I

(Resolutions, recommendations and opinions)

RECOMMENDATIONS

EUROPEAN SYSTEMIC RISK BOARD

RECOMMENDATION OF THE EUROPEAN SYSTEMIC RISK BOARD

of 2 December 2021

on a pan-European systemic cyber incident coordination framework for relevant authorities

(ESRB/2021/17)

(2022/C 134/01)

THE GENERAL BOARD OF THE EUROPEAN SYSTEMIC RISK BOARD,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to the Agreement on the European Economic Area ([1]), in particular Annex IX thereof,

Having regard to Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board ([2]), and in particular Article 3(2)(b) and (d) and Articles 16 and 18 thereof,

Having regard to Decision ESRB/2011/1 of the European Systemic Risk Board of 20 January 2011 adopting the Rules of Procedure of the European Systemic Risk Board ([3]), and in particular Articles 18 to 20 thereof,

Whereas:

(1) As noted in recital 4 of Recommendation ESRB/2013/1 of the European Systemic Risk Board ([4]), the ultimate objective of macroprudential policy is to contribute to safeguarding the stability of the financial system as a whole, including by strengthening the resilience of the financial system and decreasing the build-up of systemic risks, thereby ensuring a sustainable contribution of the financial sector to economic growth. The European Systemic Risk Board (ESRB) is responsible for the macroprudential oversight of the financial system within the Union. In fulfilling its mandate, the ESRB should contribute to the prevention and mitigation of systemic risks to financial stability, including those related to cyber incidents, and propose how these risks might be mitigated.

(2) Major cyber incidents may pose a systemic risk to the financial system given their potential to disrupt critical financial services and operations. The amplification of an initial shock can either occur through operational or financial contagion or through an erosion of confidence in the financial system. If the financial system is unable to absorb these shocks, financial stability will be at risk and this situation can result in a systemic cyber crisis ([5]).

([1]) OJ L 1, 3.1.1994, p. 3.
([2]) OJ L 331, 15.12.2010, p. 1.
([3]) OJ C 58, 24.2.2011, p. 4.
([4]) Recommendation ESRB/2013/1 of the European Systemic Risk Board of 4 April 2013 on intermediate objectives and instruments of macro-prudential policy (OJ C 170, 15.6.2013, p. 1).
([5]) See Systemic cyber risk, ESRB, February 2020, available on the ESRB website at www.esrb.europa.eu

(3) The constantly evolving cyber threat landscape and recent increase of major cyber incidents are indicators of greater risk to financial stability in the Union. The COVID-19 pandemic has highlighted the importance of the role technology plays in allowing the financial system to operate. Relevant authorities and institutions needed to adapt their technical infrastructure and risk management frameworks to a sudden increase in remote working, which has increased the overall exposure of the financial system to cyber threats and allowed criminals both to devise new modi operandi and to adapt existing ones to exploit the situation ([6]). Against this background, the number of cyber incidents reported to ECB Banking Supervision in 2020 increased by 54 % compared with 2019 ([7]).

(4) A major cyber incident's potentially large scale, speed and rate of propagation call for an effective response from the relevant authorities to mitigate the potential negative effects on financial stability. Swift coordination and communication among relevant authorities at Union level can assist in early assessment of a major cyber incident's impact on financial stability, maintaining confidence in the financial system and limiting contagion to other financial institutions and thus contribute to preventing a major cyber incident from becoming a risk to financial stability.

(5) The underlying shock originates in a novel way compared to the traditional financial and liquidity crises relevant authorities usually face. Aside from financial aspects, the overall risk assessment must include the scale and impact of operational disruptions as these might influence the choice of macroprudential tools. Likewise, financial stability might also influence the choice of operational mitigants by cyber experts. This calls for close and swift coordination and open communication to, inter alia, build situational awareness.

(6) The risk of a coordination failure by authorities exists and needs to be addressed. Relevant authorities in the Union will need to coordinate among themselves and with other authorities such as the European Union Agency for Network and Information Security (ENISA) with which they might not usually interact. As a significant number of Union financial institutions operate globally, a major cyber incident will likely not be limited to the Union or might be triggered outside the Union and might require global response coordination.

(7) The relevant authorities need to be prepared for these interactions. Otherwise, they might risk taking inconsistent actions that contradict or jeopardise other authorities' responses. Such a coordination failure could amplify the shock for the financial system by leading to an erosion of confidence in the functioning of the financial system which, in the worst-case scenario, would pose a risk to financial stability ([8]).Thus, the necessary steps should be taken to address the risk to financial stability stemming from a coordination failure in the event of a major cyber incident.

(8) The ESRB (2021) report *Mitigating systemic cyber risk* ([9]) identifies the need to establish a pan-European systemic cyber incident coordination framework (EU-SCICF) for relevant authorities in the Union. The objective of the EU-SCICF would be to increase relevant authorities' level of preparedness to facilitate a coordinated response to a potentially major cyber incident. The ESRB (2021) report *Mitigating systemic cyber risk* provides the ESRB's assessment on the framework characteristics that would be needed, prima facie, in order to address the risk of a coordination failure.

(9) The key objective of this Recommendation is to build on one of the envisaged roles of the European Supervisory Authorities (ESAs) under the proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector ([10]) (hereinafter 'DORA') of gradually enabling an effective Union-level coordinated response in the event of a major cross-border information and communication technologies (ICT) related incident or related threat having a systemic impact on the Union's financial sector as a whole. This process will lead to the creation of the EU-SCICF for relevant authorities.

([6]) See Internet Organised Crime Threat Assessment, Europol, 2020, available on the Europol website at www.europol.europa.eu
([7]) See IT and cyber risk: a constant challenge, ECB, 2021, available on the ECB Banking Supervision website at www.bankingsupervision.europa.eu
([8]) See Systemic cyber risk, ESRB, February 2020, available on the ESRB website at www.esrb.europa.eu
([9]) See Mitigating systemic cyber risk, ESRB, 2021, (forthcoming).
([10]) COM/2020/595 final.

(10) The EU-SCICF should not aim to replace existing frameworks but to bridge any coordination and communication gaps between the relevant authorities themselves and with other authorities in the Union and other key actors at international level. In this respect, the positioning of the EU-SCICF in the existing financial crisis framework and Union cyber incident framework landscape should be considered. Regarding coordination among the relevant authorities themselves, consideration should be given, but not be limited to, the roles and activities of the Network and Information Systems (NIS) Cooperation Group for financial entities under Directive (EU) 2016/1148 of the European Parliament and of the Council ([11]), and the coordination mechanisms envisaged through the establishment of the Joint Cyber Unit alongside the involvement of ENISA.

(11) In particular, the proposal to launch the preparation of the EU-SCICF aims to endorse the potential roles of the ESAs, as envisaged by the DORA proposal. DORA proposes that 'the ESAs, through the Joint Committee and in collaboration with competent authorities, the European Central Bank (ECB) and the ESRB, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across-sectors' and 'may develop crisis-management and contingency exercises involving cyberattack scenarios with a view to develop communication channels and gradually enable an effective EU-level coordinated response in the event of a major cross-border ICT-related incident or related threat having a systemic impact on the Union's financial sector as a whole' ([12]). A pan-European framework such as the EU-SCICF does not yet exist and should be established and developed in the context of DORA.

(12) Given the risk to financial stability in the Union stemming from cyber risk, preparatory work for the gradual establishment of the EU-SCICF should, to the extent feasible, start even before the required legal and policy framework for its establishment is fully applicable. This legal and policy framework would be completed fully and finalised once the relevant provisions of DORA and of its delegated acts become applicable.

(13) Effective communication contributes to situational awareness among relevant authorities and is thus an indispensable prerequisite for Union-wide coordination during major cyber incidents. In this respect, the communication infrastructure needed to coordinate on a response to a major cyber incident should be defined. This would imply specifying the type of information that needs to be shared, the regular channels to be used to share such information and the contact points with which information should be shared. Information sharing must respect existing legal requirements. In addition, a clear action plan and the protocols to be followed may need to be defined by the relevant authorities to ensure proper coordination among the authorities involved in planning a coordinated response to a major cyber incident.

(14) A systemic cyber crisis will require the setting in motion of full cooperation at national and Union level. Therefore, the designation of points of contact for the ESAs, the ECB and each Member State from among its relevant national authorities, which should be communicated to the ESAs, may be envisaged to establish the main interlocutors in the coordination scheme of the EU-SCICF to be informed in case of a major cyber incident. The need to designate points of contact should be assessed during the development of the EU-SCICF, taking into account the designated single point of contact under Directive (EU) 2016/1148 that Member States have established on the security of network and information systems to ensure cross-border cooperation with other Member States and with the NIS Cooperation Group ([13]).

(15) The conduct of crisis management and contingency exercises could facilitate the implementation of the EU-SCICF and allow authorities to evaluate their readiness and preparedness for a systemic cyber crisis at Union level. Such exercises would provide authorities with lessons learnt and would enable continuous improvement and evolution of the EU-SCICF.

([11]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).
([12]) See draft Article 43 of the proposal for DORA.
([13]) See European Commission, NIS Cooperation Group, available on the European Commission website at ec.europa.eu

(16) For the development of the EU-SCICF it is essential that the ESAs jointly carry out relevant preparatory work to consider the potential key elements of the framework and the required resources and needs to proceed with its development. After this, the ESAs could start work on a preliminary analysis of any impediments that could hinder the ESAs and relevant authorities' abilities to establish the EU-SCICF and to share relevant information through communication channels in case of a major cyber incident. Such analysis would be an important step informing any further action, either of legislative nature or other supporting initiatives that the European Commission may take in the post-DORA implementation stage,

HAS ADOPTED THIS RECOMMENDATION:

SECTION 1

RECOMMENDATIONS

Recommendation A – Establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF)

1. It is recommended that, as envisaged in the Commission's proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (hereinafter 'DORA'), the European Supervisory Authorities (ESAs), jointly through the Joint Committee, and together with the European Central Bank (ECB), the European Systemic Risk Board (ESRB) and relevant national authorities, start preparing for the gradual development of an effective Union-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the Union's financial sector. Preparatory work towards a Union-level coordinated response should entail the gradual development of EU-SCICF for the ESAs, the ECB, the ESRB and relevant national authorities. This also should include an assessment of the resource requirements for the effective development of the EU-SCICF.

2. It is recommended that the ESAs undertake, in view of sub-Recommendation A(1), in consultation with the ECB and the ESRB, a mapping and subsequent analysis of current impediments, legal and other operational barriers for the effective development of the EU-SCICF.

Recommendation B – Establishment of points of contact of the EU-SCICF

It is recommended that the ESAs, the ECB and each Member State among their relevant national authorities should designate a main point of contact which should be communicated to the ESAs. This contact list will facilitate the development of the framework and, once the EU-SCICF is in place, the points of contact and the ESRB should be informed in case of a major cyber incident. Co-ordination should also be envisaged between the EU-SCICF and the designated single point of contact under Directive (EU) 2016/1148 that Member States have established on the security of network and information systems to ensure cross-border cooperation with other Member States and with the Network and Information Systems Cooperation Group.

Recommendation C – Appropriate measures at Union level

It is recommended that, based on the result of the analyses carried out in accordance with Recommendation A, the Commission should consider the appropriate measures needed to ensure effective coordination of responses to systemic cyber incidents.

SECTION 2

IMPLEMENTATION

1. **Definitions**

For the purposes of this Recommendation the following definitions apply:

(a) 'cyber' means relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems ([14]);

([14]) See Cyber Lexicon, FSB, 12 November 2018, available on the FSB website at www.fsb.org

(b) 'major cyber incident' means an ICT-related incident with a potentially high adverse impact on the network and information systems that support critical functions of financial entities ([15]);

(c) 'systemic cyber crisis' means a major cyber incident that causes a level of disruption in the Union financial system potentially entailing serious negative consequences for the smooth operation of the internal market and the functioning of the real economy. Such a crisis could result from a major cyber incident causing shocks in a number of channels, including operational, confidence and financial;

(d) 'European Supervisory Authorities' or the 'ESAs' means the European Supervisory Authority (European Banking Authority) established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([16]), together with the European Supervisory Authority (European Insurance and Occupational Pensions Authority) established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council ([17]) and the European Supervisory Authority (European Securities and Markets Authority) established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council ([18]);

(e) 'Joint Committee' means the Joint Committee of the European Supervisory Authorities established in Article 54 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010;

(f) 'relevant national authority' means:

(1) a competent or supervisory authority in a Member State as specified in the Union acts referred to in Article 1(2) of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010 and any other national competent authority as specified in Union acts that confer tasks on the ESAs;

(2) a competent authority in a Member State designated in accordance with:

(i) Article 4 of Directive 2013/36/EU of the European Parliament and of the Council ([19]), without prejudice to the specific tasks conferred on the ECB by Council Regulation (EU) No 1024/2013 ([20]);

(ii) Article 22 of Directive (EU) 2015/2366 of the European Parliament and of the Council ([21]);

(iii) Article 37 of Directive 2009/110/EC of the European Parliament and of the Council ([22]);

(iv) Article 4 of Directive (EU) 2019/2034 of the European Parliament and of the Council ([23]);

([15]) See point (7) of draft Article 3 of the proposal for DORA.

([16]) Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

([17]) Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Investment and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

([18]) Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

([19]) Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

([20]) Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

([21]) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

([22]) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

([23]) Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU (OJ L 314, 5.12.2019, p. 64).

(v) the first indent of point (ee) of Article 3(1) of the proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 ([24]);

(vi) Article 11 of Regulation (EU) No 909/2014 of the European Parliament and of the Council ([25]);

(vii) Article 22 of Regulation (EU) No 648/2012 of the European Parliament and of the Council ([26]);

(viii) Article 67 of Directive 2014/65/EU of the European Parliament and of the Council ([27]);

(ix) Article 22 of Regulation (EU) No 648/2012;

(x) Article 44 of Directive 2011/61/EU of the European Parliament and of the Council ([28]);

(xi) Article 97 of Directive 2009/65/EC of the European Parliament and of the Council ([29]);

(xii) Article 30 of Directive 2009/138/EC of the European Parliament and of the Council ([30]);

(xiii) Article 12 of Directive (EU) 2016/97 of the European Parliament and of the Council ([31]);

(xiv) Article 47 of Directive (EU) 2016/2341 of the European Parliament and of the Council ([32]);

(xv) Article 22 of Regulation (EC) No 1060/2009 of the European Parliament and of the Council ([33]);

(xvi) Article 3(2) and Article 32 of Directive 2006/43/EC of the European Parliament and of the Council ([34]);

(xvii) Article 40 of Regulation (EU) 2016/1011 of the European Parliament and of the Council ([35]);

(xviii) Article 29 of Regulation (EU) 2020/1503 of the European Parliament and of the Council ([36]);

([24]) COM/2020/593 final.
([25]) Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1).
([26]) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).
([27]) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).
([28]) Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).
([29]) Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (OJ L 302, 17.11.2009, p. 32).
([30]) Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).
([31]) Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (OJ L 26, 2.2.2016, p. 19).
([32]) Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (OJ L 354, 23.12.2016, p. 37).
([33]) Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies (OJ L 302, 17.11.2009, p. 1).
([34]) Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87).
([35]) Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (OJ L 171, 29 June 2016, p. 1).
([36]) Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (OJ L 347, 20.10.2020, p. 1).

(3) an authority entrusted with the adoption and/or activation of macroprudential policy measures or with other financial stability tasks, such as related supporting analysis, including but not limited to:

(i) a designated authority pursuant to Chapter 4 of Title VII of Directive 2013/36/EU or Article 458(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council ([37]);

(ii) a macroprudential authority with the objectives, arrangements, tasks, powers, instruments, accountability requirements and other characteristics set out in Recommendation ESRB/2011/3 of the European Systemic Risk Board ([38]);

(g) 'relevant authority' means:

(1) an ESA;

(2) the ECB for the tasks conferred to it in accordance with Articles 4(1) and (2) and Article 5(2) of Regulation (EU) No 1024/2013;

(3) a relevant national authority.

2. **Criteria for implementation**

The following criteria apply to the implementation of this Recommendation:

(a) due regard should be paid to the need-to-know principle and the principle of proportionality, taking into account the objective and the content of each Recommendation;

(b) the specific compliance criteria set out in the Annex in relation to each Recommendation should be met.

3. **Timeline for the follow-up**

In accordance with Article 17(1) of Regulation (EU) No 1092/2010 addressees must communicate to the European Parliament, the Council, the Commission and to the ESRB the actions undertaken in response to this Recommendation or substantiate any inaction. Addressees are requested to submit such communication in compliance with the following timelines:

1. Recommendation A

(a) By 30 June 2023 but no earlier than six months after DORA enters into force, the ESAs are requested to deliver to the European Parliament, the Council, the Commission and to the ESRB an interim report on the implementation of sub-Recommendation A(1).

(b) By 30 June 2024 but no earlier than 18 months after DORA enters into force, the ESAs are requested to deliver to the European Parliament, the Council, the Commission and to the ESRB a final report on the implementation of sub-Recommendation A(1).

(c) By 30 June 2025 but no earlier than 30 months after DORA enters into force, the ESAs are requested to deliver to the European Parliament, the Council, the Commission and to the ESRB a report on the implementation of sub-Recommendation A(2).

2. Recommendation B

By 30 June 2023 but no earlier than six months after DORA enters into force, the ESAs, the ECB and Member States are requested to deliver to the European Parliament, the Council, the Commission and to the ESRB a report on the implementation of Recommendation B.

3. Recommendation C

(a) By 31 December 2023 but no earlier than 12 months after DORA enters into force, the Commission is requested to deliver to the European Parliament, the Council, and to the ESRB a report on the implementation of Recommendation C in view of the interim report of the ESAs in accordance with sub-Recommendation A(1).

([37]) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

([38]) Recommendation ESRB/2011/3 of the European Systemic Risk Board of 22 December 2011 on the macro-prudential mandate of national authorities (OJ C 41, 14.2.2012, p. 1).

(b) By 31 December 2025 but no earlier than 36 months after DORA enters into force, the Commission is requested to deliver to the European Parliament, the Council, and to the ESRB a report on the implementation of Recommendation C in view of the reports of the ESAs in accordance with Recommendation A.

4. **Monitoring and assessment**

1. The ESRB Secretariat will:

(a) assist the addressees, ensuring the coordination of reporting and the provision of relevant templates, and detailing where necessary the procedure and the timeline for the follow-up;

(b) verify the follow-up by the addressees, provide assistance at their request, and submit follow-up reports to the General Board. The assessments will be initiated as follows:

(i) within 12 months after the entry into force of DORA, regarding the implementation of Recommendation A and B;

(ii) within 18 months after the entry into force of DORA, regarding the implementation of Recommendation C;

(iii) within 24 months after the entry into force of DORA, regarding the implementation of Recommendation A;

(iv) within 36 months after the entry into force of DORA, regarding the implementation of Recommendation A;

(v) within 42 months after the entry into force of DORA, regarding the implementation of Recommendation C;

2. The General Board will assess the actions and justifications communicated by the addressees and, where appropriate, may decide that this Recommendation has not been followed and that an addressee has failed to provide adequate justification for its inaction.

Done at Frankfurt am Main, 2 December 2021.

The Head of the ESRB Secretariat,
on behalf of the General Board of the ESRB
Francesco MAZZAFERRO

ANNEX

SPECIFICATION OF THE COMPLIANCE CRITERIA APPLICABLE TO THE RECOMMENDATIONS

Recommendation A – Establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF)

For sub-Recommendation A(1), the following compliance criteria are specified.

1. When preparing for an effective Union-level coordinated response which should entail the gradual development of the EU-SCICF by exercising the power envisaged in the future Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (hereinafter 'DORA'), the European Supervisory Authorities (ESAs), acting through the Joint Committee, and together with the European Central Bank (ECB), the European Systemic Risk Board (ESRB) and relevant national authorities, and in consultation with the European Union Agency for Network and Information Security and the Commission where considered necessary, should consider including in the envisaged preparation for the EU-SCICF at least the following aspects:

   (a) analysis of the resource requirements for effective development of the EU-SCICF;

   (b) developing crisis management and contingency exercises involving cyberattack scenarios with a view to developing communication channels;

   (c) development of a common vocabulary;

   (d) development of a coherent cyber incident classification;

   (e) establishment of secure and reliable information sharing channels, including back-up systems;

   (f) establishment of points of contact;

   (g) address confidentiality in information sharing;

   (h) collaboration and information sharing initiatives with financial sector cyber intelligence;

   (i) development of effective activation and escalation processes through situational awareness;

   (j) clarification of the responsibilities of framework participants;

   (k) development of interfaces for cross-sectoral and, where relevant, third country coordination;

   (l) ensuring coherent communication by relevant authorities with the public to preserve confidence;

   (m) establishment of predefined communication lines for timely communication;

   (n) performance of appropriate framework testing exercises, including cross-jurisdictional testing and third country coordination, and assessments which result in lessons learned and framework evolution;

   (o) ensuring effective communication and countermeasures against disinformation.

Recommendation B – Establishment of points of contact of the EU-SCICF

For Recommendation B, the following compliance criteria are specified.

1. The ESAs, the ECB and each Member State among their relevant national authorities should agree on a common approach to sharing and keeping updated the list of designated points of contact of the EU-SCICF.

2. The designation of the point of contact should be assessed taking into account the designated single point of contact under Directive (EU) 2016/1148 that Member States have established in respect of the security of network and information systems to ensure cross-border cooperation with other Member States and with the Network and Information Systems Cooperation Group.

Recommendation C – Changes to the Union legal framework

For Recommendation C, the following compliance criterion is specified.

The Commission should consider whether any measures, including changes to relevant Union legislation, are needed as a result of the analysis carried out in accordance with Recommendation A to ensure that the ESAs, through the Joint Committee and together with the ECB, the ESRB and relevant national authorities, can develop the EU-SCICF in accordance with sub-Recommendation A(1) and to ensure that the ESAs, the ECB, the ESRB and the relevant national authorities, as well as other authorities can engage in coordination actions and exchange of information that is sufficiently detailed and consistent to support an effective EU-SCICF.