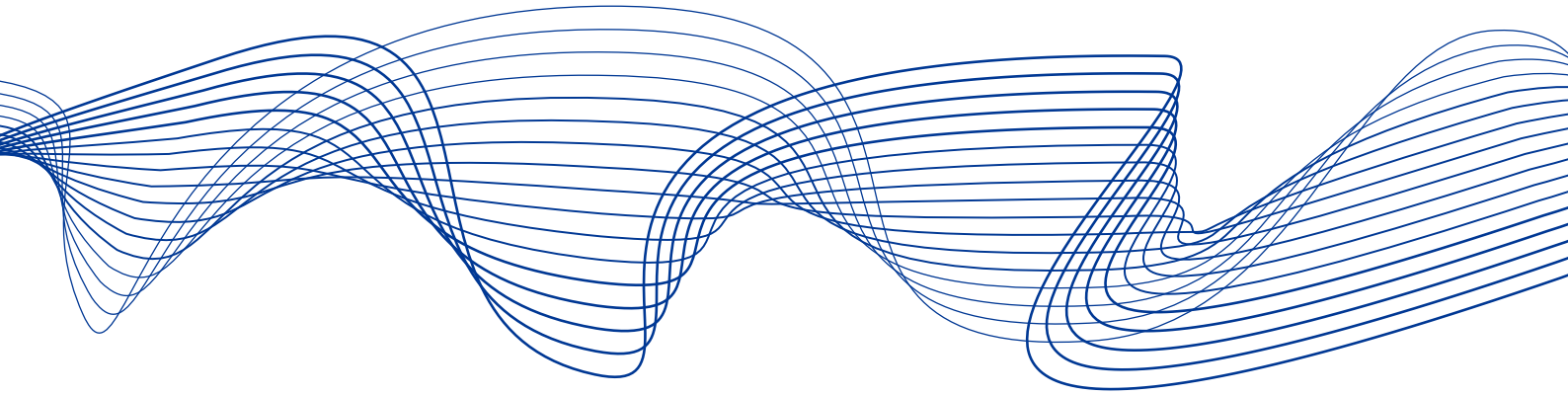
ESRB
European Systemic Risk Board
European System of Financial Supervision

Compliance report on sub-recommendation A(1) of Recommendation of the European Systemic Risk Board of 2 December 2021

August 2025

Compliance report on sub-recommendation A(1) of 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)



Contents

1 Introduction

On 2 December 2021 the General Board of the European Systemic Risk Board (ESRB) adopted Recommendation ESRB/2021/17 on a pan-European systemic cyber incident coordination framework for relevant authorities[1] **(hereinafter the "Recommendation").** This compliance report presents the outcome of the second and final assessment of compliance concerning the implementation of sub-recommendation A(1) of the Recommendation.

Recommendations issued by the ESRB are not legally binding but are subject to an "act or explain" mechanism in accordance with Article 17 of the ESRB Regulation.[2] This means that the addressees of those recommendations are under an obligation to communicate to the European Parliament, the Council of the European Union, the European Commission and the ESRB the actions they have taken to comply with those recommendations or to provide adequate justification for inaction.

Recommendation A concerns the establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF). The European Supervisory Authorities (ESAs) were asked to provide the European Parliament, the Council, the Commission and the ESRB with a final report on the implementation of sub-recommendation A(1) by 16 July 2024. Sub-recommendation A(1) recommends that the ESAs, together with the European Central Bank (ECB), the ESRB and relevant national authorities, start preparing for the gradual development of an effective EU-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the EU's financial sector. The ESAs delivered the final report on the establishment of the EU-SCICF by 16 July 2024.[3] Other information provided by the addressees during the assessment process was also considered in the assessment of compliance. This report reflects the implementation status as at December 2024.

The input from the addressees was examined by a six-person assessment team endorsed by the ESRB's Advisory Technical Committee (ATC). The assessment team was supported by ESRB Secretariat staff (see Annex I for details of its composition). The process followed the methodology set out in the Handbook on the assessment of compliance with ESRB recommendations (hereinafter the "Handbook"). The assessment was conducted taking due account of the objectives of the Recommendation; the principles underpinning the Handbook; the implementation standards prepared by the assessment team, which specify the grade to be awarded for each key element of the recommendation on the basis of

1 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) (OJ C 134, 25.3.2022, p. 1).

2 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 (OJ L 331, 15.12.2010, p. 1).

3 The ESAs' final report on the implementation of sub-recommendation A(1) was titled "EU-SCICF, A pan-European Systemic Cyber Incident Coordination Framework".

the corresponding objectives (see Annex II for details of the implementation standards); and the principle of proportionality.

Overall, the assessment team found that the addressees were largely compliant with sub-recommendation A(1). Part 1 of this compliance report recaps the policy objectives taken into account when drafting the Recommendation. Part 2 summarises the methodology set out in the Handbook, which establishes the procedure for assessing compliance with ESRB recommendations, and presents the implementation standards that the assessment team drafted and used to assess compliance with sub-recommendation A(1). Part 3 contains the assessments of compliance with sub-recommendation A(1). Part 4 discusses the overall findings of the assessment. Lastly, Part 5 concludes the assessment of sub-recommendation A(1). Annex I lists the members of the assessment team and Annex II contains the implementation standards.

2 Policy objectives

Cyber incidents, including cyberattacks, can pose a systemic risk to the financial system given their potential to disrupt critical financial services and operations and thus impair the provision of key economic functions. In a worst-case scenario, a systemic cyber crisis could unfold. The financial sector relies on resilient information and communications technology systems and is highly dependent on the confidentiality, integrity and availability of the data and systems it uses. A cyber incident could affect operational systems in the financial system and impair the provision of critical economic functions, trigger financial contagion or lead to an erosion of confidence in the financial system. If the financial system is not able to absorb these shocks, financial stability is likely to be put at risk and a systemic cyber crisis could unfold.[4]

Given the potential scale, speed and rate of propagation of a major cyber incident, it is crucial for relevant authorities to respond effectively to mitigate the potential negative effects on financial stability. While the later stages of a systemic cyber crisis can resemble a more traditional financial crisis, the impairment of the financial system's operability adds a new dimension to crisis management. Therefore, in addition to financial aspects, the overall risk assessment must also consider the scale and impact of operational disruptions, as these might influence the choice of macroprudential tools. Likewise, financial stability might also affect the choice of operational mitigants by cyber experts. This calls for close and swift coordination and communication among relevant authorities at EU level to build situational awareness. This can be useful in the initial assessment of a major cyber incident's impact on financial stability. It can also contribute to maintaining confidence in the financial system and limiting contagion to other financial institutions, thus helping to prevent a major cyber incident from becoming a risk to financial stability.

The Recommendation aims to establish a pan-European systemic cyber incident coordination framework (EU-SCICF). The objectives are to increase the preparedness of financial authorities in the EU and define a coherent and thus more effective response to a cyber incident, thereby mitigating the risk of a coordination failure. To respond effectively to potential major cyber incidents, a high level of preparedness and coordination among financial authorities is needed. As a significant number of EU financial institutions operate globally, a major cyber incident would likely not be limited to the EU or might be triggered outside it and could require coordinating and cooperating on a global response with other authorities that the financial authorities might not usually interact with, such as the European Union Agency for Cybersecurity (ENISA). The EU-SCICF aims to strengthen coordination among EU financial authorities, as well as with other authorities in the EU and key actors at international level. It would complement the existing EU cyber incident response frameworks and address the specific risk of a coordination failure. It would

[4] ESRB, Systemic Cyber Risk, February 2020.

do so by asking relevant authorities to prepare for interactions with each other and with authorities they might be less familiar with when responding to major cyber incidents to mitigate the potential negative effects on financial stability.[5]

The Recommendation and the assessment of the addressees' implementation of it recognise that cyber risk is not limited to the financial system. A number of agencies have been established and cyber incident response initiatives developed to minimise the risks of cyberattacks. The EU-SCICF, which is to be developed under sub-recommendation A(1), seeks to address threats to financial stability. It will coexist with other frameworks but will have a clear focus on financial stability aspects not covered by existing mechanisms.

2.1 Scope and content

Recommendation ESRB/2021/17 is divided into three recommendations (A, B and C). This report and its analysis focus only on sub-recommendation A(1), for which the reporting deadline was 16 July 2024.

Sub-recommendation A(1) recommends that the ESAs, together with the ECB, the ESRB and relevant national authorities, start preparing for the gradual development of an effective EU-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the EU's financial sector. Preparatory work towards a EU-level coordinated response should entail the gradual development of the 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.

The Recommendation, which was issued in December 2021 and published in January 2022, aims to ensure that the EU-SCICF is operational and fulfilling its intended function by January 2025, when the Digital Operational Resilience Act (DORA) comes into effect. Therefore, it is an important element in preventing or at least mitigating risks to financial stability that may arise from cyber incidents. The assessment team recognises that this is an ambitious objective and agrees that there may be impediments that could affect the ability of the ESAs and relevant competent authorities to establish a fully fledged EU-SCICF by January 2025. However, it believes that the Recommendation sets out a clear path for establishing such a framework by that date and developing it further over time. While implementation will require resources at all levels, these are also needed to ensure the framework supports an effective EU response and minimises the risks to financial stability.

[5] ESRB, Mitigating systemic cyber risk, January 2022.

3 Assessment methodology

The assessment of the implementation of the Recommendation was carried out on the basis of the "act or explain" mechanism, in accordance with Article 17 of the ESRB Regulation. This means that the addressees of the Recommendation can either (i) take action in response to each of the recommendations and inform the ESRB of such action, or (ii) take no action, provided that they can properly justify that inaction. The assessment team then analyses the information provided and assesses whether the action taken achieves the objectives of each recommendation or whether the justification provided for inaction is sufficient. This analysis results in a final compliance grade being assigned to each addressee.

To ensure equal treatment among addressees and the highest possible degree of transparency and consistency, the assessment team conducted its work in accordance with the following six assessment principles described in Section 4 of the Handbook:

- **fairness, consistency and transparency** – equal treatment of all addressees throughout the assessment process;
- **efficiency and appropriateness** of procedures with regard to available resources, while ensuring high-quality deliverables;
- **four-eyes review** – compliance of each addressee is assessed by at least two assessors who have not been directly involved in assessing the performance of the national authorities they come from;
- **effective dialogue** – communication with the addressees is essential to fill in information gaps on compliance;
- **principle of proportionality** – actions to be taken by the addressees are country-specific and relative to the intensity of risks targeted by the recommendation in the specific Member State; and
- **ultimate objective** – prevention and mitigation of systemic risks to financial stability in the EU.

Compliance was assessed by recommendation. Since the assessment focused on sub-recommendation A(1) only and the addressees submitted a joint report, the assessment team decided to evaluate compliance by recommendation. The assessment team therefore formed two groups. In an initial assessment, each group assessed sub-recommendation A(1) against some of the compliance criteria outlined in the Annex to the Recommendation. After completing the first assessment, the groups switched and assessed the sub-recommendation against the criteria they had not covered in the first assessment, ensuring a four-eyes review.

The assessment was based on the submission made by the addressees by the reporting deadline of 16 July 2024 as well as the dialogue maintained between the assessment team and the addressees during the assessment process. For sub-recommendation A(1), the ESAs delivered a final report on the establishment of the EU-SCICF by 16 July 2024.

Responses and information provided by the addressees during the assessment process were also included in the assessment.

3.1 Assessment criteria and implementation standards

The assessment criteria describe the actions that are required of the addressees in order to achieve the objectives of the Recommendation. The assessment criteria applied in this evaluation and the approach to the assessment are based, among other things, on the best practices established in previous assessments of compliance with ESRB recommendations. The assessment team also took due account of the implementation criteria set out in Section 2(2) of the Recommendation and in its Annex. During the assessment, the assessment team analysed the content and substance of the actions taken by each addressee to assess whether they had complied with all elements of the Recommendation. To ensure a consistent and fair analysis, the responses submitted by the addressees were assessed against the implementation standards (see Annex II).

The implementation standards are based on the assessment criteria and specify how different actions or inaction should be reflected in the final grade. In this case, the implementation standards were based on the following key criteria:

- gradual development of the EU-SCICF (final report);
- completeness and timeliness of reporting.

Sub-recommendation A(1) recommended that the addressees start preparations for the gradual development of the EU-SCICF, so the addressees provided a final report. The follow-up to sub-recommendation A(1) is divided into two milestones: an interim report and a final report (Section 2(3) of the Recommendation). This assessment is limited to the final report only, which was to be delivered 18 months after the entry into force of the Digital Operational Resilience Act (DORA). The final report should include details on the status of the gradual development of the EU-SCICF, thus taking into account the specified compliance criteria set out in the Annex to the Recommendation. In the previous assessment for sub-recommendation A(1), the ESAs were assessed as “fully compliant” based on their interim report. Since the current assessment considers the final report, the compliance criteria were expected to be fully met at this point, with concrete steps and plans in place for the development and implementation of the EU-SCICF as of January 2025.

3.2 Grading methodology

The assessment team followed a four-step grading methodology to assign a grade to each addressee for their compliance with sub-recommendation A(1). This methodology ensures full transparency of the single overall compliance grade and a high level of objectivity throughout the assessment process. It also allows room for high-quality expert judgement, which can easily be identified and reviewed to understand the rationale behind the allocation of specific overall grades.

Step I

Each key criterion of sub-recommendation A(1) was assessed and graded on the basis of the assessment criteria – in accordance with the established implementation standards – in terms of each addressee's action or inaction. The full grading scale is shown in Table 1 below.

Table 1
Grading scale

Grading scale for action	
Fully compliant (FC)	The addressee complies entirely with the recommendation.
Largely compliant (LC)	The objectives of the recommendation have been met almost entirely and only negligible requirements are still to be implemented.
Partially compliant (PC)	The most important requirements have been met. There are certain deficiencies that affect the implementation process, although this does not result in a situation where the recommendation has not been acted on.
Materially non-compliant (MNC)	Requirements have been fulfilled to a limited degree, resulting in significant deficiencies in the implementation.
Non-compliant (NC)	Almost none of the requirements have been met, even if steps have been taken towards implementation.
Grading scale for inaction	
Sufficiently explained (SE)	A complete and well-reasoned explanation for the lack of implementation has been provided. If one or more of the sub-recommendations are intended to address a particular systemic risk that does not affect a particular addressee, this justification or explanation may be considered sufficient. This grade is also assigned if the reporting was delayed but the addressee provided sufficient justification for the delay.
Insufficiently explained (IE)	The explanation given for the lack of implementation is not sufficient to justify inaction.

Step II

The compliance grades for sub-recommendation A(1) were converted into numerical grades (see Table 2).

Table 2

Conversion of compliance grades into numerical grades

Compliance grade	Numerical grade
Action	
Fully compliant	1
Largely compliant	0.75
Partially compliant	0.50
Materially non-compliant	0.25
Non-compliant	0
Inaction	
Sufficiently explained	1
Insufficiently explained	0

Step III

The numerical grades were then weighted and aggregated into a single overall numerical grade showing the degree of compliance with sub-recommendation A(1). When allocating the weights, the assessment team considered the importance of each element of the sub-recommendation in the achievement of the policy objectives as outlined in Section 1 of this report.

The final weights established by the assessment team are set out in Table 3.

Table 3

Weights of key elements

Sub-recommendation A(1)	Weight
Gradual development of the EU-SCICF (final report)	90%
Reporting	10%

Step IV

The overall compliance grade was determined by converting the single numerical grade for the sub-recommendation as a whole into a final compliance grade using the conversion table below.

Table 4

Conversion of numerical grades into compliance grades

Numerical grade for sub-recommendation A(1)	Compliance grade
0.90 – 1.00	Fully compliant
0.67 – 0.90	Largely compliant
0.40 – 0.67	Partially compliant
0.158 – 0.40	Materially non-compliant
0.00 – 0.158	Non-compliant

The level of compliance was then expressed in colour-coded form.

Table 5

Colour codes for levels of compliance

Positive grades	Mid-grade	Negative grades
FC – Actions taken fully implement the recommendation		MNC – Actions taken implement only a small part of the recommendation
LC – Actions taken implement almost all of the recommendation	PC – Actions taken implement only part of the recommendation	NC – Actions taken are not in line with the nature of the recommendation
SE – No actions were taken but the addressee provided sufficient justification		IE – No actions were taken, and the addressee did not provide sufficient justification

4 Assessment reports by recommendation

This section analyses the results of the assessment. The assessment team assessed compliance by recommendation, as only sub-recommendation A(1) was subject to assessment and the addressees submitted a joint report. The assessment is therefore provided on a joint basis for sub-recommendation A(1).

The overall compliance grade attributed to each relevant authority is accompanied by the reasons for the underlying assessment and a table summarising the compliance grades.

In addition to assessing the report submitted by the addressees for sub-recommendation A(1), the assessment team engaged in an informal dialogue with the ESAs. Implementing sub-recommendation A(1) was envisaged as a gradual process. However, even though the information gathered during this process establishes the foundation for setting up the EU-SCICF, the framework was intended to be operational from January 2025, the month in which DORA becomes applicable, and set a clear path for further development in line with the compliance criteria set out.

The assessment of the final report provides feedback to the addressees of the Recommendation on the work they have done since 2022 on the gradual development of the EU-SCICF to ensure an effective EU response to systemic cyber incidents. However, the addressees' final report also forms the basis for a follow-up discussion to fast-track the process of gradually developing the EU-SCICF. Consequently, the assessment team engaged in a dialogue with the ESAs to share its preliminary findings in a timely manner. In this way, the team has been able to provide timely input for the further development and implementation of the EU-SCICF.

4.1 Sub-recommendation A(1)

The European Supervisory Authorities received the overall grade of largely compliant for sub-recommendation A(1).

4.1.1 Final report – general findings

The EU-SCICF aims to increase relevant authorities' level of preparedness to facilitate an effective EU-level coordinated response to a potentially major cyber incident that could endanger financial stability. It is intended to exercise the powers provided for in DORA. The EU-SCICF is to be operational in its initial set-

up and fulfil its intended function when DORA becomes applicable in January 2025. This assumes that the key elements for cooperation under this new framework have been agreed and their effectiveness is ensured (tested) before January 2025. Given that the Recommendation refers to the gradual development of the EU-SCICF, the assessment team also focused on the proposed future development. Therefore, the team mainly focused on whether the EU-SCICF would be able to fulfil the tasks foreseen for this framework from January 2025 and continue to evolve into an effective framework over time, taking account of testing exercises, experience and other developments. In doing so, the assessment team examined the compliance criteria in the Annex to the Recommendation that were to be considered in the development of the EU-SCICF. However, the assessment team also recognises that this list was non-exhaustive. Fulfilling all criteria on the list is not sufficient for the EU-SCICF to function.

The actions taken and described in the final report should indicate that the criteria were met by the time the final report was due. The ESAs provided a final report on the establishment of the EU-SCICF by 16 July 2024, 18 months after DORA entered into force. The final report was expected to include details on the status of the preparatory work for the gradual development of the EU-SCICF, taking into account the specified compliance criteria set out in the Annex to the Recommendation. The final report was then assessed from a risk-based perspective, with it being acknowledged that, even though a gradual development of the EU-SCICF is foreseen in the Recommendation, the compliance criteria were to be fully met at this point in time and the EU-SCICF should be operational from January 2025.

The final report does contain the theoretical structure and resource planning for the EU-SCICF, consistent with the assurances given by the ESAs during the assessment of the interim report. Compared with the interim report, a number of aspects have been developed more clearly and explicitly and show how the EU-SCICF could be used to address possible risks to financial stability stemming from cyber incidents. However, the report remains somewhat unclear as regards the concrete implementation of the theoretical framework from January 2025 onwards. The assessment team acknowledges that the EU-SCICF is to be implemented in gradual stages and was expected to be operational at the beginning of 2025, but also noted that further efforts and resources are needed to ensure its effective implementation.

The assessment team was of the opinion that the report does not fully dispel all doubts about the practical implementation of the EU-SCICF from January 2025 and its further development to ensure an effective EU-level response. The assessment of the interim report had already highlighted the importance of involving all addressees of the Recommendation for the EU-SCICF to succeed and be operational from January 2025. Although the ESAs will play a leading role in developing the EU-SCICF, responsibility for its functioning and gradual implementation lies with all the authorities involved, including, in particular, the national authorities. However, this aspect continues to be somewhat understated in the final report. While the cooperation between the ESAs and with the ESRB and the

ECB is described in detail in many places, reference to the other authorities, particularly the national authorities, is partially lacking. This concerns aspects of resource planning, where it is acknowledged that the ESAs can only comment to a limited extent. However, it also applies to other areas, such as the design of crisis management and contingency exercises. The assessment team emphasises the importance of involving all addressees of the Recommendation in the establishment of the EU-SCICF, including the relevant national authorities, and notes the importance of their continued involvement in the practical implementation of the EU-SCICF from January 2025.

The assessment of the final report serves as feedback for the addressees of the Recommendation on the work done so far, but it can also form the basis for follow-up discussions to promote the further development and timely implementation of the EU-SCICF in response to an real-life incident. Therefore, the assessment team engaged in a dialogue with the ESAs during the assessment process. It was acknowledged that the final report presents a snapshot of the efforts made towards the gradual development of the EU-SCICF after just 18 months. However, the transition to practical implementation is less advanced and the ESRB will – after this specific assessment – continue to monitor how the planned design and supporting resources work from January 2025, when the EU-SCICF should be able to respond to a crisis situation, especially given the limited resources available. In line with Recommendation C, the European Commission, based on the result of the analyses carried out in accordance with Recommendation A, should consider the appropriate measures needed to ensure the effective coordination of responses to systemic cyber incidents.

Overall, the final report provides adequate measures that ensure the compliance criteria were largely met by 16 July 2024, the date the final report on the implementation of sub-recommendation A(1) was due. However, the assessment team was not fully convinced that the EU-SCICF framework set out in the final report and the resources allocated to its development would result in an operational EU-SCICF in January 2025 and emphasised the need for adequate resources to support the timely development of the EU-SCICF as a prerequisite for supporting an effective EU-level response to systemic cyber incidents. Owing to these shortcomings, the assessment team considered the overall level of compliance with sub-recommendation A(1) of ESRB Recommendation 2021/17 to be largely compliant.

4.1.2 Reporting

The reporting was assessed as **fully compliant**, as the addressees reported the information in a timely manner.

Table 6

Grades for sub-recommendation A(1)

Gradual development of the EU-SCICF (final report)						
Fully compliant	Largely compliant	Partially compliant	Materially non-compliant	Non-compliant	Sufficiently explained	Insufficiently explained
Reporting						
Fully compliant	Largely compliant	Partially compliant	Materially non-compliant	Non-compliant	Sufficiently explained	Insufficiently explained
Overall grade for sub-recommendation A(1)						
Fully compliant	Largely compliant	Partially compliant	Materially non-compliant	Non-compliant	Sufficiently explained	Insufficiently explained

5 Overall results

For sub-recommendation A(1) the ESAs were assessed as largely compliant.

Table 7

Sub-recommendation A(1) - Gradual development of the EU-SCICF (final report)

Addressee	Sub-recommendation A(1)	Reporting	OVERALL ASSESSMENT GRADE
ESAs	Largely compliant	Fully compliant	Largely compliant

6 Conclusions

The assessment team assessed the level of compliance with sub-recommendation A(1) of Recommendation ESRB/2021/17 on a pan-European systemic cyber incident coordination framework for relevant authorities on the basis of the ESAs' final report produced in accordance with sub-recommendation A(1).

The Recommendation aims to establish a pan-European systemic cyber incident coordination framework (EU-SCICF). The objective is to increase the level of preparedness of financial authorities in the EU and to define a coherent, and thus more effective, response to cyber incidents, thereby mitigating the risk of a coordination failure. Therefore, sub-recommendation A(1) recommends that the ESAs, together with the ECB, the ESRB and relevant national authorities, start preparing for the gradual development of an effective EU-level coordinated response in the event of a major cross-border cyber incident or related threat that could have a systemic impact on the EU's financial sector. Preparatory work towards an EU-level coordinated response should entail the gradual development of an EU-SCICF.

The overall level of compliance with Recommendation ESRB/2021/17 is good. For sub-recommendation A(1) all addressees were assessed as "largely compliant".

While the ESAs were assessed as largely compliant on the basis of their final report on the implementation of sub-recommendation A(1), the assessment team had some general remarks and identified points that should be considered in the ongoing development of the EU-SCICF to ensure an effective coordinated EU-level response to cyber incidents. In particular, it was not always clear how individual areas identified in the compliance criteria will be further developed, as some concrete steps to be taken are not indicated in the final report. However, the basic features of the EU-SCICF were laid out in the report, albeit not in full detail.

Two points identified as areas for improvement are (i) ensuring that the necessary resources are either in place or that those responsible for allocating the necessary resources in the European and national authorities seek to address any constraints, and (ii) the need to ensure that the EU-SCICIF can be activated and operational from January 2025 onwards and further developed in a timely manner to ensure a robust framework that supports an effective EU-level response. All participating authorities should also be involved in the practical implementation of the EU-SCICF from January 2025. However, the topic of asking the relevant national authorities to be involved in the process continues to be somewhat understated in the ESAs' final report. This concerns aspects of resource planning, where it is acknowledged that the ESAs that can only comment to a certain extent, but it also applies to other areas which are likely to require increased resources, such as the running of crisis management and contingency exercises at an earlier stage than envisaged in the report to help develop the framework.

Therefore, the assessment team engaged in a dialogue with the ESAs during the assessment, outlining the concerns mentioned. The assessment team acknowledged that the EU-SCICF is to be implemented gradually and is expected to be operational from the beginning of 2025, but also noted that further efforts and resources are needed to ensure it is implemented effectively. This applies in particular to the testing of the framework and its processes as soon as it becomes operational in January 2025. Such tests are indispensable for a framework of this kind that aims to improve coordination between the relevant authorities. It would therefore be unacceptable to wait for a crisis to test the ability of the framework to function under stress.

Although a number of aspects are developed more clearly and explicitly than in the interim report and show how the EU-SCICF could be used to address possible risks to financial stability stemming from cyberattacks, the final report remains somewhat unclear when it comes to the concrete implementation of the theoretical framework from January 2025. In conclusion, the design and set-up of the EU-SCICF, as explained in the report submitted by the ESAs, are well advanced on the conceptual level. However, the transition to practical implementation is less advanced and the ESRB will – following this specific assessment – continue to monitor how the planned design and supporting resources work from January 2025, when the EU-SCICF should be able to respond to a crisis situation, especially given the limited resources available. In this context, the assessment team would encourage the addressees to set more ambitious goals for the development of the EU-SCICF, with a view to making the response framework stronger and more effective. While this may incur higher costs in terms of resources and IT systems, it would enable all parties involved to make the necessary decisions on a transparent basis. This is the only way to ensure that the EU-SCICF is operational from January 2025 and then further developed into a crucial coordination mechanism in the management and mitigation of systemic risks posed by cyber incidents.

Annexes

Annex I: Composition of the assessment team

The assessment team was approved by the Advisory Technical Committee of the ESRB via written procedure (ATC/WP/2024/045) and chaired by **Jari Friebel**.

Aaron Goldmann	Bundesanstalt für Finanzdienstleistungsaufsicht
Aoife Langford	Central Bank of Ireland
Janina Schuh	Bundesanstalt für Finanzdienstleistungsaufsicht
Jari Friebel (Chair of the assessment team)	Deutsche Bundesbank
Pascal Jourdain	Banque de France
Vadim Kravchenko	European Central Bank
Joana Vaz Baptista	ESRB Secretariat
Maximilian Liegler	ESRB Secretariat
Margarida Cepeda Lopes	ESRB Secretariat

Annex II: Implementation standards for Recommendation ESRB/2021/17

Table A1

Sub-recommendation A(1) - Gradual development of the EU-SCICF (final report)

	Gradual development of the EU-SCICF (final report)	
Positive grades	**Fully compliant (FC)** – Actions taken fully implement the Recommendation	• In the course of the preparations the addressees have demonstrated the actions they have taken to date in response to the Recommendation and compliance criteria and provided sufficient assurance that they will ensure compliance with the criteria which would enable the EU-SCICF to be operational and fulfilling its intended function by January 2025, when DORA comes into effect. • In the course of the preparations the addressees considered[6] all the aspects listed in the Annex to the Recommendation, and in particular: (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; and (o) ensuring effective communication and countermeasures against disinformation.
	Sufficiently explained (SE) – No actions were taken but the addressee provided sufficient justification	• The addressees have not yet started preparations for the gradual development of an effective EU-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the EU's financial sector but have provided sufficient justification.
	Largely compliant (LC) – Actions taken implement almost all of the Recommendation	• In the course of the preparations the addressees have demonstrated the actions they have taken to date in response to the Recommendation and compliance criteria and provided sufficient assurance that it will ensure compliance with the criteria that would enable the EU-SCICF to be operational and fulfilling its intended function by January 2025, when DORA comes into effect. • However, not all criteria listed in the Annex to the Recommendation were considered to be fully met, and the assessment revealed minor/non-material deviations from the aspects proposed in the Annex. These raised minor doubts as to whether the framework set out in the final report would enable a fully operational EU-SCICF in January 2025.
Mid-grade	**Partially compliant (PC)** – Actions taken implement only part of the Recommendation	• The addressees have started preparations for the gradual development of an effective EU-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the EU's financial sector, but the actions taken do not provide sufficient assurance that they will ensure compliance with the criteria that would enable the EU-SCICF to be operational and fulfilling its intended function by January 2025, when DORA comes into effect. • Most of the criteria listed in the Annex to the Recommendation were considered to be fully met. However, the assessment revealed some material deviations from the aspects proposed in the Annex. These raised doubts as to whether the framework set out in the final report would enable a fully operational EU-SCICF in January 2025.
	Materially non-compliant (MNC) – Actions taken implement only a small part of the Recommendation	• The addressees have started preparations for the gradual development of an effective EU-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the EU's financial sector, but the actions taken do not provide sufficient assurance that they will ensure compliance with the criteria that would enable the EU-SCICF to be operational and fulfilling its intended function by January 2025, when DORA comes into effect. • Only some of the criteria listed in the Annex to the Recommendation were considered to be fully met, and the assessment revealed material deviations from the aspects proposed in the Annex. These raised serious doubts as to whether the framework set out in the final report would enable a fully operational EU-SCICF in January 2025.

6 Meaning included or provided a reasonable explanation as to why they were not included.

		Gradual development of the EU-SCICF (final report)
Negative grades	**Non-compliant (NC)** – Actions taken are not in line with the nature of the Recommendation	• The addressees have started preparations for the gradual development of an effective EU-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the EU's financial sector but, based on the actions taken, it does not seem likely that the compliance criteria will be met by the time the final report is due. • None or only very few of the aspects in the Annex to the Recommendation were considered in the report or a decent number of the aspects in the Annex to the Recommendation were considered, but significant aspects were not, and the final report does not indicate that they will be considered in the future.
	[Inaction] Insufficiently explained (IE) – No action was taken, and the addressee failed to provide sufficient justification	• The addressees have not started preparations for the gradual development of an effective EU-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the EU's financial sector and did not provide any further justification for inaction.

Table A2

Reporting as regards sub-recommendation A(1)

		Reporting by 16 July 2024
Positive grades	**Fully compliant (FC)** – Actions taken fully implement the Recommendation	• The addressees have provided a final report that includes details about the current status of the gradual development of the EU-SCICF for the ESAs, the ECB, the ESRB and relevant national authorities. The addressees therefore submitted the fully completed template or an alternative report to the ESRB via the ESRB Secretariat by 16 July 2024. • Alternatively, the addressees have collaborated with the other addressees and submitted a joint reporting template or an alternative joint report to the ESRB via the ESRB Secretariat by 16 July 2024.
	Sufficiently explained (SE) – The reporting was delayed but the addressee provided sufficient justification	• The addressees submitted the fully completed (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat later than 16 July 2024 but have sufficiently explained the delay.
	Largely compliant (LC) – Actions taken implement almost all of the Recommendation	• The addressees submitted the (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat by 16 July 2024, but some non-material information[7] is missing.
Mid-grade	**Partially compliant (PC)** – Actions taken implement only part of the Recommendation	• The addressees submitted the (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat by 16 July 2024, but some essential information is missing.
	Materially non-compliant (MNC) – Actions taken implement only a small part of the Recommendation	• The addressees submitted the (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat by 16 July 2024, but a lot of essential information is missing.
Negative grades	**Non-compliant (NC)** – Actions taken are not in line with the nature of the Recommendation	• The addressees submitted the (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat by 16 July 2024, but most of the essential information is missing.
	[Inaction] Insufficiently explained (IE) – No action was taken, and the addressee failed to provide sufficient justification	• The addressees did not submit a final report to the ESRB Secretariat by 16 July 2024 and did not provide any justification for inaction, or the addressees did not submit templates to the ESRB Secretariat by 16 July 2024. They provided justification for inaction, but this is inadequate.

[7] This is without prejudice to the requirements above. This refers instead to information determined in the template.

Annex III: Overall table of results

Table A3

Sub-recommendation A(1) - Gradual development of the EU-SCICF (final report)

Addressee	Sub-recommendation A(1)	Reporting	OVERALL ASSESSMENT GRADE
ESAs	Largely compliant	Fully compliant	Largely compliant

Imprint and acknowledgements

This compliance report is based on the results of the assessment conducted by the assessment team, chaired by Jari Friebel, and was prepared by:

Aaron Goldmann
Bundesanstalt für Finanzdienstleistungsaufsicht

Aoife Langford
Central Bank of Ireland

Janina Schuh
Bundesanstalt für Finanzdienstleistungsaufsicht

Jari Friebel (Chair of the assessment team)
Deutsche Bundesbank

Pascal Jourdain
Banque de France

Vadim Kravchenko
European Central Bank

Joana Vaz Baptista
ESRB Secretariat

Margarida Cepeda Lopes
ESRB Secretariat

Maximilian Liegler
ESRB Secretariat

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.esrb.europa.eu

For specific terminology please refer to the ESRB glossary (available in English only).

PDF ISBN 978-92-9472-426-7, doi:10.2849/7208860, DT-01-25-011-EN-N