for at bringe CSD'ernes smidige funktion i fare. IKT-risici er derfor væsentlige for de relevante myndigheder, som bør have en fuldstændig og detaljeret oversigt over disse risici med henblik på at vurdere dem og påvirke CSD'ernes tilgang til risikostyring. Der bør i forordningsforslaget ikke fastsættes mindre restriktive krav hvad angår IKT-risici sammenlignet med dem, der er fastsat i CSD-forordningen og de gældende lovgivningsmæssige tekniske standarder.

2.2.4 Desuden bør Unionens lovgivende organer præcisere samspillet mellem den forordningsforslaget ([39]) og de lovgivningsmæssige tekniske standarder, der supplerer CSD-forordningen. Det er navnlig uklart, hvorvidt en CSD skal fritages for forpligtelsen til at have sit eget sekundære afviklingssted, hvis dens IKT-tredjepartstjenesteudbyder vedligeholder et sådant sted ([40]). Hvis en CSD skal fritages for denne forpligtelse til at opretholde et sekundært afviklingssted, er det uklart, hvilken retlig værdi dette krav vil have. På samme måde henvises der i

([33]) Findes på ECB's websted www.ecb.europa.eu.

([34]) Jf. artikel 12 i forordning (EU) nr. 909/2014.

([35]) Jf. også artikel 13, artikel 17, stk. 4, og artikel 22, stk. 6, i forordning (EU) nr. 909/2014.

([36]) Jf. afsnit 7.3 i Den Europæiske Centralbanks udtalelse af 6. april 2017 om identifikation af kritisk infrastruktur med henblik på IT-sikkerhed (CON/2017/10), afsnit 7.2 i Den Europæiske Centralbanks udtalelse af 8. november 2018 om udpegning af væsentlige tjenester med henblik på netværks- og informationssystemssikkerhed (CON/2018/47), afsnit 3.5.2 i Den Europæiske Centralbanks udtalelse af 2. maj 2019 om netværks- og informationssystemssikkerhed (CON/2019/17) og afsnit 3.5.2 i Den Europæiske Centralbanks udtalelse af 11. november 2019 om netværks- og informationssystemssikkerhed (CON/2019/38).

([37]) Jf. forordningsforslagets artikel 54, stk. 5, og artikel 45, stk. 7, i forordning (EU) nr. 909/2014.

([38]) Jf. forordningsforslagets artikel 54, stk. 4, og artikel 45, stk. 6, i forordning (EU) nr. 909/2014.

([39]) Jf. forordningsforslagets artikel 11, stk. 5.

([40]) Jf. artikel 78, stk. 3, i Kommissionens delegerede forordning (EU) nr. 2017/2013 af 11. november 2016 om supplerende regler til Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 for så vidt angår reguleringsmæssige tekniske standarder for krav vedrørende tilladelse, tilsyn og drift i forbindelse med værdipapircentraler (EUT L 65 af 10.3.2017, s. 48).

forordningsforslaget ([41]) til målene for genopretningstid og genopretningspunkter for hver funktion ([42]), mens den relevante lovgivningsmæssige tekniske standard skelner mellem kritiske funktioner ([43]) og kritiske operationer ([44]) i forhold til den genopretningstid, der er fastsat for CSD'ers kritiske operationer. Der er behov for yderligere præcisering og overvejelser fra EU's lovgivende organer om samspillet mellem den forordningsforslaget og de lovgivningsmæssige tekniske standarder, der supplerer CSD-forordningen, for at undgå risikoen for modstridende krav. Endelig bør det præciseres, at de undtagelser, der gives CSD'er, der drives af visse offentlige enheder i henhold til CSD-forordningen ([45]), udvides i henhold til den forordningsforslaget.

2.3 *ESCB's beføjelser inden for værdipapirclearing*

2.3.1 ESCB-centralbankerne har beføjelser til at føre tilsyn med centrale modparter (CCP'er). I den forbindelse samarbejder de nationale centralbanker i Eurosystemet ofte med de relevante nationale kompetente myndigheder i forbindelse med overvågningen af og tilsynet med CCP'er og deltager i de respektive CCP-kollegier, der er oprettet i henhold til Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 ([46]) (herefter »EMIR«). De relevante medlemmer af Eurosystemet ([47]) deltager i EMIR's tilsynskollegier og repræsenterer Eurosystemet som udstedende centralbank for CCP'er, hvor euroen er en af de mest relevante valutaer for de clearede finansielle instrumenter (og for offshore-CCP'er, der clearer en betydelig andel af de finansielle instrumenter i euro). ECB er udstedende centralbank for CCP'er uden for euroområdet.

2.3.2 I henhold til forordningsforslaget ([48]) er ESCB-centralbanker ikke involveret i udarbejdelsen af tekniske standarder hvad angår præciseringen af IKT-risici. Desuden indeholder forordningsforslaget ([49]) ingen henvisning til målet om genoprettelsestid og de objektive krav til inddrivelsespunktet i henhold til EMIR ([50]). Den foreslåede reguleringsordning bør ikke gøre det muligt at fastsætte mindre restriktive krav vedrørende IKT-risici end de, der eksisterer på nuværende tidspunkt. Det er derfor afgørende at fastsætte klare mål for genopretningstid og -punkter for at have en sund ramme for styring af forretningskontinuiteten. Fastholdelse af specifikke mål for genopretningstid og -punkter er også en del af CPMI-IOSCO-principperne for finansielle markedsinfrastrukturer ([51]). Den nuværende bestemmelse i EMIR bør bibeholdes, og den foreslåede forordning bør tilpasses i overensstemmelse hermed. ESCB-centralbankerne bør inddrages i udarbejdelsen af eventuel afledt lovgivning samt yderligere præcisering og overvejelse i Unionens lovgivende organer af samspillet mellem forordningsforslaget og de supplerende lovgivningsmæssige tekniske standarder for at undgå risikoen for modstridende eller sammenfaldende krav.

3. **Specifikke bemærkninger om de tilsynsmæssige aspekter**

3.1 ECB overdrages i henhold til Rådets forordning (EU) nr. 1024/2013 ([52]) (herefter »SSM-forordningen«) specifikke opgaver vedrørende tilsyn med kreditinstitutter i euroområdet og gør ECB ansvarlig for, at den fælles tilsynsmekanisme (SSM) fungerer effektivt og konsekvent, hvor specifikke tilsynsopgaver fordeles mellem ECB og de deltagende kompetente nationale myndigheder. ECB har navnlig til opgave at udstede og tilbagekalde alle kreditinstitutters tilladelser. ECB har også til opgave bl.a. at sikre overholdelse af den relevante EU-lovgivning, der pålægger kreditinstitutterne tilsynsmæssige krav, herunder kravet om etablerede solide styringsordninger, såsom sunde risikostyringsprocedurer og interne kontrolmekanismer ([53]). Med henblik herpå har ECB alle tilsynsbeføjelser

([41]) Jf. forordningsforslagets artikel 11, stk. 6.
([42]) Jf. forordningsforslagets artikel 3, stk. 17.
([43]) Jf. artikel 76, stk. 2, litra d) og e), i Kommissionens delegerede forordning (EU)2017/392
([44]) Jf. artikel 78, stk. 2 og 3, i Kommissionens delegerede forordning (EU) 2017/392
([45]) Jf. artikel 1, stk. 4, i forordning (EU) nr. 909/2014.
([46]) Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).
([47]) Jf. artikel 18, stk. 2, litra g) og h), i EMIR.
([48]) Jf. forordningsforslagets artikel 53, stk. 2, litra b), og stk. 3, og artikel 34, stk. 3, i EMIR.
([49]) Jf. forordningsforslagets artikel 53, stk. 2, litra a.
([50]) Jf. artikel 34 i EMIR .
([51]) Jf. CPMI-IOSCO's principper for finansielle markedsinfrastrukturer, som findes på Den Internationale Betalingsbanks websted: www.bis.org.
([52]) Rådets forordning (EU) nr. 1024/2013 af 15. oktober 2013 om overdragelse af specifikke opgaver til Den Europæiske Centralbank i forbindelse med politikker vedrørende tilsyn med kreditinstitutter (EUT L 287 af 29.10.2013, s. 63).
([53]) Jf. artikel 4, stk. 1 og 4 i forordning (EU) nr. 1024/2013.

til at gribe ind i kreditinstitutternes aktiviteter, hvor disse er nødvendige for udøvelsen af ECB's funktioner. ECB og de relevante kompetente nationale myndigheder er således de kompetente myndigheder, der udøver specifikke tilsynsbeføjelser i henhold til Europa-Parlamentets og Rådets forordning 2013/575/EU ([54]) (herefter »kapitalkravsravsforordningen«) og Europa-Parlamentets og Rådets direktiv 2013/36/EU ([55]) (herefter »kapitalkravsdirektivet«).

3.2 I forordningsforslaget fastsættes det, at det fælles regelsæt og tilsynssystemet bør udvikles yderligere for at omfatte digital operationel modstandsdygtighed og IKT-sikkerhed ved at udvide mandaterne for de finansielle tilsynsmyndigheder, der har til opgave at overvåge og beskytte den finansielle stabilitet og markedsintegriteten ([56]). Målet er at fremme en omfattende IKT-ramme eller en ramme for operationelle risici gennem harmonisering af centrale krav til digital operationel modstandsdygtighed for alle finansielle enheder ([57]). Den foreslåede forordning har navnlig til formål at konsolidere og opgradere IKT-risikokravene, som hidtil er behandlet særskilt i forskellige retsakter ([58]).

3.3 Kravene vedrørende IKT-risici for den finansielle sektor er i øjeblikket spredt over en række EU-retsakter, herunder kapitalkravsdirektivet, og bløde lovgivningsinstrumenter (som EBA's retningslinjer), og de er forskelligartede og undertiden ufuldstændige. I nogle tilfælde er IKT-risikoen kun blevet behandlet implicit som en del af den operationelle risiko, mens den i andre slet ikke er blevet behandlet. Dette bør afhjælpes ved at tilpasse forordningsforslaget og de pågældende retsakter. Med henblik herpå indeholder det foreslåede ændringsdirektiv en række ændringer, der forekommer nødvendige for at skabe retlig klarhed og konsekvens i forbindelse med anvendelsen af de forskellige krav til digital operationel modstandsdygtighed. De ændringer af kapitalkravsdirektivet, der i øjeblikket foreslås i det foreslåede ændringsdirektiv ([59]), henviser imidlertid kun til bestemmelserne om beredskabsplaner og forretningskontinuitetsplaner ([60]), da de angiveligt indirekte tjener som grundlag for håndteringen af IKT-risikostyring.

3.4 Desuden fastsættes det i forordningsforslaget ([61]), at finansielle enheder, herunder kreditinstitutter, skal have interne styrings- og kontrolrammer, der sikrer en effektiv og forsigtig styring af alle IKT-risici. Forordningsforslaget ([62]) indeholder bestemmelser om anvendelsen af de krav, der er fastsat heri, på individuelt og konsolideret niveau, men uden tilstrækkelig koordinering med den sektorspecifikke lovgivning, der henvises til. Endelig fastsættes det i forordningsforslaget ([63]), at den kompetente myndighed, der er udpeget i henhold til artikel 4 i kapitalkravsdirektivet, med forbehold af bestemmelserne om tilsynsrammen for udbydere af kritiske IKT-tjenester, der er omhandlet i forordningsforslaget ([64]), skal sikre, at de deri fastsatte forpligtelser for kreditinstitutter overholdes af den kompetente myndighed, der er udpeget i henhold til i kapitalkravsdirektivet, uden at dette berører de specifikke opgaver, som overdrages til ECB i henhold til SSM-forordningen.

3.5 I lyset af ovenstående forstår ECB det således, at forordningsforslaget, for så vidt angår kreditinstitutter og med undtagelse af bestemmelserne i forordningsforslaget vedrørende overvågningsrammen for kritiske IKT-tredjepartstjenesteudbydere ([65]), har til formål at fastlægge en tilsynsmæssig intern styringsramme for styring af IKT-risici, som vil blive integreret i den generelle interne styringsramme i henhold til kapitalkravsdirektivet. I betragtning af den foreslåede rammes tilsynsmæssige karakter vil de kompetente myndigheder, der er ansvarlige for tilsynet med overholdelsen af de forpligtelser, der er fastsat i den foreslåede ramme, herunder ECB, desuden være de myndigheder, der er ansvarlige for banktilsyn i overensstemmelse med SSM-forordningen.

([54]) Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).

([55]) Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

([56]) Jf. betragtning 8 til forordningsforslaget.

([57]) Jf. betragtning 11 til forordningsforslaget.

([58]) Jf. betragtning 12 til forordningsforslaget.

([59]) Jf. betragtning 4 og 5 til det foreslåede ændringsdirektiv.

([60]) Jf. kapitalkravsdirektivets artikel 85.

([61]) Jf. forordningsforslagets artikel 4, stk. 1.

([62]) Jf. forordningsforslagets artikel 25, stk. 3, nr. 4.

([63]) Jf. forordningsforslagets artikel 41.

([64]) Jf. forordningsforslagets kapitel V, afsnit II.

([65]) Jf. forordningsforslagets kapitel V, afsnit II.

3.6 Unionens lovgivende organer kan således ønske at tage hensyn til følgende forslag for at øge klarheden og koordineringen mellem forordningsforslaget og kapitalkravsdirektivet. For det første kan kravene i forordningsforslaget udtrykkeligt betegnes som tilsynsmæssige, som det bl.a. er sket i CSD-forordningen ([66]). For det andet kan ordlyden af betragtningerne i det foreslåede ændringsdirektiv ([67]) udvides, eftersom kravene i forordningsforslaget rækker ud over den eneste fase beredskabs-og driftskontinuitetsplaner. IKT-risikostyringsforanstaltninger er generelt omfattet af det mere generelle anvendelsesområde for solide ledelsesordninger i henhold til kapitalkravsdirektivets artikel 74 ([68]). For det tredje bør forordningsforslaget ([69]) ændres for i betragtningerne at minde om ECB's kompetence med hensyn til tilsynet med kreditinstitutter i henhold til traktaten og SSM-forordningen. For det fjerde bør henvisningen til anvendelsen på individuelt og konsolideret niveau af kravene deri ([70]) revideres, eftersom delkonsolideret og konsolideret niveau ikke er defineret i forordningsforslaget, og visse typer formidlere ikke er underlagt konsolideret tilsyn i henhold til den relevante lovgivning (f.eks. betalingsinstitutter). Desuden bør anvendelsesniveauet for kravene i forordningsforslaget udelukkende komme fra den lovgivning, der gælder for hver enkelt type finansiel enhed. For kreditinstitutterne er der en klar forbindelse mellem kapitalkravsdirektivet og forordningsforslaget, og derfor vil kravene i forordningsforslaget automatisk finde anvendelse på individuelt, delkonsolideret eller konsolideret niveau ([71]), alt efter hvad der er relevant. Endelig kan EU's lovgivende organer overveje at indføre en overgangsordning for at forvalte perioden mellem forordningsforslagets ikrafttrædelse og de reguleringsmæssige tekniske standarders ikrafttrædelse, der er omhandlet i forordningsforslaget, eftersom nogle formidlere, herunder kreditinstitutter, allerede er underlagt regler om IKT-risici, der gælder for specifikke sektorer, og som er mere detaljerede end de generelle bestemmelser i forordningsforslaget.

3.7 ECB har i henhold til SSM-forordningen fået til opgave at sikre, at kreditinstitutterne overholder de EU-retlige krav om, at kreditinstitutterne skal have robuste risikostyringsprocedurer og interne kontrolmekanismer ([72]). Det betyder, at ECB skal sikre, at kreditinstitutterne gennemfører politikker og processer til vurdering og håndtering af deres eksponering for operationel risiko, herunder modelrisici, som dækker sjældne og meget alvorlige hændelser. Kreditinstitutterne skal præcisere, hvad der forstås ved operationel risiko med henblik på disse politikker og procedurer ([73]).

3.8 I juli 2017 vedtog Den Europæiske Centralbank (ECB) rammen for indberetning af cyberhændelser (herefter »rammen«) på grundlag af et udkast fra Tilsynsrådet i overensstemmelse med SSM-forordningens artikel 26, stk. 8, og artikel 6, stk. 2, og artikel 21, stk. 1, i Den Europæiske Centralbanks forordning (EU) nr. 468/2014 (ECB/2014/17) ([74]). Rammen består af en bindende anmodning (individuelle afgørelser rettet til kreditinstitutter) om oplysninger og/eller indberetning på grundlag af SSM-forordningens artikel 10 ([75]). Nogle lande har allerede indført en procedure for indberetning af hændelser, hvorefter det kræves, at kreditinstitutterne indberetter alle væsentlige cyberhændelser til deres kompetente nationale myndigheder. I de pågældende lande indberetter de signifikante kreditinstitutter stadig hændelser til de kompetente nationale myndigheder, som derefter uden unødigt

([66]) Jf. overskriften til kapitel II, afdeling 4, »Tilynsmæssige krav« i CSD-forordningen.
([67]) Jf. betragtning 4 til det foreslåede ændringsdirektiv.
([68]) I artikel 85 i direktiv 2013/36/EU er blot en præcisering. Jf. i den forbindelse også s. 4, 11 og 37 i Den Europæiske Banktilsynsmyndigheds retningslinjer for IKT-styring og sikkerhedsrisikostyring af 29. november 2019 (herefter »EBA's retningslinjer«), hvor det generelle retsgrundlag udtrykkeligt fremgår af artikel 74 i direktiv 2013/36/EU.
([69]) Jf. forordningsforslagets artikel 41, stk. 1.
([70]) Jf. forordningsforslagets artikel 25, stk. 3 og 4.
([71]) Jf. også kapitalkravsdirektivets artikel 109.
([72]) Jf. SSM-forordningens artikel 4, stk. 1, litra e).
([73]) Jf. kapitalkravsdirektivets artikel 85.
([74]) Den Europæiske Centralbanks forordning (EU) nr. 468/2014 af 16. april 2014 om fastlæggelse af en ramme for samarbejde inden for Den Fælles Tilsynsmekanisme mellem Den Europæiske Centralbank og de kompetente nationale myndigheder og med de udpegede nationale myndigheder (SSM-rammeforordningen) (ECB/2014/17) (EUT L 141 af 14.5.2014, s. 1).
([75]) Særligt skal en cyberhændelse (et identificeret muligt brud på informationssikkerheden (uanset om det er ondsindet eller utilsigtet) indberettes til ECB, hvis mindst en af følgende betingelser er opfyldt: 1) der er en potentiel finansiel indvirkning på 5 mio. euro eller 0,1 pct. af CET1, 2) hændelsen er offentligt rapporteret eller forårsager omdømmemæssige skader, 3) hændelsen er bragt til den øverste informationsansvarlige uden for den regelmæssig rapportering, 4) banken har underrettet computerkriseberedskabsteamet/computersikkerhedsberedskabsteamet, et sikkerhedsorgan eller politiet om hændelsen, 5) hændelsen har udløst nødbackup- eller forretningskontinuitetsprocedurer, eller der er indgivet et cyberforsikringskrav, 6) der er sket en overtrædelse af lovkrav eller reguleringsmæssige krav, 7) banken anvender interne kriterier og ekspertvurdering (herunder en potentiel systemisk virkning) og beslutter at informere ECB.

ophold videresender dem til ECB på vegne af enhederne under tilsyn. Derfor er ovennævnte afgørelser også rettet til de kompetente nationale myndigheder om på grundlag af rammen at fremsende disse oplysninger til ECB. ECB støtter EU-lovgivningsorganernes bestræbelser på at fremme harmonisering og tilpasning, bl.a. for så vidt angår de regler og forpligtelser, der gælder for kreditinstitutterne om indberetning af hændelser. I lyset heraf er ECB parat til at ændre (og eventuelt ophæve) rammen, hvor det er nødvendigt, i lyset af forordningsforslagets endelige vedtagelse.

4. Specifikke bemærkninger om IKT-risikostyring, indberetning af hændelser, test af operationel modstandsdygtighed og IKT-tredjepartsrisiko

4.1 *IKT-risikostyring*

4.1.1 ECB glæder sig over, at der med forordningsforslaget indføres en solid og omfattende IKT-risikostyringsramme, der omfatter CPMI-IOSCO's vejledning om cyberrobusthed og er nøje afstemt efter bedste praksis, herunder Eurosystemets forventninger til overvågning af cyberrobusthed for FMI'er.

4.1.2 ECB støtter forestillingen om, at finansielle enheder bør foretage risikovurderinger efter hver »større ændring« i net- og informationssystemets infrastruktur ([76]). Forordningsforslaget indeholder dog ingen definition af »større ændringer«, hvilket skaber uønsket mulighed for forskellige fortolkninger fra finansielle enheder, hvilket i sidste ende kan hæmme den forordningsforslagets harmoniseringsmål. Af hensyn til retssikkerheden kan EU's lovgivende organer overveje at indføre en definition af »større ændringer« i forordningsforslaget.

4.1.3 ECB støtter generelt ideen om, at andre finansielle enheder end mikrovirksomheder skal indberette relevante omkostninger og tab som følge af IKT-afbrydelser og IKT-relaterede hændelser til de kompetente myndigheder ([77]). For at sikre systemets overordnede effektivitet og for at undgå risikoen for at overvælde de kompetente myndigheder og finansielle enheder med et uforholdsmæssigt stort antal rapporter kan det imidlertid være nyttigt for Unionens lovgivende organer at undersøge indførelsen af relevante tærskler, eventuelt af kvantitativ art.

4.1.4 ECB anerkender muligheden for, at de finansielle enheder delegerer opgaverne med at kontrollere overholdelsen af IKT-risikostyringskravene til koncerninterne eller eksterne virksomheder efter godkendelse fra de kompetente myndigheder ([78]). Samtidig er det vigtigt, at Unionens lovgivende organer præciserer, hvordan de kompetente myndigheders godkendelse vil blive givet i tilfælde, hvor en finansiel enhed er underlagt flere kompetente myndigheder. Det kan forekomme, hvis en finansiel enhed er et kreditinstitut, en udbyder af kryptoaktivtjenester og/eller en betalingstjenesteudbyder. Hvad endelig angår den identifikation og klassificering, der skal foretages af de finansielle enheder i henhold til forordningsforslaget ([79]), er ECB med henblik på klassificeringen af aktiver af den opfattelse, at det i henhold til forordningsforslaget også kræves, at de finansielle enheder tager hensyn til sådanne aktivers kritiske karakter (dvs. om de understøtter kritiske funktioner).

4.2 *Indberetning af hændelser*

4.2.1 ECB glæder sig over de bestræbelser, der i forordningsforslaget er skitseret med henblik på at harmonisere IKT-hændelsesindberetningslandskabet i Unionen og arbejde hen imod en centraliseret indberetning af større IKT-relaterede hændelser ([80]). Indførelsen af en harmoniseret ramme for indberetningen af større IKT-relaterede hændelser ([81]) til de relevante kompetente myndigheder vil i princippet strømline og harmonisere indberetningsbyrden for de finansielle enheder, herunder kreditinstitutterne. De kompetente myndigheder vil drage fordel af det bredere omfang af de hændelser, der er omfattet, og som rækker ud over cyberrelaterede hændelser, der i øjeblikket er omfattet af de eksisterende rammer ([82]). Den fremtidige vedtagelse af forordningsforslaget vil kræve en revision og potentielt ophævelse af de eksisterende rammer, herunder SSM's ramme for indberetning af cyberhændelser. For at opnå en reel strømlining og fuld tilpasning på tværs af alle rammer er det dog afgørende at sikre, at anvendelsesområdet for bestemmelserne om indberetning af hændelser i forordningsforslaget, herunder alle relevante definitioner, tærskler og indberetningsparametre, bringes i fuld overensstemmelse med de relevante

([76]) Jf. forordningsforslagets artikel 7, stk. 3.
([77]) Jf. forordningsforslagets artikel 10, stk. 9.
([78]) Jf. forordningsforslagets artikel 5, stk. 10.
([79]) Jf. forordningsforslagets artikel 7.
([80]) Jf. artikel 19 i den foreslåede forordning.
([81]) Jf. forordningsforslagets artikel 3, stk. 7 og 18.
([82]) Jf. eksempelvis rammen.

rammer. Det er navnlig yderst vigtigt at sikre overensstemmelse mellem forordningsforslaget på den ene side og Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 ([83]) (herefter »PSD2«) og EBA's retningslinjer om indberetning af større hændelser (herefter »EBA's retningslinjer«) på den anden side. Det foreslåede ændringsdirektiv ([84]) indeholder ændringer til PSD2 hvad angår afgrænsningen af indberetningen af hændelser mellem forordningsforslaget og PSD2, som først og fremmest vil berøre betalingstjenesteudbydere, som også kan få tilladelse som kreditinstitutter, samt de kompetente myndigheder. Der mangler klarhed med hensyn til proceduren for anmeldelse af hændelser, og der er et potentielt sammenfald mellem nogle af de hændelser, der skal indberettes i henhold til både forordningsforslaget og EBA's retningslinjer.

4.2.2 Procedurerne for indberetning af større hændelser i henhold til henholdsvis forordningsforslaget ([85]), PSD2 og de tilsvarende retningslinjer fra EBA vil kræve, at betalingstjenesteudbyderne indsender en hændelsesindberetning til deres respektive kompetente myndigheder, når hændelsen er blevet klassificeret. De første rapporter indfanger reelt ikke kernen, den årsag eller det funktionelle område, der er berørt af hændelsen, og betalingstjenesteudbyderne vil måske kun være i stand til at foretage sådanne sondringer på et senere tidspunkt, når der foreligger mere detaljerede oplysninger om hændelsen. Som følge heraf kan de første indberetninger af hændelser indsendes både i henhold til forordningsforslaget og EBA's retningslinjer, eller betalingstjenesteudbyderne kan træffe afgørelse om et fælles regelsæt for indberetning og korrigere deres indberetninger på et senere tidspunkt. Den samme usikkerhed (f.eks. med hensyn til den grundlæggende årsag til en hændelse) kan også afspejles i foreløbige og endelige rapporter. Dette vil igen øge potentialet for parallel indsendelse af rapporter til de kompetente myndigheder i henhold til forordningsforslaget og PSD2.

4.2.3 Nogle hændelser, der kan kategoriseres som IKT-relaterede hændelser, kan også have indvirkning på andre områder og vil derfor skulle indberettes i henhold til EBA's retningslinjer. Dette kan være tilfældet, hvis en hændelse har en indvirkning fra et IKT-perspektiv, men samtidig også har påvirket leveringen af betalingstjenester direkte og/eller andre ikke-IKT-funktionelle områder eller kanaler. Der kan desuden være tilfælde, hvor det ikke er muligt at skelne mellem operationelle og IKT-relaterede hændelser. I tilfælde, hvor den samme finansielle enhed er et signifikant kreditinstitut og en udbyder af betalingstjenester, skal den samme enhed i henhold til forordningsforslaget indberette den IKT-relaterede hændelse to gange, idet den er underlagt to kompetente myndigheder. I lyset af ovenstående bør det i forordningsforslaget præciseres, hvordan samspillet mellem PSD2 og EBA's retningslinjer skal fungere i praksis. Af hensyn til harmoniseringen og strømliningen af indberetningsforpligtelserne er det vigtigt, at Unionens lovgivende organer overvejer de resterende spørgsmål om dobbeltindberetning, og at det afklares, om forordningsforslaget på den ene side og PSD2 og EBA's retningslinjer på den anden side vil eksistere side om side, eller om der bør være en enkelt række krav om indberetning af hændelser.

4.2.4. Der indføres med forordningsforslaget et krav om, at de kompetente myndigheder ([86]), når de har modtaget en rapport, anerkender modtagelsen af underretningen og hurtigst muligt giver den finansielle enhed den nødvendige feedback eller vejledning, navnlig med henblik på at drøfte afhjælpende foranstaltninger på virksomhedsniveau eller metoder til at minimere de negative virkninger på tværs af sektorerne. Dette vil betyde, at de kompetente myndigheder aktivt bør bidrage til at håndtere og afhjælpe hændelser og samtidig vurdere en enhed under tilsyns reaktion på kritiske hændelser. ECB understreger, at ansvaret for og ejerskabet til afhjælpningen og følgerne af en hændelse udelukkende og klart bør ligge hos den pågældende finansielle enhed. ECB vil derfor foreslå, at feedback og vejledning begrænses til kun at omfatte tilsynsmæssig feedback og vejledning på højt niveau. Hvis feedbacken var bredere, ville det kræve specialiserede fagfolk med meget betydelig teknisk viden, der som regel ikke findes i den talentpulje, som tilsynsmyndighederne har adgang til.

4.3 *Test af digital operationel modstandsdygtighed*

4.3.1 ECB glæder sig over forordningsforslagets ([87]) krav om test af den digitale operationelle modstandsdygtighed på tværs af de finansielle enheder og behovet for, at hver institution har sit eget testprogram. Forskellige testtyper beskrives i forordningsforslaget ([88]) som vejledende for finansielle enheder. Testtyperne er ikke særlig klare, og nogle test, såsom kompatibilitetstest, spørgeskemaer eller scenariebaserede test, kan fortolkes af ESA'er, kompetente

([83]) Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, og om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35).
([84]) Jf. artikel 7, stk. 9 i det foreslåede ændringsdirektiv.
([85]) Jf. forordningsforslagets artikel 17, stk. 3.
([86]) Jf. forordningsforslagets artikel 20.
([87]) Jf. forordningsforslagets artikel 21 og 22.
([88]) Jf. forordningsforslagets artikel 22, stk. 1.

myndigheder eller finansielle enheder. Derudover foreligger der heller ikke nogen vejledning hvad angår hyppigheden af hver enkelt test. En mulig løsning kan være, at der i forordningsforslaget fastsættes fælles testkrav med en mere præcis beskrivelse af de testtyper, der er fastsat i de lovgivningsmæssige og gennemførelsesmæssige tekniske standarder.

4.3.2 Trusselsstyret penetrationstest (TLPT) er et effektivt redskab til at teste sikkerhedsbeskyttelsen og -beredskabet. ECB opfordrer derfor de finansielle enheder til at foretage TLPT. Det er ikke kun de tekniske foranstaltninger, der testes med dette værktøj, men også personale og processer. Resultaterne af disse test kan i betydelig grad øge den øverste ledelses kendskab til sikkerheden i de enheder, der testes. De europæiske rammer for samarbejde mellem etiske red teams baseret på trusselsefterretninger (TIBER-EU) ([89]) og andre TLPT-værktøjer, der allerede er til rådighed uden for Unionen, er primære instrumenter, som enhederne selv kan bruge til selv at vurdere, afprøve, praktisere og forbedre deres cyberrobusthed og -forsvar.

4.3.3 I de fleste medlemsstater, hvor TIBER-EU er blevet gennemført, spiller overvågere og tilsynsmyndigheder ikke en aktiv rolle i gennemførelsen af et lokalt TIBER-XX-program, og Tiber Cyber Team (TCT) er i næsten alle tilfælde placeret uafhængigt af disse funktioner. Derfor bør avanceret testning i henhold til forordningsforslaget ([90]) ved hjælp af TLPT gennemføres som et værktøj til at styrke det finansielle økosystem og øge den finansielle stabilitet snarere end som et rent tilsynsværktøj. Desuden er der ikke behov for at udvikle en ny avanceret ramme for test af cyberrobusthed, da medlemsstaterne allerede i vid udstrækning har vedtaget TIBER-EU, som på nuværende tidspunkt er den eneste af disse rammer i EU.

4.3.4 Kravene til testere bør ikke fremgå af forordningsforslagets hoveddel, da den TLPT-relaterede sektor stadig er under udvikling, og innovationen kan hæmmes af, at der stilles særlige krav. ECB er dog af den opfattelse, at de finansielle enheder for at sikre en høj grad af uafhængighed i udførelsen af test ikke bør ansætte eller kontraktansætte testere, som er ansat af eller har indgået kontrakt med finansielle enheder i deres egen koncern, eller som på anden vis ejes og/eller kontrolleres af de finansielle enheder, der skal testes.

4.3.5 For at mindske risikoen for fragmentering og sikre harmonisering bør der i forordningsforslaget gives mandat til én TLPT, der gælder for den finansielle sektor i Unionen. Fragmentering kan føre til øgede omkostninger og tekniske, operationelle og finansielle ressourcekrav for både de kompetente myndigheder og finansielle institutioner. Disse øgede omkostninger og krav kan i sidste ende have en negativ indvirkning på den gensidige anerkendelse af test. Denne manglende harmonisering og de deraf følgende problemer med gensidig anerkendelse er særlig kritiske for finansielle enheder, som kan have flere tilladelser og/eller operere i flere jurisdiktioner i Unionen. De lovgivningsmæssige og gennemførelsesmæssige tekniske standarder, der i henhold til forordningsforslaget skal udarbejdes for TLPT, bør være i overensstemmelse med TIBER-EU. ECB glæder sig desuden over muligheden for at blive inddraget i udarbejdelsen af disse lovgivningsmæssige og gennemførelsesmæssige tekniske standarder i samarbejde med ESA'erne.

4.3.6 En aktiv inddragelse af de kompetente myndigheder i testene kan føre til en potentiel interessekonflikt med den anden funktion, de udfører, dvs. vurderingen af den finansielle enheds ramme for test. ECB foreslår på den baggrund, at enhver forpligtelse for kompetente myndigheder hvad angår validering af dokumenter og udstedelse af en attestering til en TLPT test fjernes fra forordningsforslaget.

4.4 IKT-tredjepartsrisiko

4.4.1 ECB glæder sig over indførelsen af en omfattende række centrale principper og en solid tilsynsramme til at identificere og styre IKT-risici, der hidrører fra udbydere af IKT-tjenester, uanset om de tilhører samme gruppe af finansielle enheder. For at opnå en effektiv IKT-risikoidentifikation og -styring er det dog vigtigt at identificere og klassificere bl.a. kritiske eksterne udbydere af IKT-tjenester korrekt. I den forbindelse hilses indførelsen af delegerede retsakter ([91]), som supplerer de kriterier, der skal anvendes til klassificeringsformål ([92]), velkommen, men ECB bør høres forud for vedtagelsen af sådanne delegerede retsakter.

([89]) Findes på ECB's websted www.ecb.europa.eu.
([90]) Forordningsforslagets artikel 23 og 24.
([91]) Jf. forordningsforslagets artikel 28, stk. 3.
([92]) Jf. forordningsforslagets artikel 28, stk. 2.

4.4.2 Hvad angår tilsynsrammens struktur ([93]) er der behov for yderligere præcisering af den rolle, det blandede udvalg skal spille. ECB glæder sig samtidig over at være medtaget i tilsynsforummet som observatør, da denne rolle vil give ECB den samme adgang til dokumentation og information som stemmeberettigede medlemmer ([94]). ECB vil gerne henlede EU's lovgivende organers opmærksomhed på, at ECB i sin rolle som observatør vil bidrage til tilsynsforummets arbejde både i sin egenskab af udstedende centralbank med ansvar for tilsynet med markedsinfrastrukturer og som tilsynsførende for kreditinstitutter. ECB bemærker desuden, at ECB ud over at være observatør i tilsynsforummet også vil være en del af det fælles undersøgelsesteam som kompetent myndighed. I den forbindelse kan sammensætningen af de fælles undersøgelsesteam ([95]) overvejes yderligere af Unionens lovgivende organer for at sikre en passende inddragelse af de relevante kompetente myndigheder. ECB mener ligeledes, at det maksimale antal deltagere i de fælles undersøgelsesteam bør øges under hensyntagen til IKT-tredjepartstjenesternes kritikalitet, kompleksitet og omfang.

4.4.3 ECB bemærker, at den hovedansvarlige for overvågningen i henhold til forordningsforslaget kan forhindre kritiske IKT-tredjepartstjenesteudbydere i at indgå yderligere underentrepriseordninger, hvis i) den påtænkte underleverandør er en IKT-tredjepartstjenesteudbyder eller en IKT-underkontrahent, der er etableret i et tredjeland, og ii) underentreprisen vedrører en kritisk eller væsentlig funktion for den finansielle enhed. ECB ønsker at understrege, at disse beføjelser kun kan udøves af den hovedansvarlige for overvågningen i forbindelse med underentrepriseordninger, hvor en kritisk IKT-tjenesteudbyder leverer en kritisk eller væsentlig funktion i underentreprise til en særskilt juridisk enhed, der er etableret i et tredjeland. ECB forstår det således, at den hovedansvarlige for overvågningen ikke kunne udøve tilsvarende beføjelser for at forhindre en udbyder af kritiske IKT-tjenester i at outsource den finansielle enheds kritiske eller væsentlige funktioner til den pågældende tjenesteudbyders faciliteter, der er beliggende i et tredjeland. Det kan f.eks. være tilfældet, at kritiske data og/eller oplysninger ud fra et operationelt synspunkt lagres eller behandles af faciliteter uden for Det Europæiske Økonomiske Samarbejdsområde (EØS). I et sådant tilfælde giver beføjelserne for den hovedansvarlige for overvågningen måske ikke de kompetente myndigheder tilstrækkelige beføjelser til at få adgang til alle oplysninger, lokaler, infrastrukturer og personale, der er relevante for udførelsen af alle den finansielle enheds kritiske eller væsentlige funktioner. For at sikre, at de kompetente myndigheder uhindret kan udføre deres opgaver, foreslår ECB, at den hovedansvarlige for overvågningen får beføjelse til også at begrænse kritiske tredjeparters brug af faciliteter uden for EØS. Den beføjelse kunne udøves i de specifikke tilfælde, hvor der ikke findes administrative ordninger med de relevante tredjelandsmyndigheder, som fastsat i forordningsforslaget ([96]), eller repræsentanterne for de kritiske IKT-tredjepartstjenesteudbydere ikke giver tilstrækkelige garantier inden for rammerne af det relevante tredjeland med hensyn til adgang til de oplysninger, lokaler, infrastruktur og personale, der er nødvendige for at udføre overvågnings- eller tilsynsopgaverne.

4.4.4 Endelig kan et krav om, at de kompetente myndigheder skal følge op på anbefalingerne fra den hovedansvarlige for overvågningen ([97]), risikere at være ineffektive, da de kompetente myndigheder måske ikke har et holistisk syn på de risici, som hver enkelt udbyder af kritiske IKT-tjenester genererer. Det kan desuden være påkrævet for de kompetente myndigheder, at de træffer foranstaltninger over for deres finansielle enheder under tilsyn, hvis anbefalingerne ikke følges af de kritiske tredjepartstjenesteudbydere. De kompetente myndigheder kan i henhold til forordningsforslaget ([98]) kræve, at deres finansielle enheder under tilsyn midlertidigt suspenderer den kritiske tredjepartstjeneste eller bringer udestående kontrakter med kritiske tredjepartstjenesteudbydere til ophør. Det er vanskeligt at omsætte den planlagte opfølgningsproces til konkrete tiltag. Det er navnlig ikke klart, om en finansiel enhed under tilsyn vil være i stand til at suspendere eller opsige en kontrakt med en kritisk tredjepartstjenesteudbyder. Det skyldes, at den kritiske IKT-tredjepartstjenesteudbyder kan være en væsentlig udbyder for den pågældende finansielle enhed, eller på grund af de omkostninger og skader, som den finansielle enhed kontraktmæssigt eller på anden måde kan lide som følge af en sådan suspension eller opsigelse. Desuden understøtter denne tilgang ikke tilsynskonvergens, da de kompetente myndigheder kan fortolke den samme henstilling forskelligt. Det kan i sidste ende hæmme den påtænkte harmonisering og konsekvente tilgang til overvågning af kritiske IKT-tredjepartsrisici på EU-plan. I lyset af ovenstående kan Unionens lovgivende organer overveje at tildele de retlige overvågere specifikke håndhævelsesbeføjelser over for udbydere af kritiske IKT-tjenester under hensyn til de begrænsninger, der er fastsat i *Meroni*-doktrinen, som delvist blev lempet af Domstolen i sin dom i ESMA-sagen ([99]).

([93]) Jf. artikel 29 i den foreslåede forordning.
([94]) Jf. forordningsforslagets artikel 29, stk. 3.
([95]) Jf. forordningsforslagets artikel 35.
([96]) Jf. forordningsforslagets artikel 39, stk. 1.
([97]) Jf. forordningsforslagets artikel 29, stk. 4 og 37.
([98]) Jf. forordningsforslagets artikel 37, stk. 3.
([99]) Jf. Domstolens dom (Store Afdeling) af 22. januar 2014, Det Forenede Kongerige Storbritannien og Nordirland mod Europa-Parlamentet og Rådet for Den Europæiske Union (EU) nr. 236/2012 — Sag C-270/12.

Hvor ECB foreslår ændringer af forordningsforslaget, vedlægges som bilag ændringsforslag med en begrundelse herfor i et separat teknisk arbejdsdokument. Det tekniske arbejdsdokument er tilgængeligt på engelsk på EUR-Lex.

Udfærdiget i Frankfurt am Main, den 4. juni 2021.

Formand for ECB
Christine LAGARDE