I

(Resoluties, aanbevelingen en adviezen)

AANBEVELINGEN

EUROPEES COMITÉ VOOR SYSTEEMRISICO'S

AANBEVELING VAN HET EUROPEES COMITÉ VOOR SYSTEEMRISICO'S

van 2 december 2021

inzake een pan-Europees coördinatiekader voor de betrokken autoriteiten met betrekking tot systemische cyberincidenten

(ESRB/2021/17)

(2022/C 134/01)

DE ALGEMENE RAAD VAN HET EUROPEES COMITÉ VOOR SYSTEEMRISICO'S,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien de Overeenkomst betreffende de Europese Economische Ruimte ([1]), en met name bijlage IX,

Gezien Verordening (EU) nr. 1092/2010 van het Europees Parlement en de Raad van 24 november 2010 betreffende macroprudentieel toezicht van de Europese Unie op het financiële stelsel en tot oprichting van een Europees Comité voor systeemrisico's ([2]), en met name artikel 3, lid 2, punten b) en d), en de artikelen 16 en 18,

Gezien Besluit ESRB/2011/1 van het Europees Comité voor systeemrisico's van 20 januari 2011 tot vaststelling van het reglement van orde van het Europees Comité voor systeemrisico's ([3]), en met name de artikelen 18 tot en met 20,

Overwegende hetgeen volgt:

(1) Zoals opgemerkt in overweging 4 van Aanbeveling ESRB/2013/1 van het Europees Comité voor systeemrisico's ([4]), is de uiteindelijke doelstelling van macroprudentieel beleid bij te dragen tot het waarborgen van de stabiliteit van het financiële stelsel als geheel, met inbegrip van het versterken van de schokbestendigheid van het financiële stelsel en het verminderen van de opbouw van systeemrisico's, en daarbij een duurzame bijdrage te verzekeren aan economische groei. Het Europees Comité voor systeemrisico's (ESRB) is verantwoordelijk voor het macroprudentieel toezicht op het financiële stelsel in de Unie. Bij het vervullen van zijn mandaat dient het ESRB bij te dragen aan het voorkomen en beperken van systeemrisico's voor de financiële stabiliteit, met inbegrip van de risico's in verband met cyberincidenten, en aanbevelingen te doen voor risicobeperking.

(2) Ernstige cyberincidenten kunnen een systeemrisico voor het financiële stelsel opleveren, gelet op hun vermogen kritieke financiële diensten en operaties te verstoren. De versterking van een initiële schok kan, hetzij door een operationele of financiële besmetting, hetzij door een uitholling van het vertrouwen in het financiële stelsel geschieden. Indien het financiële stelsel niet in staat is deze schokken op te vangen, komt de financiële stabiliteit in gevaar en kan deze situatie leiden tot een systemische cybercrisis ([5]).

([1]) PB L 1 van 3.1.1994, blz. 3.
([2]) PB L 331 van 15.12.2010, blz. 1.
([3]) PB C 58 van 24.2.2011, blz. 4.
([4]) Aanbeveling ESRB/2013/1 van het Europees Comité voor systeemrisico's van 4 april 2013 inzake tussentijdse doelstellingen en instrumenten van macroprudentieel beleid (PB C 170 van 15.6.2013, blz. 1).
([5]) Zie "Systemic cyber risk", ESRB, februari 2020, beschikbaar op de website van het ESRB onder: www.esrb.europa.eu

(3) Het voortdurend evoluerende cyberdreigingslandschap en de recente stijging van ernstige cyberincidenten zijn indicatoren voor een groter risico voor de financiële stabiliteit in de Unie. De COVID-19-pandemie heeft het belang van de rol die technologie speelt voor de werking van het financiële stelsel benadrukt. Betrokken autoriteiten en instellingen moesten hun technische infrastructuur en risicobeheersingskaders aanpassen aan een plotselinge toename van werken op afstand, waardoor de algemene blootstelling van het financiële stelsel aan cyberdreigingen is toegenomen en criminelen de mogelijkheid hadden, zowel nieuwe modi operandi te ontwikkelen, als bestaande modi operandi aan te passen om misbruik te maken van de situatie ([6]). Tegen deze achtergrond is het aantal aan het ECB-Bankentoezicht gemelde cyberincidenten in 2020 met 54 % gestegen ten opzichte van 2019 ([7]).

(4) De potentiële grootschaligheid, snelheid en mate van verspreiding van een ernstig cyberincident vereisen een doeltreffende reactie van de betrokken autoriteiten om de mogelijke negatieve gevolgen voor de financiële stabiliteit te beperken. Snelle coördinatie en communicatie tussen de betrokken autoriteiten op Unieniveau kunnen helpen de impact van een ernstig cyberincident voor de financiële stabiliteit vroegtijdig te beoordelen, het vertrouwen in het financiële stelsel te bewaren en de besmetting naar andere financiële instellingen te beperken, en zo te helpen voorkomen dat een ernstig cyberincident een risico vormt voor de financiële stabiliteit.

(5) De onderliggende schok ontstaat op nieuwe wijze in vergelijking met de traditionele financierings- en liquiditeitscrises waarmee de betrokken autoriteiten gebruikelijk geconfronteerd worden. Afgezien van de financiële aspecten, moet de algehele risicobeoordeling de schaal en impact van operationele verstoringen omvatten, omdat zij de keuze van de macroprudentiële instrumenten kunnen beïnvloeden. Evenzo kan de financiële stabiliteit eveneens van invloed zijn op de keuze van operationele matigingen door cyberexperten. Dit vraagt om nauwe en snelle coördinatie en open communicatie om onder andere het situationeel bewustzijn te versterken.

(6) Het risico van een coördinatiefalen door autoriteiten bestaat en moet worden aangepakt. De betrokken autoriteiten in de Unie moeten onderling en met andere autoriteiten, zoals het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), waarmee zij gewoonlijk geen interacties hebben, coördineren. Aangezien een aanzienlijk aantal financiële instellingen van de Unie wereldwijd actief is, zal een ernstig cyberincident waarschijnlijk niet tot de Unie beperkt blijven of buiten de Unie kunnen worden geïnitieerd en kan het nodig zijn om de respons wereldwijd te coördineren.

(7) De betrokken autoriteiten moeten voorbereid zijn op deze interacties. Anders dreigen zij inconsistente maatregelen te treffen die in tegenspraak zijn met de reacties van andere autoriteiten of deze in gevaar brengen. Een dergelijk coördinatiefalen zou de schok voor het financiële stelsel kunnen versterken door te leiden tot een uitholling van het vertrouwen in de werking van het financiële stelsel, hetgeen in het ergste geval een risico voor de financiële stabiliteit zou vormen ([8]). Bijgevolg moeten de nodige stappen worden ondernomen om het risico voor de financiële stabiliteit als gevolg van een coördinatiefalen in geval van een ernstig cyberincident aan te pakken.

(8) In het ESRB-rapport "Mitigating systemic cyber risk" (2021) ([9]) wordt de noodzaak vastgesteld voor het vaststellen van een pan-Europees kader voor de coördinatie van systemische cyberincidenten (*pan-European systemic cyber incident coordination framework* – EU-SCICF) voor de betrokken autoriteiten in de Unie. De doelstelling van het EU-SCICF zou zijn om de mate van bereidheid van de betrokken autoriteiten te vergroten voor het faciliteren van een gecoördineerde reactie op een potentieel ernstig cyberincident. Het ESRB-rapport "Mitigating systemic cyber risk" (2021) presenteert de beoordeling van het ESRB van de kaderkenmerken die op het eerste gezicht nodig zouden zijn om het risico van een coördinatiefalen aan te pakken.

(9) Het hoofddoel van deze aanbeveling is om voort te bouwen op één van de beoogde rollen van de Europese toezichthoudende autoriteiten (ETA's) in het kader van het voorstel voor een verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector ([10]) (hierna "DORA" genoemd), namelijk een doeltreffende gecoördineerde respons op EU-niveau mogelijk te maken in het geval van een ernstig grensoverschrijdend ICT-gerelateerd incident of een gerelateerde dreiging met een systemisch effect op de financiële sector van de Unie in zijn geheel. Dit proces zal leiden tot de vaststelling van het EU-SCICF voor de betrokken autoriteiten.

([6]) Zie "Internet Organised Crime Threat Assessment", Europol, 2020, beschikbaar op de website van Europol onder www.europol.europa.eu

([7]) Zie "IT and cyber risk: a constant challenge", ECB, 2021, beschikbaar op de ECB-Bankentoezicht website onder: www.bankingsupervision.europa.eu

([8]) Zie "Systemic cyber risk", ESRB, februari 2020, beschikbaar op de website van het ESRB op www.esrb.europa.eu

([9]) Zie "Mitigating systemic cyber risk", ESRB, 2021, (verschijnt binnenkort).

([10]) COM/2020/595 final.

(10) Het EU-SCICF mag niet gericht zijn op de vervanging van bestaande kaders, maar op het overbruggen van eventuele coördinatie- en communicatiekloven tussen de betrokken autoriteiten onderling en met andere autoriteiten in de Unie en andere belangrijke actoren op internationaal niveau. In dit verband moet rekening worden gehouden met de positionering van het EU-SCICF binnen het landschap met het bestaande kader voor financiële crises en het Uniekader voor cyberincidenten. Wat de coördinatie tussen de betrokken autoriteiten onderling betreft, moet rekening worden gehouden met onder andere de rollen en activiteiten van de samenwerkingsgroep voor netwerk- en informatiesystemen (NIS) voor financiële entiteiten uit hoofde van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([11]), en de met de coördinatiemechanismen die in het kader van de oprichting van de gezamenlijke cybereenheid worden overwogen, naast de betrokkenheid van Enisa.

(11) Het voorstel om een begin te maken met de voorbereiding van het EU-SCICF heeft met name tot doel de mogelijke rollen van de ETA's te bevestigen, zoals beoogd in het DORA-voorstel. In DORA wordt het volgende voorgesteld: "de ETA's, kunnen via het Gemengd Comité en in samenwerking met de bevoegde autoriteiten, de Europese Centrale Bank (ECB) en het ESRB, mechanismen vaststellen met het oog op het verbeteren van de situatiekennis en de aanwijzing van gemeenschappelijke cyberkwetsbaarheden en sectoroverschrijdende risico's", en: "zij kunnen crisisbeheer- en noodoefeningen met cyberaanvalscenario's ontwikkelen om communicatiekanalen te ontwikkelen en geleidelijk een doeltreffende gecoördineerde respons op EU-niveau mogelijk te maken in geval van een groot grensoverschrijdend ICT-gerelateerd incident of een daarmee samenhangende dreiging die een systemische impact heeft op de financiële sector van de Unie als geheel" ([12]). Een pan-Europees kader zoals het EU-SCICF bestaat nog niet en moet in het kader van DORA worden vastgesteld en ontwikkeld.

(12) Gezien het risico dat cyberrisico's voor de financiële stabiliteit in de Unie kunnen vormen, moeten de voorbereidende werkzaamheden voor de geleidelijke vaststelling van het EU-SCICF, voor zover haalbaar, van start gaan zelfs voordat het voor de vaststelling vereiste juridische en beleidskader voor de vaststelling ervan volledig van toepassing is. Dit juridische en beleidskader zou volledig worden opgezet en voltooid zodra de desbetreffende bepalingen van DORA en de bijbehorende gedelegeerde handelingen van toepassing worden.

(13) Doeltreffende communicatie draagt bij tot het situationeel bewustzijn onder de betrokken autoriteiten en is dus een onontbeerlijke voorwaarde voor coördinatie in de gehele Unie bij ernstige cyberincidenten. In dit verband is het nodig om de communicatie-infrastructuur te definiëren die nodig is om een respons op een ernstig cyberincident te coördineren. Dit houdt in dat moet worden vastgesteld welke soort informatie moet worden gedeeld, welke reguliere kanalen moeten worden gebruikt om dergelijke informatie te delen en met welke contactpunten informatie moet worden gedeeld. Bij de informatie-uitwisseling moeten de bestaande wettelijke voorschriften in acht worden genomen. Daarnaast moeten mogelijkerwijs een duidelijk actieplan en de te volgen protocollen worden vastgesteld door de betrokken autoriteiten om te zorgen voor een goede coördinatie tussen de autoriteiten die betrokken zijn bij de planning van een gecoördineerde reactie op een ernstig cyberincident.

(14) Een systemische cybercrisis vereist dat er volledige samenwerking op nationaal en Unieniveau tot stand wordt gebracht. Bijgevolg kunnen de aangewezen contactpunten voor de ETA's, de ECB en de betrokken nationale autoriteiten van elke lidstaat uit het midden van de bevoegde nationale autoriteiten worden aangewezen en aan de ETA's worden meegedeeld, teneinde de belangrijkste gesprekspartners in de coördinatieregeling van het EU-SCICF vast te stellen die moeten worden geïnformeerd in geval van een ernstig cyberincident. De noodzaak om contactpunten aan te wijzen moet worden beoordeeld tijdens de ontwikkeling van het EU-SCICF, rekening houdend met het aangewezen centrale contactpunt uit hoofde van Richtlijn (EU) 2016/1148 dat de lidstaten hebben ingesteld met betrekking tot de beveiliging van netwerk- en informatiesystemen om grensoverschrijdende samenwerking met andere lidstaten en de NIS-samenwerkingsgroep te waarborgen ([13]).

(15) Het uitvoeren van nood- en crisisbeheersingsoefeningen kan de tenuitvoerlegging van het EU-SCICF vergemakkelijken en de autoriteiten in staat stellen hun gereedheid en paraatheid voor een systemische cybercrisis op Unieniveau te evalueren. Autoriteiten zouden lering kunnen trekken uit dergelijke oefeningen, die eveneens een voortdurende verbetering en ontwikkeling van het EU-SCICF mogelijk maken.

([11]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).
([12]) Zie ontwerpartikel 43 van het voorstel voor DORA.
([13]) Zie Europese Commissie, NIS Cooperation Group, beschikbaar op de website van de Europese Commissie op www.ec.europa.eu

(16) Voor de ontwikkeling van het EU-SCICF is het van essentieel belang dat de ETA's gezamenlijk relevante voorbereidende werkzaamheden verrichten om rekening te houden met de mogelijke essentiële elementen van het kader en de vereiste middelen en behoeften die voor de verdere ontwikkeling ervan noodzakelijk zijn. Daarna zouden de ETA's kunnen beginnen met het uitvoeren van een voorlopige analyse van eventuele belemmeringen die de ETA's en de betrokken autoriteiten zouden kunnen beletten om het EU-SCICF op te richten en relevante informatie via communicatiekanalen te delen in geval van een ernstig cyberincident. Een dergelijke analyse zou een belangrijke stap zijn in de richting van verdere maatregelen, hetzij van wetgevende aard, hetzij via andere ondersteunende initiatieven die de Europese Commissie in de uitvoeringsfase na DORA kan nemen,

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

AFDELING 1

AANBEVELINGEN

Aanbeveling A – Vaststelling van een pan-Europees coördinatiekader voor systemische cyberincidenten (EU-SCICF)

1. Aanbevolen wordt dat, zoals beoogd in het voorstel van de Commissie voor een verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector (hierna "DORA" genoemd), de Europese toezichthoudende autoriteiten (ETA's) gezamenlijk via het Gemengd Comité en samen met de Europese Centrale Bank (ECB), het Europees Comité voor systeemrisico's (ESRB) en de betrokken nationale autoriteiten voorbereidingen treffen voor de geleidelijke ontwikkeling van een doeltreffende gecoördineerde reactie op Unieniveau in het geval van een grensoverschrijdend ernstig cyberincident of een daarmee samenhangende dreiging die een systemische impact kan hebben op de financiële sector van de Unie. Voorbereidende werkzaamheden voor een gecoördineerde reactie op Unieniveau moeten een geleidelijke ontwikkeling van het EU-SCICF inhouden voor ETA's, de ECB, het ESRB en de betrokken nationale autoriteiten. Dit moet ook een beoordeling omvatten van de middelen die nodig zijn voor de doeltreffende ontwikkeling van het EU-SCICF.

2. In het kader van subaanbeveling A(1) wordt het aanbevolen dat de ETA's, in overleg met de ECB en het ESRB, een inventarisatie maken en een daaropvolgende analyse uitvoeren van de huidige belemmeringen en juridische en andere operationele barrières voor de effectieve ontwikkeling van het EU-SCICF.

Aanbeveling B – Vaststelling van contactpunten van het EU-SCICF

Aanbevolen wordt dat de ETA's, de ECB en de betrokken nationale autoriteiten van elke lidstaat een eerste contactpunt aanwijzen dat aan de ETA's moet worden meegedeeld. Deze contactlijst zal de ontwikkeling van het kader vergemakkelijken en zodra het EU-SCICF is ingesteld, moeten de contactpunten en het ESRB worden geïnformeerd in het geval van een ernstig cyberincident. Er moet ook worden voorzien in een coördinatie tussen het EU-SCICF en het centraal contactpunt dat de lidstaten krachtens Richtlijn (EU) 2016/1148 hebben aangewezen voor de beveiliging van netwerk- en informatiesystemen met het oog op grensoverschrijdende samenwerking met andere lidstaten en met de samenwerkingsgroep voor netwerk- en informatiesystemen.

Aanbeveling C – Passende maatregelen op Unieniveau

Aanbevolen wordt dat, op basis van het resultaat van de overeenkomstig aanbeveling A uitgevoerde analyses, de Commissie passende maatregelen bestudeert die nodig zijn voor het waarborgen van een effectieve coördinatie van reacties op systemische cyberincidenten.

AFDELING 2

TENUITVOERLEGGING

1. **Definities**

Voor de toepassing van deze aanbeveling gelden de volgende definities:

a) "cyber": betrekking hebbend op, binnen of via het medium van de onderling gekoppelde informatie-infrastructuur van interacties tussen personen, processen, gegevens en informatiesystemen ([14]);

([14]) Zie Cyber Lexicon, FSB, 12 november 2018, beschikbaar op de FSB website op www.fsb.org

b) "ernstig cyberincident": een ICT-gerelateerd incident dat mogelijk ernstige negatieve gevolgen kan hebben voor de netwerk- en informatiesystemen die kritieke functies van financiële entiteiten ondersteunen ([15]);

c) "systemische cybercrisis": een ernstig cyberincident dat een mate van verstoring van het financiële stelsel in de Unie veroorzaakt met mogelijk ernstige negatieve gevolgen voor de goede werking van de interne markt en de functionering van de reële economie. Een dergelijke crisis kan het gevolg zijn van een ernstig cyberincident dat schokken in een aantal kanalen veroorzaakt, met inbegrip van operationele, vertrouwelijke en financiële kanalen;

d) "Europese toezichthoudende autoriteiten" of "ETA's": de krachtens Verordening (EU) nr.1093/2010 van het Europees Parlement en de Raad opgerichte Europese toezichthoudende autoriteit (Europese Bankautoriteit) ([16]), samen met de krachtens Verordening (EU) nr.1094/2010 van het Europees Parlement en de Raad ([17]) opgerichte Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen) en de krachtens Verordening (EU) nr.1095/2010 van het Europees Parlement en de Raad ([18]) opgerichte Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten);

e) "Gemengd Comité": het Gemengd Comité van de Europese toezichthoudende autoriteiten, opgericht krachtens artikel 54 van Verordening (EU) nr. 1093/2010, Verordening (EU) nr. 1094/2010 en Verordening (EU) nr. 1095/2010;

f) "betrokken nationale autoriteit":

1. een bevoegde of toezichthoudende autoriteit in een lidstaat als bedoeld in de handelingen van de Unie genoemd in artikel 1, lid 2, van Verordening (EU) nr. 1093/2010, Verordening (EU) nr. 1094/2010 en Verordening (EU) nr. 1095/2010 en elke andere bevoegde nationale autoriteit als bedoeld in de handelingen van de Unie die taken opdragen aan de ETA's;

2. een bevoegde autoriteit in een lidstaat die is aangewezen uit hoofde van:

i. artikel 4 van Richtlijn 2013/36/EU van het Europees Parlement en de Raad ([19]), onverlet de specifieke taken die aan de ECB zijn opgedragen uit hoofde van Verordening (EU) nr. 1024/2013 ([20]);

ii. artikel 22 van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad ([21]);

iii. artikel 37 van Richtlijn 2009/110/EG van het Europees Parlement en de Raad ([22]);

iv. artikel 4 van Richtlijn (EU) 2019/2034 van het Europees Parlement en de Raad ([23]);

([15]) Zie ontwerpartikel 3, punt 7, van het voorstel voor DORA.

([16]) Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12).

([17]) Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie (PB L 331 van 15.12.2010, blz. 48).

([18]) Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie (PB L 331 van 15.12.2010, blz. 84).

([19]) Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (PB L 176 van 27.6.2013, blz. 338).

([20]) Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen (PB L 287 van 29.10.2013, blz. 63).

([21]) Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35).

([22]) Richtlijn 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (PB L 267 van 10.10.2009, blz. 7).

([23]) Richtlijn (EU) 2019/2034 van het Europees Parlement en de Raad van 27 november 2019 betreffende het prudentiële toezicht op beleggingsondernemingen en tot wijziging van Richtlijnen 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU en 2014/65/EU (PB L 314 van 5.12.2019, blz. 64).

v. artikel 3, lid 1, punt ee) , eerste streepje, van het voorstel voor een verordening van het Europees Parlement en de Raad betreffende markten in cryptoactiva en tot wijziging van Richtlijn (EU) 2019/1937 ([24]);

vi. artikel 11 van Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad ([25]);

vii. artikel 22 van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad ([26]);

viii. artikel 67 van Richtlijn 2014/65/EU van het Europees Parlement en de Raad ([27]);

ix. artikel 22 van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad;

x. artikel 44 van Richtlijn 2011/61/EU van het Europees Parlement en de Raad ([28]);

xi. artikel 97 van Richtlijn 2009/65/EG van het Europees Parlement en de Raad ([29]);

xii. artikel 30 van Richtlijn 2009/138/EG van het Europees Parlement en de Raad ([30]);

xiii. artikel 12 van Richtlijn (EU) 2016/97 van het Europees Parlement en de Raad ([31]);

xiv. artikel 47 van Richtlijn (EU) 2016/2341 van het Europees Parlement en de Raad ([32]);

xv. artikel 22 van Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad ([33]);

xvi. artikel 3, lid 2, en artikel 32 van Richtlijn 2006/43/EG van het Europees Parlement en de Raad ([34]);

xvii. artikel 40 van Verordening (EU) nr. 2016/1011 van het Europees Parlement en de Raad ([35]);

xviii. artikel 29 van Verordening (EU) 2020/1503 van het Europees Parlement en de Raad ([36]);

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

([25]) Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012 (PB L 257 van 28.8.2014, blz. 1).

([26]) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 201 van 27.7.2012, blz. 1).

([27]) Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (PB L 173 van 12.6.2014, blz. 349).

([28]) Richtlijn 2011/61/EU van het Europees Parlement en de Raad van 8 juni 2011 inzake beheerders van alternatieve beleggingsinstellingen en tot wijziging van de Richtlijnen 2003/41/EG en 2009/65/EG en van de Verordeningen (EG) nr. 1060/2009 en (EU) nr. 1095/2010 (PB L 174 van 1.7.2011, blz. 1).

([29]) Richtlijn 2009/65/EG van het Europees Parlement en de Raad van 13 juli 2009 tot coördinatie van de wettelijke en bestuursrechtelijke bepalingen betreffende bepaalde instellingen voor collectieve belegging in effecten (icbe's) (PB L 302 van 17.11.2009, blz. 32).

([30]) Richtlijn 2009/138/EG van het Europees Parlement en de Raad van 25 november 2009 betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (PB L 335 van 17.12.2009, blz. 1).

([31]) Richtlijn (EU) 2016/97 van het Europees Parlement en de Raad van 20 januari 2016 betreffende verzekeringsdistributie (PB L 26 van 2.2.2016, blz. 19).

([32]) Richtlijn (EU) 2016/2341 van het Europees Parlement en de Raad van 14 december 2016 betreffende de werkzaamheden van en het toezicht op instellingen voor bedrijfspensioenvoorziening (IBPV's) (PB L 354 van 23.12.2016, blz. 37).

([33]) Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad van 16 september 2009 inzake ratingbureaus (PB L 302 van 17.11.2009, blz. 1).

([34]) Richtlijn 2006/43/EG van het Europees Parlement en de Raad van 17 mei 2006 betreffende de wettelijke controles van jaarrekeningen en geconsolideerde jaarrekeningen, tot wijziging van de Richtlijnen 78/660/EEG en 83/349/EEG van de Raad en houdende intrekking van Richtlijn 84/253/EEG van de Raad (PB L 157 van 9.6.2006, blz. 87).

([35]) Verordening (EU) 2016/1011 van het Europees Parlement en de Raad van 8 juni 2016 betreffende indices die worden gebruikt als benchmarks voor financiële instrumenten en financiële overeenkomsten of om de prestatie van beleggingsfondsen te meten en tot wijziging van Richtlijnen 2008/48/EG en 2014/17/EU en Verordening (EU) nr. 596/2014 (PB L 171 van 29.6.2016, blz. 1).

([36]) Verordening (EU) 2020/1503 van het Europees Parlement en de Raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van Verordening (EU) 2017/1129 en Richtlijn (EU) 2019/1937 (PB L 347 van 20.10.2020, blz. 1).

3. een autoriteit die is belast met de vaststelling en/of activering van macroprudentiële beleidsmaatregelen of met andere taken op het gebied van financiële stabiliteit, zoals daaraan gerelateerde ondersteunende analyses, met inbegrip van, maar niet beperkt tot:

   i. een aangewezen autoriteit krachtens titel VII, hoofdstuk 4, van Richtlijn 2013/36/EU of artikel 458, lid 1, van Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad ([37]);

   ii. een macroprudentiële autoriteit met de doelstellingen, regelingen, taken, bevoegdheden, instrumenten, verantwoordingsvereisten en andere in Aanbeveling ESRB/2011/3 van het Europees Comité voor systeemrisico's ([38]) uiteengezette kenmerken.

g) "betrokken autoriteit":

   1. een ETA;

   2. de ECB voor de taken die haar zijn opgedragen uit hoofde van artikel 4, leden 1 en 2, en artikel 5, lid 2, van Verordening (EU) nr. 1024/2013;

   3. een betrokken nationale autoriteit.

2. **Uitvoeringscriteria**

De volgende criteria zijn van toepassing op de uitvoering van deze aanbeveling:

a) het need-to-know-beginsel en het evenredigheidsbeginsel moeten naar behoren in aanmerking worden genomen, rekening houdend met de doelstelling en de inhoud van elke aanbeveling;

b) De in de bijlage opgenomen specifieke criteria voor de naleving van elke aanbeveling moeten worden nageleefd.

3. **Tijdschema voor het opvolgen van de aanbevelingen**

Overeenkomstig artikel 17, lid 1, van Verordening (EU) nr. 1092/2010 moeten geadresseerden het Europees Parlement, de Raad, de Commissie en het ESRB te informeren over de maatregelen die zij naar aanleiding van deze aanbeveling hebben genomen, of het uitblijven ervan motiveren. De geadresseerden worden verzocht een dergelijke mededeling in te dienen met inachtneming van de volgende termijnen:

1. Aanbeveling A

   a) Uiterlijk op 30 juni 2023, maar niet eerder dan zes maanden na de inwerkingtreding van DORA, worden de ETA's verzocht aan het Europees Parlement, de Raad, de Commissie en het ESRB een tussentijds verslag uit te brengen over de uitvoering van subaanbeveling A(1).

   b) Uiterlijk op 30 juni 2024, maar niet eerder dan 18 maanden na de inwerkingtreding van DORA, worden de ETA's verzocht aan het Europees Parlement, de Raad, de Commissie en het ESRB een eindverslag uit te brengen over de uitvoering van subaanbeveling A(1).

   c) Uiterlijk op 30 juni 2025, maar niet eerder dan 30 maanden na de inwerkingtreding van DORA, worden de ETA's verzocht aan het Europees Parlement, de Raad, de Commissie en het ESRB een verslag uit te brengen over de uitvoering van subaanbeveling A(2).

2. Aanbeveling B

   Uiterlijk op 30 juni 2023, maar niet eerder dan zes maanden na de inwerkingtreding van DORA, worden de ETA's, de ECB en de lidstaten verzocht aan het Europees Parlement, de Raad, de Commissie en het ESRB een verslag uit te brengen over de uitvoering van aanbeveling B.

3. Aanbeveling C

   a) Uiterlijk op 31 december 2023, maar niet eerder dan twaalf maanden na de inwerkingtreding van DORA, wordt de Commissie verzocht aan het Europees Parlement, de Raad en het ESRB een verslag uit te brengen over de uitvoering van aanbeveling C met het oog op het tussentijds verslag overeenkomstig subaanbeveling A(1).

([37]) Verordening (EU) Nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 176 van 27.6.2013, blz. 1).

([38]) Aanbeveling ESRB/2011/3 van het Europees Comité voor systeemrisico's van 22 december 2011 inzake het macroprudentieel mandaat van nationale autoriteiten (PB C 41 van 14.2.2012, blz. 1).

b) Uiterlijk op 31 december 2025, maar niet eerder dan 36 maanden na de inwerkingtreding van DORA, wordt de Commissie verzocht aan het Europees Parlement, de Raad en het ESRB een verslag uit te brengen over de uitvoering van aanbeveling C met het oog op de verslagen van de ETA's overeenkomstig aanbeveling A.

4. **Toezicht en beoordeling**

1. Het ESRB-secretariaat zal:

a) de geadresseerden bijstaan door te zorgen voor de coördinatie van de rapportage en de verstrekking van toepasselijke modelformulieren, en zo nodig de procedure en het tijdschema voor opvolging nader toe te lichten;

b) de opvolging door de geadresseerden verifiëren, op hun verzoek bijstand verlenen en voortgangsverslagen indienen bij de Algemene Raad. De beoordelingen worden als volgt uitgevoerd:

i) binnen twaalf maanden na de inwerkingtreding van DORA voor wat betreft uitvoering van aanbevelingen A en B;

ii) binnen 18 maanden na de inwerkingtreding van DORA voor wat betreft de uitvoering van aanbeveling C;

iii) binnen 24 maanden na de inwerkingtreding van DORA voor wat betreft de uitvoering van aanbeveling A;

iv) binnen 36 maanden na de inwerkingtreding van DORA voor wat betreft de uitvoering van aanbeveling A;

v) binnen 42 maanden na de inwerkingtreding van DORA voor wat betreft de uitvoering van aanbeveling C.

2. De Algemene Raad zal de door de geadresseerden meegedeelde acties en rechtvaardigingen beoordelen en kan, waar passend, besluiten dat deze aanbeveling niet is opgevolgd en dat een geadresseerde er niet in is geslaagd het niet-ondernemen van actie genoegzaam te rechtvaardigen.

Gedaan te Frankfurt am Main, 2 december 2021.

Hoofd van het ESRB-secretariaat,
namens de Algemene Raad van het ESRB,
Francesco MAZZAFERRO

BIJLAGE

SPECIFICATIE VAN DE NALEVINGSCRITERIA DIE VAN TOEPASSING ZIJN OP DE AANBEVELINGEN

Aanbeveling A – Vaststelling van een pan-Europees coördinatiekader voor systemische cyberincidenten (EU-SCICF)

Voor subaanbeveling A(1) zijn de volgende nalevingscriteria vastgesteld.

1. Bij de voorbereiding van een doeltreffende gecoördineerde reactie op Unieniveau, die de geleidelijke ontwikkeling van het EU-SCICF met zich mee zou moeten brengen door de bevoegdheid uit te oefenen die is voorzien in de toekomstige verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht van de financiële sector (hierna "DORA" genoemd), moeten de Europese toezichthoudende autoriteiten (ETA's), handelend via het Gemengd Comité en samen met de Europese Centrale Bank (ECB), het Europees Comité voor systeemrisico's (ESRB) en de betrokken nationale autoriteiten, en in overleg met het Agentschap van de Europese Unie voor cyberbeveiliging en de Commissie, indien nodig, overwegen ten minste de volgende aspecten op te nemen bij de voorgenomen voorbereiding van het EU-SCICF:

   a. analyse van de middelen die nodig zijn voor een doeltreffende ontwikkeling van het EU-SCICF;

   b. ontwikkeling van nood- en crisisbeheersingsoefeningen met cyberaanvalscenario's met het oog op de ontwikkeling van communicatiekanalen;

   c. ontwikkeling van een gemeenschappelijke woordenlijst;

   d. ontwikkeling van een coherente classificatie van cyberincidenten;

   e. oprichting van veilige en betrouwbare gegevensuitwisselingskanalen, met inbegrip van back-upsystemen;

   f. aanwijzing van contactpunten;

   g. inachtneming van vertrouwelijkheid bij de uitwisseling van informatie aanpakken;

   h. initiatieven voor samenwerking en informatie-uitwisseling met de cyberinlichtingendiensten van de financiële sector;

   i. ontwikkeling van effectieve activerings- en escalatieprocessen door middel van situationeel bewustzijn;

   j. verduidelijking van de verantwoordelijkheden van de deelnemers aan het kader;

   k. ontwikkeling van interfaces voor sectoroverschrijdende coördinatie en, in voorkomend geval, coördinatie met derde landen;

   l. zorgen voor coherente communicatie tussen de betrokken autoriteiten en het publiek om het vertrouwen te behouden;

   m. vaststelling van vooraf bepaalde communicatielijnen voor tijdige communicatie;

   n. uitvoering van passende kadertestoefeningen, met inbegrip van rechtsgebied-overschrijdende tests en coördinatie met derde landen, en beoordelingen waaruit lering getrokken kan worden en waardoor de verdere ontwikkeling van het kader teweeggebracht kan worden;

   o. zorgen voor doeltreffende communicatie en tegenmaatregelen tegen desinformatie.

Aanbeveling B – Vaststelling van contactpunten van het EU-SCICF

Voor aanbeveling B zijn de volgende nalevingscriteria vastgesteld.

1. De ETA's, de ECB en de betrokken nationale autoriteiten van elke lidstaat moeten overeenstemming bereiken over een gemeenschappelijke aanpak voor het uitwisselen en bijwerken van de lijst van aangewezen contactpunten van het EU-SCICF.

2. Bij de beoordeling van de aanwijzing van het contactpunt moet rekening worden gehouden met het uit hoofde van Richtlijn (EU) 2016/1148 aangewezen centraal contactpunt dat de lidstaten hebben aangewezen voor de beveiliging van netwerk- en informatiesystemen met het oog op grensoverschrijdende samenwerking met andere lidstaten en met de samenwerkingsgroep voor netwerk- en informatiesystemen.

Aanbeveling C – Wijzigingen van het rechtskader van de Unie

Voor aanbeveling C is het volgende nalevingscriterium vastgesteld.

De Commissie moet nagaan of, naar aanleiding van de overeenkomstig aanbeveling A uitgevoerde analyse, maatregelen, met inbegrip van wijzigingen van de desbetreffende Uniewetgeving, nodig zijn om ervoor te zorgen dat de ETA's, via het Gemengd Comité en samen met de ECB, het ESRB en de betrokken nationale autoriteiten, het EU-SCICF kunnen ontwikkelen overeenkomstig subaanbeveling A(1), en om ervoor te zorgen dat de ETA's, de ECB, het ESRB en de betrokken nationale autoriteiten, alsook andere autoriteiten, kunnen deelnemen aan coördinatieacties en de uitwisseling van informatie die voldoende gedetailleerd en consistent is om een doeltreffend EU-SCICF te ondersteunen.