I

*(Resolutioner, rekommendationer och yttranden)*

REKOMMENDATIONER

# EUROPEISKA SYSTEMRISKNÄMNDEN

## EUROPEISKA SYSTEMRISKNÄMNDENS REKOMMENDATION

**av den 2 december 2021**

**om ett europeisk ramverk för relevanta myndigheters samordning av åtgärder mot systemiska cyberincidenter**

**(ESRB/2021/17)**

(2022/C 134/01)

EUROPEISKA SYSTEMRISKNÄMNDENS STYRELSE HAR ANTAGIT DENNA REKOMMENDATION

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av avtalet om Europeiska ekonomiska samarbetsområdet ([1]), särskilt bilaga IX,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 1092/2010 av den 24 november 2010 om makrotillsyn av det finansiella systemet på EU-nivå och om inrättande av en europeisk systemrisknämnd ([2]), särskilt artikel 3.2 b och 3.2 d samt artiklarna 16 och 18,

med beaktande av Europeiska systemrisknämndens beslut ESRB/2011/1 av den 20 januari 2011 om arbetsordningen för Europeiska systemrisknämnden ([3]), särskilt artiklarna 18–20, och

av följande skäl:

(1) Enligt vad som framgår av skäl 4 i Europeiska systemrisknämndens rekommendation ESRB/2013/1 ([4]) är makrotillsynens slutmål att bidra till att värna stabiliteten i det finansiella systemet som helhet, genom att bland annat stärka det finansiella systemets förmåga att återhämta sig efter störningar och minska uppbyggnaden av systemrisker, för att därigenom säkerställa att finanssektorn på ett uthålligt sätt bidrar till den ekonomiska tillväxten. Europeiska systemrisknämnden (ESRB) ansvarar för makrotillsynen över det finansiella systemet inom unionen. ESRB bör därför bidra till att förhindra eller minska systemrisker för den finansiella stabiliteten, inklusive risker som hör samman medcyberincidenter och lämnar förslag på hur dessa risker kan reduceras.

(2) Större cyberincidenter kan utgöra en systemrisk för det finansiella systemet med tanke på deras potential att störa kritiska finansiella tjänster och transaktioner. Den inledande chocken kan förstärkas genom operativa eller finansiella spridningseffekter eller genom att förtroendet för det finansiella systemet urholkas. Om det finansiella systemet inte kan absorbera dessa chocker äventyras den finansiella stabiliteten och situationen kan leda till en systemisk cyberkris ([5]).

([1]) EGT L 1, 3.1.1994, s 3.
([2]) EGT L 331, 15.12.2010, s 1.
([3]) EUT C 58, 24.2.2011, s. 4.
([4]) Europeiska systemrisknämndens rekommendation ESRB/2013/1 av den 4 april 2013 om makrotillsynspolitikens mellanliggande mål och instrument (EUT C 170, 15.6.2013, s. 1).
([5]) Se *Systemic cyber risk*, ESRB, februari 2020, finns på ESRB:s webbplats www.esrb.europa.eu

(3) De ständigt föränderliga cyberhoten och den senaste tidens ökning av större cyberincidenter är indikatorer på större risker för den finansiella stabiliteten i unionen. Covid-19 pandemin har visat vilken betydelse tekniken har för att det finansiella systemet ska fungera. Relevanta myndigheter och institutioner tvingades anpassa sin tekniska infrastruktur och sina ramar för riskhantering till en plötslig ökning av distansarbete, vilket har ökat det finansiella systemets totala exponering för cyberhot och gjort det möjligt för brottslingar att utforma nya metoder och anpassa befintliga metoder för att utnyttja situationen ([6]). Mot denna bakgrund ökade antalet cyberincidenter som rapporterades till ECB:s banktillsyn under 2020 med 54 procent jämfört med 2019 ([7]).

(4) En större cyberincidents potentiellt storskaliga, hastighet och snabba spridningstakt kräver ett effektivt svar från de relevanta myndigheterna för att begränsa de potentiella negativa effekterna för den finansiella stabiliteten. Snabb samordning och kommunikation mellan relevanta myndigheter på unionsnivå kan bidra till en tidig bedömning av större cyberincidenters inverkan på den finansiella stabiliteten, upprätthålla förtroendet för det finansiella systemet och begränsa spridningen till andra finansinstitut och därigenom bidra till att förhindra att en större cyberincident blir en risk för den finansiella stabiliteten.

(5) Den underliggande chocken uppstår på ett nytt sätt jämfört med traditionella finans- och likviditetskriser som de relevanta myndigheterna tidigare ställts inför. Utöver de ekonomiska aspekterna måste den övergripande riskbedömningen omfatta omfattningen och effekterna av driftsstörningar, eftersom dessa kan påverka valet av makrotillsynsverktyg. På samma sätt kan den finansiella stabiliteten också påverka cyberexperternas val av riskreducerande åtgärder. Detta kräver nära och snabb samordning och öppen kommunikation, bl.a. för att skapa en helhetsbild.

(6) Det finns en risk för att myndigheterna misslyckas med samordningen och detta måste åtgärdas. Relevanta myndigheter i unionen måste inrätta en samordning sinsemellan och även med andra myndigheter, t.ex. Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), med vilka de inte har något etablerat samarbete. Eftersom ett betydande antal av unionens finansinstitut är verksamma globalt kommer en större cyberincident sannolikt inte att vara begränsad till unionen, eller kan utlösas utanför unionen, och kan kräva en global samordning av insatserna.

(7) De relevanta myndigheterna måste vara förberedda för sådana kontakter. Annars finns det risk för att de vidtar inkonsekventa åtgärder som strider mot, eller äventyrar, andra myndigheters åtgärder. En misslyckad samordning kan förvärra chocken för det finansiella systemet genom att förtroendet för det finansiella systemets funktion urholkas, vilket i värsta fall kan utgöra en risk för den finansiella stabiliteten ([8]). Därför bör man vidta nödvändiga åtgärder för att hantera riskerna för den finansiella stabiliteten som kan uppstå till följd av bristfällig samordning i händelse av en större cyberincident.

(8) I ESRB:s (2021) rapport *"Mitigating systemisk cyberrisk"* ([9]) beskrivs behovet av att inrätta en europeisk ram för samordning av systemiska cyberincidenter (EU-SCICF) för relevanta myndigheter i unionen. Målet för EU-SCICF skulle vara att öka de relevanta myndigheternas beredskap för att underlätta samordnade insatser vid en större cyberincident. Rapporten *"Mitigating systemisk cyberrisk"* (2021) innehåller ESRB:s bedömning av de övergripande regelverk som kan behövas för att hantera risken för att en samordning kan misslyckas.

(9) Syftet med denna rekommendation är att vidareutveckla en av de roller som de europeiska tillsynsmyndigheterna föreslås få enligt förslaget till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn ([10]) (nedan kallat *Dora*) att gradvis möjliggöra en effektiv samordnad reaktion på EU-nivå i händelse av en större gränsöverskridande incident som är relaterad till informations- och kommunikationsteknik (IKT) eller därmed sammanhängande hot som har en systempåverkan på unionens finansiella sektor som helhet. Denna process kommer att leda till att EU-SCICF inrättas för relevanta myndigheter.

([6]) Se *Internet Organised Crime Threat Assessment*, Europol, 2020, finns på Europols webbplats www.europol.europa.eu
([7]) Se *IT and cyber risk: a constant challenge*, ECB, 2021, finns på webbplatsen för ECB:s banktillsyn på www.bankingsupervision.europa.eu
([8]) Se *Systemic cyber risk*, ESRB, februari 2020, finns på ESRB:s webbplats www.esrb.europa.eu
([9]) Se *Mitigating systemic cyber risk*, ESRB, 2021, (ännu ej publicerad).
([10]) COM(2020) 595 final.

(10) EU-SCICF bör inte syfta till att ersätta befintliga ramar utan till att överbrygga eventuella luckor i samordningen och kommunikationen mellan de relevanta myndigheterna och med andra myndigheter i unionen och andra viktiga aktörer på internationell nivå. I detta avseende bör EU-SCICF:s ställning i den befintliga ramen för finanskriser och unionens ramverk för cyberincidenter klargöras. När det gäller samordningen mellan de relevanta myndigheterna bör hänsyn tas till bl.a. den roll och den verksamhet som samarbetsgruppen för nätverks- och informationssystem har för finansiella enheter enligt Europaparlamentets och rådets direktiv (EU) 2016/1148 ([11]), och de samordningsmekanismer som planeras genom inrättandet av den gemensamma cyberenheten vid sidan av Enisas deltagande.

(11) Förslaget om att inleda förberedelserna av EU-SCICF syftar särskilt till att stödja de europeiska tillsynsmyndigheternas potentiella uppgifter i linje med Dora-förslaget. Av Dora framgår att ”de europeiska tillsynsmyndigheterna får, genom den gemensamma kommittén och i samarbete med behöriga myndigheter, ECB och ESRB, inrätta mekanismer för att möjliggöra utbyte av effektiv praxis mellan olika finansiella sektorer för att öka situationsmedvetenheten och identifiera gemensamma sårbarheter och risker på it-området” och ”de får utveckla krishanterings- och beredskapsövningar som inbegriper it-attacker i syfte att utveckla kommunikationskanaler och gradvis möjliggöra en effektiv samordnad reaktion på EU-nivå i händelse av en större gränsöverskridande IKT-relaterad incident eller därmed sammanhängande hot som har en systempåverkan på unionens finansiella sektor som helhet ([12]).” Det finns ännu ingen europeisk ram som EU-SCICF men denna bör inrättas och utvecklas inom ramen för Dora.

(12) Med tanke på den risk som cyberhot utgör för den finansiella stabiliteten, bör förberedelsearbetet för det gradvisa inrättandet av EU-SCICF om möjligt inledas redan innan den rättsliga och politiska ram som krävs för dess inrättande är fullt tillämplig. Denna rättsliga och politiska ram skulle kompletteras och färdigställas när de relevanta bestämmelserna i Dora och dess delegerade akter blir tillämpliga.

(13) Effektiv kommunikation bidrar till att relevanta myndigheter får en god helhetsbild och är därför en grundförutsättning för en samordning i unionen vid större cyberincidenter. För detta ändamål bör man definiera den kommunikationsinfrastruktur som behövs för att samordna insatserna vid större cyberincidenter. Detta innebär att man specificerar vilken typ av information som behöver delas, vilka kanaler som normalt ska användas för att dela sådan information och med vilka kontakter informationen bör delas. Informationsutbytet måste ske i enlighet med gällande rättsregler. Dessutom kan en tydlig handlingsplan och de protokoll som ska följas behöva fastställas av de relevanta myndigheterna för att säkerställa en fullgod samordning mellan de myndigheter som deltar i planeringen av en samordnad reaktion på en större cyberincident.

(14) En systemisk cyberkris kommer att kräva ett fullständigt samarbete på nationell nivå och unionsnivå. Därför bör man överväga att utse kontaktpunkter för de europeiska tillsynsmyndigheterna, ECB och alla medlemsstater hos de relevanta nationella myndigheterna, vilka bör meddelas de europeiska tillsynsmyndigheterna, för att inrätta de viktigaste kontakterna i ett samordnat EU-SCICF som ska informeras om varje större cyberincident. Behovet av att utse kontaktpunkter bör bedömas under utvecklingen av EU-SCICF, med beaktande av den utsedda gemensamma kontaktpunkten enligt direktiv (EU) 2016/1148 som medlemsstaterna har inrättat för säkerhet i nätverks- och informationssystem för att säkerställa gränsöverskridande samarbete med andra medlemsstater och med samarbetsgruppen för nätverks- och informationssäkerhet ([13]).

(15) Genomförandet av krishanterings- och beredskapsövningar skulle kunna underlätta genomförandet av EU-SCICF och göra det möjligt för myndigheterna att utvärdera sin beredskap inför en systemisk cyberkris på unionsnivå. Sådana övningar skulle ge myndigheterna nya insikter och möjliggöra en kontinuerlig förbättring och utveckling av EU-SCICF.

([11]) 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).

([12]) Se artikel 43 i förslaget till Dora.

([13]) Se Europeiska kommissionen, Samarbetsgruppen för nätverks- och informationssäkerhet, finns på EU-kommissionens webbplats ec. europa.eu

(16) För utvecklingen av EU-SCICF är det viktigt att de europeiska tillsynsmyndigheterna gemensamt utför relevant förberedande arbete för att beakta de centrala delarna av ramverket och de resurser som krävs för att denna ska kunna utvecklas. Därefter skulle de europeiska tillsynsmyndigheterna kunna påbörja arbetet med en preliminär analys av eventuella hinder som skulle kunna försvåra de europeiska tillsynsmyndigheternas samt de berörda myndigheternas förmåga att inrätta EU-SCICF och ha ett relevant informationsutbyte via kommunikationskanaler i händelse av en större cyberincident. En sådan analys skulle vara ett viktigt steg för framtida eventuella ytterligare åtgärder, antingen av lagstiftningskaraktär eller andra stödjande initiativ som Europeiska kommissionen kan vidta efter genomförandet av Dora.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

AVSNITT 1

**REKOMMENDATIONER**

**Rekommendation A – Inrättande av en europeisk ram för samordning av systemiska cyberincidenter (EU-SCICF)**

1. I enlighet med kommissionens förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn (nedan kallat *Dora*) rekommenderas att de europeiska tillsynsmyndigheterna, gemensamt genom den gemensamma kommittén och tillsammans med Europeiska centralbanken (ECB), Europeiska systemrisknämnden (ESRB) och relevanta nationella myndigheter, börjar förbereda en gradvis utveckling av en effektiv samordnad reaktion på unionsnivå i händelse av en gränsöverskridande större cyberincident eller därmed sammanhängande hot som kan ha systemiska konsekvenser för unionens finanssektor. Det förberedande arbetet för samordnade reaktioner på unionsnivå bör inbegripa en gradvis utveckling av EU-SCICF för de europeiska tillsynsmyndigheterna, ECB, ESRB och relevanta nationella myndigheter. Detta bör också inkludera en bedömning av vilka resurser som behövs för en effektiv utveckling av EU-SCICF.

2. Det rekommenderas att de europeiska tillsynsmyndigheterna, mot bakgrund av delrekommendation A.1 och i samråd med ECB och ESRB, gör en kartläggning samt en konsekvensanalys av befintliga hinder, rättsliga och andra operativa hinder för en effektiv utveckling av EU-SCICF.

**Rekommendation B – Inrättande av kontaktpunkter för EU-SCICF**

Det rekommenderas att de europeiska tillsynsmyndigheterna, ECB och alla medlemsstater bland sina relevanta nationella myndigheter utser en huvudsaklig kontaktpunkt som bör meddelas de europeiska tillsynsmyndigheterna. Denna kontaktlista kommer att underlätta utvecklingen av ramverket och, när EU-SCICF har inrättats, bör dessa kontaktpunkterna och ESRB informeras om varje större cyberincident. En samordning bör också övervägas mellan EU-SCICF och den utsedda gemensamma kontaktpunkten enligt direktiv (EU) 2016/1148 som medlemsstaterna har inrättat för säkerhet i nätverks- och informationssystem för att säkerställa gränsöverskridande samarbete med andra medlemsstater och med samarbetsgruppen för nätverks- och informationssäkerhet.

**Rekommendation C – Lämpliga åtgärder på unionsnivå**

Det rekommenderas att kommissionen, utifrån resultaten av de analyser som utförts i enlighet med rekommendation A, bör överväga vilka åtgärder som behövs för att säkerställa en effektiv samordning av reaktionen vid systemiska cyberincidenter.

AVSNITT 2

**GENOMFÖRANDE**

1. **Definitioner**

I denna rekommendation gäller följande definitioner:

a) *cyber*: avser interaktion mellan personer, processer, data och informationssystem inom eller genom sammankopplad informationsinfrastruktur ([14]).

([14]) Se *Cyber Lexicon*, FSB, 12 november 2018, finns på FSB:s webbplats www.fsb.org

b) *större cyberincident*: en IKT-relaterad incident med potentiellt stor negativ inverkan på nätverks- och informationssystem som stöder de finansiella enheternas kritiska funktioner ([15]).

c) *systemisk cyberkris*: en större cyberincident som orsakar en nivå av störningar i unionens finansiella system som kan få allvarliga negativa konsekvenser för en väl fungerande inre marknad och för realekonomins funktion. En sådan kris kan uppstå till följd av en större cyberincident som orsakar chocker i flera kanaler, t.ex. operativa, förtroendeskapande och finansiella.

d) *europeiska tillsynsmyndigheter (ESA)*: den europeiska tillsynsmyndigheten (Europeiska bankmyndigheten) som inrättats genom Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([16]), tillsammans med den europeiska tillsynsmyndigheten (Europeiska försäkrings- och tjänstepensionsmyndigheten) som inrättats genom Europaparlamentets och rådets förordning (EU) nr 1094/2010 ([17]) och europeiska tillsynsmyndigheten (Europeiska värdepappers- och marknadsmyndigheten) som inrättats genom Europaparlamentets och rådets förordning (EU) nr 1095/2010 ([18]).

e) *gemensamma kommitté*: den gemensamma kommitté för de europeiska tillsynsmyndigheterna som inrättas genom artikel 54 i förordning (EU) nr 1093/2010, förordning (EU) nr 1094/2010 och förordning (EU) nr 1095/2010.

f) *relevant nationell myndighet*:

1. en behörig myndighet eller tillsynsmyndighet i en medlemsstat i enlighet med de unionsakter som avses i artikel 1.2 i förordning (EU) nr 1093/2010, i förordning (EU) nr 1094/2010 och i förordning (EU) nr 1095/2010 och varje annan nationell behörig myndighet i enlighet med de unionsakter som tilldelar de europeiska tillsynsmyndigheterna uppgifter.

2. en behörig myndighet i en medlemsstat som har utsetts i enlighet med

i. artikel 4 i Europaparlamentets och rådets direktiv 2013/36/EU ([19]), utan att det påverkar de särskilda uppgifter som ECB tilldelas genom rådets förordning (EU) nr 1024/2013 ([20]).

ii. artikel 22 i Europaparlamentets och rådets direktiv (EU) 2015/2366 ([21]).

iii. artikel 37 i Europaparlamentets och rådets direktiv 2009/110/EG ([22]).

iv. artikel 4 i Europaparlamentets och rådets direktiv (EU) 2019/2034 ([23]).

([15]) Se artikel 3.7 i förslaget till Dora.

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

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

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

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

([20]) 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).

([21]) 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).

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

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

v. artikel 3.1 ee första ledet i förslag till Europaparlamentets och rådets förordning om marknader för kryptotillgångar och om ändring av direktiv (EU) 2019/1937 ([24]).

vi. artikel 11 i Europaparlamentets och rådets förordning (EU) 909/2014 ([25]).

vii. artikel 22 i Europaparlamentets och rådets förordning (EU) 648/2012 ([26]).

viii. artikel 67 i Europaparlamentets och rådets direktiv 2014/65/EU ([27]).

ix. artikel 22 i förordning (EU) nr 648/2012.

x. artikel 44 i Europaparlamentets och rådets direktiv 2011/61/EU ([28]).

xi. artikel 97 i Europaparlamentets och rådets direktiv 2009/65/EG ([29]).

xii. artikel 30 i Europaparlamentets och rådets direktiv 2009/138/EG ([30]).

xiii. artikel 12 i Europaparlamentets och rådets direktiv (EU) 2016/97 ([31]).

xiv. artikel 47 i Europaparlamentets och rådets direktiv (EU) 2016/2341 ([32]).

xv. artikel 22 i Europaparlamentets och rådets förordning (EG) 1060/2009 ([33]).

xvi. artikel 3.2 och artikel 32 i Europaparlamentets och rådets direktiv 2006/43/EG ([34]).

xvii. artikel 40 i Europaparlamentets och rådets förordning (EU) 2016/1011 ([35]).

xviii. artikel 29 i Europaparlamentets och rådets förordning (EU) 2020/1503 ([36]).

([24]) COM(2020) 593 final.

([25]) 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).

([26]) 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).

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

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

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

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

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

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

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

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

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

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

3. en myndighet som är behörig att anta och/eller aktivera makrotillsynsåtgärder eller utföra andra uppgifter avseende finansiell stabilitet, t.ex. tillhörande analysarbete, inklusive men inte begränsat till:

   i. en utsedd myndighet i enlighet med avdelning VII kapitel 4 i direktiv 2013/36/EU eller artikel 458.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 ([37]),

   ii. ett makrotillsynsorgan med de mål, arrangemang, uppgifter, befogenheter, instrument, ansvar och andra särdrag som fastställs i Europeiska systemrisknämndens rekommendation ESRB/2011/3 ([38]).

g) *relevant myndighet*:

   1. en europeisk tillsynsmyndighet.

   2. ECB för de uppgifter som tilldelats ECB i enlighet med artiklarna 4.1, 4.2 och 5.2 i förordning (EU) nr 1024/2013.

   3. en relevant nationell myndighet.

## 2. **Kriterier för genomförandet**

Följande kriterier gäller för genomförandet av denna rekommendation:

a) Principen om behovsenlig behörighet och proportionalitetsprincipen ska beaktas så att man beaktar målsättningen och innehållet i varje rekommendation.

b) De särskilda efterlevnadskriterier avseende varje rekommendation som anges i bilagan bör uppfyllas.

## 3. **Tidsfrister för uppföljning**

I enlighet med artikel 17.1 i förordning (EU) nr 1092/2010 ska mottagarna underrätta Europaparlamentet, rådet, kommissionen och ESRB om vilka åtgärder som vidtagits med anledning av rekommendationen och motivera eventuell passivitet. Mottagarna uppmanas att inkomma med denna information i enlighet med följande tidsfrister:

1. Rekommendation A

   a) Senast den 30 juni 2023, dock tidigast sex månader efter det att Dora trätt i kraft, ska de europeiska tillsynsmyndigheterna överlämna en interimsrapport om genomförandet av delrekommendation A.1 till Europaparlamentet, rådet, kommissionen och ESRB.

   b) Senast den 30 juni 2024, dock tidigast arton månader efter det att Dora trätt i kraft, ska de europeiska tillsynsmyndigheterna överlämna en slutrapport om genomförandet av delrekommendation A.1 till Europaparlamentet, rådet, kommissionen och ESRB.

   c) Senast den 30 juni 2025, dock tidigast trettio månader efter det att Dora trätt i kraft, ska de europeiska tillsynsmyndigheterna överlämna en rapport om genomförandet av delrekommendation A.2 till Europaparlamentet, rådet, kommissionen och ESRB.

2. Rekommendation B

   Senast den 30 juni 2023, dock tidigast sex månader efter det att Dora trätt i kraft, ska de europeiska tillsynsmyndigheterna, ECB och medlemsstaterna överlämna en rapport om genomförandet av rekommendation B till Europaparlamentet, rådet, kommissionen och ESRB.

3. Rekommendation C

   a) Senast den 31 december 2023, dock tidigast tolv månader efter det att Dora trätt i kraft, ska kommissionen överlämna en rapport om genomförandet av rekommendation C till Europaparlamentet, rådet och ESRB mot bakgrund av interimsrapporten från de europeiska tillsynsmyndigheterna i enlighet med delrekommendation A.1.

([37]) 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).

([38]) Europeiska systemrisknämndens rekommendation ESRB/2011/3 av den 22 december 2011 om de nationella myndigheternas mandat för makrotillsyn (EUT C 41, 14.2.2012, s. 1).

b) Senast den 31 december 2025, dock tidigast trettiosex månader efter det att Dora trätt i kraft, ska kommissionen överlämna en rapport om genomförandet av rekommendation C till Europaparlamentet, rådet och ESRB mot bakgrund av rapporten från de europeiska tillsynsmyndigheterna i enlighet med rekommendation A.

4. **Granskning och utvärdering**

1. ESRB-sekretariatet kommer att

a) stödja adressaterna, säkerställa en samordnad rapportering, tillhandahållandet av relevanta förlagor och information om tillvägagångssätt och tidsfrister för uppföljningen,

b) verifiera adressaternas uppföljning, hjälpa adressaterna när dessa så önskar och lämna rapporter om uppföljningen till styrelsen. Utvärderingarna kommer att initieras enligt följande:

i) Inom 12 månader efter ikraftträdandet av Dora, när det gäller genomförandet av rekommendationerna A och B.

ii) Inom 18 månader efter ikraftträdandet av Dora, när det gäller genomförandet av rekommendation C.

iii) Inom 24 månader efter ikraftträdandet av Dora, när det gäller genomförandet av rekommendation A.

iv) Inom 36 månader efter ikraftträdandet av Dora, när det gäller genomförandet av rekommendation A.

v) Inom 42 månader efter ikraftträdandet av Dora, när det gäller genomförandet av rekommendation C.

2. Styrelsen kommer att bedöma adressaternas åtgärder och förklaringar och i förekommande fall besluta huruvida denna rekommendation inte har efterlevts och huruvida en adressat har underlåtit att motivera sin passivitet på lämpligt sätt.

Utfärdad i Frankfurt am Main den 2 december 2021.

*På ESRB-styrelsens vägnar*
Francesco MAZZAFERRO
*Chef för ESRB:s sekretariat*

*BILAGA*

**SPECIFICERING AV DE KRITERIER SOM SKA UPPFYLLAS FÖR REKOMMENDATIONERNA**

**Rekommendation A – Inrättande av en europeisk ram för samordning av systemiska cyberincidenter (EU-SCICF)**

För delrekommendation A.1 ska nedanstående kriterier uppfyllas.

1. När de förbereder en effektiv samordnad reaktion på unionsnivå som bör inbegripa en gradvis utveckling av EU-SCICF genom att utöva den befogenhet som avses i Europaparlamentets och rådets framtida förordning om digital operativ motståndskraft för finanssektorn (nedan kallad Dora) bör de europeiska tillsynsmyndigheterna, genom den gemensamma kommittén och tillsammans med Europeiska centralbanken (ECB), Europeiska systemrisknämnden (ESRB) och relevanta nationella myndigheter, i samråd med Europeiska unionens byrå för nät- och informationssäkerhet och kommissionen när så anses nödvändigt, överväga att i den planerade förberedelsen för EU och SCICF inkludera åtminstone följande aspekter:

   a. En analys av resursbehoven för en effektiv utveckling av EU-SCICF.

   b. Utveckling av krishanterings- och beredskapsövningar som inbegriper cyberattackscenarier i syfte att utveckla kommunikationskanaler.

   c. Ta fram en gemensam vokabulär.

   d. Utveckla en enhetlig klassificering av cyberincidenter.

   e. Inrätta säkra och tillförlitliga kanaler för informationsutbyte, inbegripet reservsystem.

   f. Inrätta kontaktpunkter.

   g. Granska konfidentialitetsaspekten vid informationsutbyte.

   h. Utveckla initiativ för samarbete och informationsutbyte med finanssektorn om cyberincidenter.

   i. Ta fram effektiva aktiverings- och eskaleringsprocesser genom en god helhetsbild.

   j. Förtydliga vilket ansvar olika deltagare i ramverket har.

   k. Utveckla gränssnitt för sektorsövergripande samordning och, i förekommande fall, samordning med tredjeländer.

   l. Säkerställa att relevanta myndigheter kommunicerar med allmänheten på ett enhetligt sätt för att upprätthålla förtroendet.

   m. Skapa fördefinierade kommunikationsvägar för snabb kommunikation.

   n. Genomföra lämpliga tester inom ramverket, inbegripet tester mellan olika jurisdiktioner och samordning med tredjeländer, och göra utvärderingar av erfarenheterna med målet att vidareutveckla ramverket.

   o. Säkerställa effektiv kommunikation och motåtgärder mot desinformation.

**Rekommendation B – Inrättande av kontaktpunkter för EU-SCICF**

För rekommendation B ska nedanstående kriterier uppfyllas.

1. De europeiska tillsynsmyndigheterna, ECB och alla medlemsstaterna (bland sina relevanta nationella myndigheter) bör enas om en gemensam strategi för att dela och uppdatera förteckningen över utsedda kontaktpunkter för EU-SCICF.

2. När man utser kontaktpunkter bör man beakta den utsedda gemensamma kontaktpunkten enligt direktiv (EU) 2016/1148 som medlemsstaterna har inrättat avseende säkerhet i nätverks- och informationssystem för att säkerställa gränsöverskridande samarbete med andra medlemsstater och med samarbetsgruppen för nätverks- och informationssäkerhet.

**Rekommendation C – Ändringar av unionens rättsliga ram**

För rekommendation C ska nedanstående kriterium uppfyllas.

Kommissionen bör överväga om det behövs några åtgärder, inbegripet ändringar av relevant unionslagstiftning, till följd av den analys som utförts i enlighet med rekommendation A för att säkerställa att de europeiska tillsynsmyndigheterna, genom den gemensamma kommittén och tillsammans med ECB, ESRB och relevanta nationella myndigheter, kan utveckla EU-SCICF i enlighet med delrekommendation A.1 och för att säkerställa att de europeiska tillsynsmyndigheterna, ECB, ESRB och relevanta nationella myndigheter, samt andra myndigheter, kan delta i samordningsåtgärder och informationsutbyte som är tillräckligt detaljerade och konsekventa för att stödja en effektiv EU-SCICF.