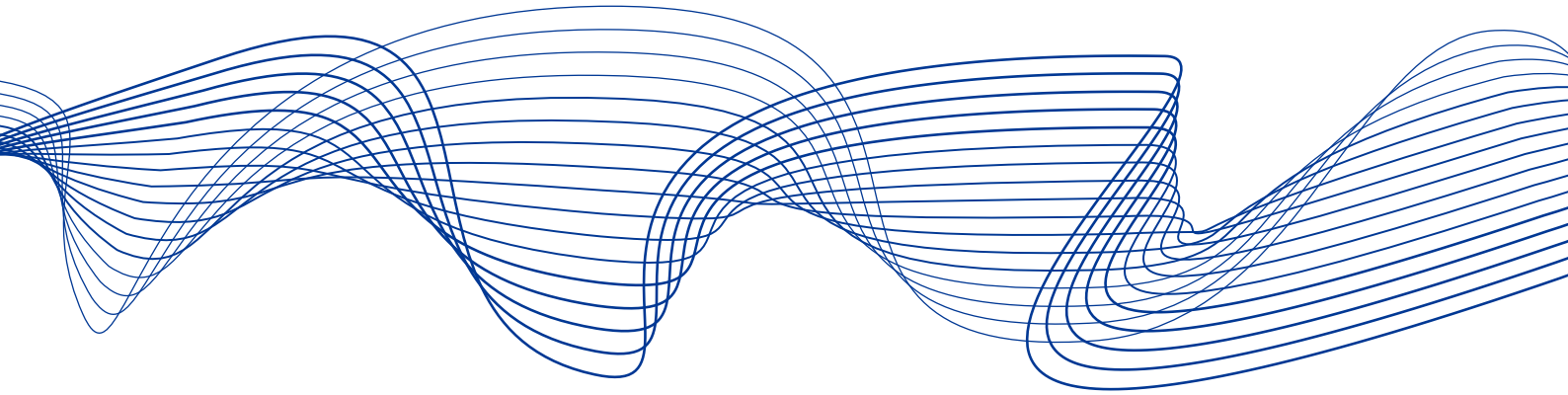
ESRB
European Systemic Risk Board
European System of Financial Supervision

Summary Compliance report

June 2026

Sub-recommendation A(2) of the 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] **(the "Recommendation").** This compliance report presents the outcome of the assessment of compliance concerning the implementation of sub-recommendation A(2) 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 their 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 deliver, by 16 July 2025, a final report to the European Parliament, the Council, the European Commission and the ESRB on the implementation of sub-recommendation A(2).[3] Sub-recommendation A(2) calls on the ESAs to undertake, in consultation with the European Central Bank (ECB) and the ESRB, a mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF. The ESAs delivered the final report on the mapping of current impediments by 16 July 2025. Other information provided by the addressees during the assessment process was also included in the assessment of compliance. This report reflects the implementation status as of December 2025.

The input from the addressees was examined by a four-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[4] (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

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(2), titled "EU-SCICF: A pan-European Systemic Cyber Incident Coordination Framework", was delivered to the European Parliament, the Council, the European Commission and the ESRB by 16 July 2025.

4 "Handbook on the assessment of compliance with ESRB recommendations", ESRB Secretariat, ESRB, April 2016.

for each key element of the Recommendation on the basis of the corresponding objectives (see Annex II); and the principle of proportionality.

Overall, the assessment team found that the addressees were largely compliant with sub-recommendation A(2). 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 drafted by the assessment team and used to assess compliance with sub-recommendation A(2). Part 3 contains the assessments of compliance with sub-recommendation A(2). Part 4 discusses the overall findings of the assessment. Lastly, Part 5 concludes the assessment of sub-recommendation A(2). Annex I lists the members of the assessment team and Annex II contains the implementation standards.

2 Policy objectives

Cyber incidents, including cyberattacks, may pose a systemic risk to the financial system, given their potential to disrupt critical financial services and operations and thereby 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 erode confidence in the financial system. If the financial system is unable to absorb these shocks, financial stability could be jeopardised, potentially giving rise to a systemic cyber crisis.[5]

Major cyber incidents can move fast and propagate rapidly, calling for an effective response from the relevant authorities 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 consider the scale and impact of operational disruptions, as these might influence the choice of macroprudential tools. Likewise, financial stability considerations can influence 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. Such coordination can support the prompt assessment of the impact of a major cyber incident on financial stability, help maintain confidence in the financial system and limit 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 behind such a mechanism are to increase the 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. 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 will likely not be limited to the EU or may be triggered outside the EU and might therefore require a global response as well as coordination and cooperation 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 this 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 do so by asking relevant authorities to

[5] "Systemic cyber risk", ESRB, 2020.

prepare for interactions both with each other and with other authorities they might not typically interact with when responding to major cyber incidents, with a view to mitigating the potential negative effects on financial stability.[6]

The Recommendation and the assessment of the addressees' implementation of it recognise that cyber risk is not confined to the financial system. A number of agencies have been set up and cyber incident response initiatives have been developed to minimise the risks of cyberattacks. The EU-SCICF to be developed under the Recommendation will address threats to financial stability; it will coexist with other fora but with a clear focus on financial stability aspects not covered by such existing frameworks.

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(2), for which the reporting deadline was 16 July 2025.

Sub-recommendation A(2) calls on the ESAs, in the context of the gradual development of an effective EU-level coordinated cyber incident response, to undertake, in consultation with the ECB and the ESRB, a mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF.

The Recommendation, which was adopted on 2 December 2021 and published in the Official Journal on 25 March 2022, aims to ensure that the EU-SCICF is operational and able to fulfil its intended function by January 2025, when the Digital Operational Resilience Act (DORA) came into effect. It is therefore an important element in preventing, or at least mitigating, risks to financial stability that may arise from cyber incidents.

Sub-recommendation A(2) acknowledges that there may be obstacles that could make it harder for the ESAs and relevant authorities to further develop the EU-SCICF and share relevant information through communication channels in the event of a major cyber incident. Therefore, in implementing sub-recommendation A(2), the addressees are asked to map and analyse such impediments. This analysis is an important step in informing any further action, either of a legislative nature or in the form of other supporting initiatives that the European Commission may take in the post-DORA implementation stage.

As already underlined by the assessment team in the compliance report for sub-recommendation A(1), the assessment team recognises that the time frames established in the Recommendation may not consider all impediments that could affect the ability of the ESAs and relevant competent authorities to establish a fully-fledged EU-SCICF. This report therefore aims to examine the mapping and analysis of the impediments identified or encountered by the ESAs in

[6] "Mitigating systemic cyber risk", ESRB, January 2022.

the context of the implementation of sub-recommendation A(2), and to contribute to the ongoing efforts of the ESAs, in consultation with the ECB and the ESRB, to develop an effective and operational EU-SCICF within the time frame envisaged in the Recommendation, while acknowledging that the framework will continue to evolve.

3 Assessment methodology

The implementation of the Recommendation was assessed 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 could 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 could properly justify that inaction. On that basis, the assessment team then analysed the information provided and assessed whether the action taken was successful in achieving the objectives of each recommendation or whether the justification provided for inaction was sufficient. Following this analysis, a final compliance grade was 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** – the level of 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 from which they come;
- **effective dialogue** – communication with the addressees is essential to fill in information gaps regarding compliance;
- **principle of proportionality** – actions to be taken by the addressees are country-specific and proportionate to the intensity of risks targeted by the Recommendation in the Member State concerned;
- **ultimate objective** – prevention and mitigation of systemic risks to financial stability in the European Union.

Compliance was assessed by recommendation. Since this assessment focuses on sub-recommendation A(2) only and the addressees have submitted a joint report, the assessment team decided to assess the implementation of, and compliance with, sub-recommendation A(2) jointly. This approach also ensured compliance with the four-eyes principle throughout the assessment process.

The assessment was based on the submission by the addressees of a final report on the analysis of impediments and barriers to the effective development of the EU-SCICF by the reporting deadline of 16 July 2025, as well as on further dialogue between the assessment team and the addressees in December 2025.

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 best practices established in previous assessments of compliance with ESRB recommendations. In contrast to sub-recommendation A(1), no specific assessment criteria beyond formal ones (e.g. “consultation with the ECB and the ESRB”, “mapping and subsequent analysis”) were specified in the Annex to the Recommendation for sub-recommendation A(2). However, due to their relevance, the assessment team took due account of the implementation criteria set out in Section 2(2) to aid its assessment of the mapping and analysis of the impediments to the EU-SCICF’s development. While conducting the assessment, the assessment team analysed the content and substance of the actions taken by each addressee to determine 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). In this regard, the assessment team was also guided by the fact that the analysis to be carried out by the addressees when implementing sub-recommendation A(2) is an important step in informing any further action, either of a legislative nature or in the form of any other supporting initiatives that the European Commission may take in the post-DORA implementation stage.

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:

- analysis of the impediments and barriers for the development of a pan-European systemic cyber incident coordination framework (EU-SCICF) (final report);
- completeness and timeliness of reporting.

Sub-recommendation A(2) called on the addressees to analyse the impediments and barriers for the development of the EU-SCICF. In response, the addressees delivered a final report, which is the subject of this assessment.

3.2 Grading methodology

The assessment team followed a four-step grading methodology to assign a grade to each addressee regarding its compliance with sub-recommendation A(2). This methodology is necessary to ensure absolute transparency in assigning

the single overall compliance grade and a high level of objectivity throughout the assessment process. At the same time, it allows for high-quality expert judgement that can easily be identified and reviewed to understand the rationale behind the allocation of particular overall grades.

Step I

The content of sub-recommendation A(2) was first assessed and graded on the basis of the assessment criteria – in accordance with the established implementation standard – in terms of each addressee's action or inaction . The full grading scale is given 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, with only negligible requirements 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)	The 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 the inaction.

Step II

The compliance grades for sub-recommendation A(2) were subsequently converted into numerical grades, as follows:

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(2). When allocating the weights, the assessment team took into consideration the importance of each element of the recommendation in relation to the achievement of the policy objectives as outlined in Section 1 of this report.

The final weights established by the assessment team are as follows:

Table 3
Weights of key elements

Sub-Recommendation A(2)	Weight
Analysis of impediments and barriers (final report)	90%
Reporting	10%

Step IV

Lastly, the overall compliance grade was determined by converting the single numerical grade for the entire Recommendation into a final compliance grade using the conversion table set out below.

Table 4

Conversion of numerical grades into compliance grades

Numerical grade for sub-recommendation A(2)	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 showing 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 consistent 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

The assessment team assessed compliance by recommendation, as only sub-recommendation A(2) was to be assessed, and a joint report prepared by the addressees was delivered. The assessment is therefore presented on a joint basis for sub-recommendation A(2).

This section analyses the results of the assessment. 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 delivered by the addressees for sub-recommendation A(2), the assessment team engaged with the ESAs in an informal dialogue. The assessment of the final report provides useful feedback to the addressees of the Recommendation on the work carried out so far in detecting and analysing the impediments and barriers to the development of the EU-SCICF, thereby supporting the development of an effective EU response to systemic cyber incidents. According to Recital 16 of the Recommendation, this report also serves as the basis for the European Commission to consider the appropriate measures needed to ensure effective coordination of responses to systemic cyber incidents, in light of the results of the analysis. Consequently, the dialogue with the ESAs was initiated to identify remaining gaps, align approaches and secure their input when designing and implementing the framework. This approach ensures a coherent, coordinated and well-informed foundation for the further development and implementation of the EU-SCICF.

4.1 Sub-recommendation A(2)

The European Supervisory Authorities (ESAs) received the overall grade of largely compliant for sub-recommendation A(2).

4.1.1 Final report – general findings

The objective of the EU-SCICF is to increase the level of preparedness among relevant authorities to facilitate an effective, EU-level coordinated response to a major cyber incident that could threaten financial stability. Given that the Recommendation refers to the gradual development of the EU-SCICF, the assessment team acknowledges the progress made to date. This includes the establishment of points of contact and the successful execution of drills and a workshop, all of which are essential steps towards operational readiness. Accordingly, the assessment team's main focus is now on examining the extent to

which the report maps and analyses current impediments, legal barriers and other operational challenges affecting the effective development of the EU-SCICF.

The report builds on the A(1) report on the theoretical structure, resource planning and gradual implementation of the EU-SCICF. It presents a mapping and analysis of impediments and legal and operational barriers and is intended to complement the efforts and resources already set out in the A(1) report, which are needed to ensure the effective implementation of the EU-SCICF.

The assessment of the final report serves as feedback for the addressees of the Recommendation on the work carried out so far in mapping and analysing the impediments and operational barriers to the EU-SCICF, while forming the basis for a follow-up discussion in order to promote the further development and timely implementation of the EU-SCICF in response to a real-life incident. Accordingly, the assessment team engaged in dialogue with the ESAs over the course of the assessment. It was acknowledged that, while the final report presents the impediments detected through the current work on the gradual development of the EU-SCICF, this is based on work carried out over a short time frame and with limited operational experience. Building on this assessment, and in line with Recommendation C, the European Commission shall, on the basis of the results of the analysis carried out in accordance with Recommendation A, consider the appropriate measures needed to ensure effective coordination of responses to systemic cyber incidents.

Overall, the final report adequately addresses the mapping and analysis of the impediments and legal and operational barriers that had been identified by the time the final report on the implementation of sub-recommendation A(2) was due, i.e. 16 July 2025. However, given the limited operational experience gained to date from exercises or real-life incidents, as outlined above, the mapping and analysis in the report remains relatively high level, and the report lacks the extra depth and insight needed to ensure that all impediments have been identified and comprehensively analysed. This makes it difficult to fully analyse the obstacles, as practical insights have not been taken into account, partly owing again to limited experience in conducting exercises and tests. Therefore, the assessment team considered the overall level of compliance with sub-recommendation A(2) of ESRB Recommendation 2021/17 to be largely compliant.

The assessment team recognises that, as noted in the report, the findings presented are based on limited operational experience of the EU-SCICF. It also acknowledges that additional obstacles may emerge during future tests, exercises or real-life events (as indicated in Section 2, point 7 of the report). Consequently, the report may not fully capture all current impediments that could undermine the effective implementation of the EU-SCICF. The assessment team therefore encourages the addressees to continue to examine and report, in particular to the European Commission, any obstacles they may encounter, in the further development of the EU-SCICF.

With regard to sub-recommendation A(2), which emphasises the identification of impediments, the assessment team notes that the report primarily

highlights hurdles rather than impediments. The assessment team considers this distinction between hurdles and impediments to be significant, including in light of the wording of the Recommendation, as it believes that hurdles generally represent challenges that can be overcome, often as part of a process or expected development, whereas impediments suggest more severe or inherent barriers that are harder to address and may significantly slow progress. The assessment team is therefore of the view that, while there are currently no impediments preventing the EU-SCICF from operating, there are nevertheless hurdles that require attention to ensure that the framework can effectively meet its key objective. This objective, as stated in Recital 9 of the Recommendation, is to enable a coordinated, EU-level response in the event of a major cross-border ICT-related incident with systemic implications for the EU's financial sector.

Furthermore, the assessment team welcomes the fact that the report provides proposals for addressing the hurdles identified. These proposals are directed at various stakeholders, including the European Commission, the ESAs, competent authorities, and potentially other relevant entities. The inclusion of these recommendations demonstrates a proactive approach among the addressees to overcoming the challenges and ensuring the EU-SCICF can operate effectively.

In summary, the assessment team appreciates the progress achieved thus far in the EU-SCICF's development, acknowledges the limitations of the report in identifying all potential obstacles, and supports the proactive recommendations aimed at addressing the hurdles identified to ensure the framework meets its intended purpose.

4.1.2 Reporting

The reporting was assessed as "fully compliant", as the addressees reported the information in due course.

Table 6

Grades for sub-recommendation A(2)

Mapping and analysis of current impediments and legal and other operational barriers (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(2)						
Fully compliant	Largely compliant	Partially compliant	Materially non-compliant	Non-compliant	Sufficiently explained	Insufficiently explained

5 Overall results

For sub-recommendation A(2), the ESAs were assessed as "largely compliant" (LC).

Table 7

Sub-recommendation A(2) – Mapping and analysis of current impediments and legal and other operational barriers (final report)

Addressee	Sub-Recommendation A(2)	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(2) of Recommendation ESRB/2021/17 on a pan-European systemic cyber incident coordination framework for relevant authorities in view of the ESAs' final report, in accordance with sub-recommendation A(2).

The Recommendation aims to establish a pan-European systemic cyber incident coordination framework (EU-SCICF). The objective behind such a mechanism 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. More precisely, sub-recommendation A(2) calls on the ESAs, in consultation with the ECB and the ESRB, to undertake a mapping and subsequent analysis of current impediments and of legal and other operational barriers to the effective development of the EU-SCICF.

The overall level of compliance with Recommendation ESRB/2021/17 is high. For sub-recommendation A(2), all addressees were assessed as "largely compliant" (LC).

While the ESAs were assessed as largely compliant in light of their final report on the implementation of sub-recommendation A(2), the assessment team made a number of general remarks and identified certain points meriting further consideration in the ongoing mapping and analysis of impediments and hurdles to ensure an effective, coordinated EU-level response to cyber incidents. In particular, further specificity would have been useful in relation to certain hurdles, including information sharing and the interaction between existing frameworks. In this respect, the final report would have benefited from further practical insights and therefore remains rather theoretical in nature. Moreover, certain overlaps were identified across hurdles (e.g. in relation to mandates and information sharing), suggesting that more horizontal action at EU level could be effective in addressing multiple issues simultaneously. While the basic impediments to the EU-SCICF and the commitment to continue its development are set out in the report, the practical implications of the identified impediments need to be further elaborated in order to assess their impact on the effectiveness of the EU-SCICF and to support the effective operationalisation of the framework.

The impediments and barriers identified in the report as outstanding are considered to require further work, as they constitute hurdles that call for concrete remedial action. In some instances, however, additional mapping and analysis would have been beneficial to provide greater specificity and granularity regarding the hurdles that need to be addressed, particularly in relation to information-sharing arrangements.

In other cases, it appears that the nature of the hurdle may relate more to a lack of clarity concerning the interaction between different frameworks than to actual overlaps between them. This distinction is important, as it may imply the

need for additional or slightly different mitigating actions, such as measures focused on building awareness and improving our understanding of how the various frameworks are meant to work together in practice.

At the same time, there appear to be overlaps between several of the hurdles identified in the report. For example, issues relating to mandates are raised in multiple areas, as is the topic of information sharing. This suggests that certain horizontal actions could help to address more than one hurdle simultaneously. For example, the development of a clear and shared mandate for the EU-SCICF could help resolve some of the issues identified in relation to the interaction between the various existing frameworks. However, the call for a clear mandate could have been supplemented by further arguments highlighting the advantages of establishing a legal basis for a coordination framework such as the EU-SCICF. The assessment team is concerned that the level of detail provided in the report may not be sufficient to support the initiation of a legislative initiative at European level for the creation of such a mandate without further engagement between the European Commission and the ESAs.

At this stage, it is difficult to determine whether all current impediments and hurdles have been fully mapped, given that the assessment has largely been conducted on a theoretical basis, without the benefit of extensive practical experience from either exercises or real-life invocations. In light of this, and taking into account the issues outlined above, the work undertaken to date under sub-Recommendation A(2) is assessed as “largely compliant”. However, the assessment team notes that additional resources should be allocated to support the further development and operationalisation of the EU-SCICF. This would also allow the identification and review of impediments and hurdles to be pursued on an ongoing, iterative basis as the framework evolves.

In view of the early stage of development of the EU-SCICF, the assessment team welcomes that the final report explicitly commits to continuing efforts to establish an EU response capacity for dealing with systemic cyber incidents. The assessment team also welcomes that the ESAs are already considering measures within their remit to mitigate the hurdles identified, even while acknowledging that such measures may not, on their own, be entirely sufficient (see Section 3, “Conclusions”, of the report). A key tool in this regard will be the design and conduct of targeted exercises, which can be used both to test and refine the framework and to further identify, assess and address practical hurdles. For example, exercises could help to determine what specific types of information need to be shared in different scenarios and how the EU-SCICF should interact with existing Union-level and national frameworks. In the absence of real-life invocations, such targeted exercises are indispensable for the ongoing assessment of impediments and for the progressive strengthening of the framework.

Annexes

Annex I: Composition of the assessment team

The assessment team was endorsed by the Advisory Technical Committee of the ESRB via Written Procedure ATC/WP/2025/041 and was chaired by **Jari Friebel**, who represented and headed the assessment team.

Aaron Goldmann	Bundesanstalt für Finanzdienstleistungsaufsicht
Aoife Langford	Central Bank of Ireland
Jari Friebel	Deutsche Bundesbank
Pascal Jourdain	Banque de France
Joana Vaz Baptista	ESRB Secretariat
Elpis Pentheroudaki	ESRB Secretariat
Maximilian Liegler	ESRB Secretariat

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

Table A1

Sub-recommendation A(2) – Analysis of impediments and barriers for the development of a pan-European systemic cyber incident coordination framework (EU-SCICF) (final report)

	Analysis of impediments and barriers for the development of a pan-European systemic cyber incident coordination framework (EU-SCICF) (final report)	
Positive grades	**Fully compliant (FC)** – Actions taken fully implement the Recommendation	In view of sub-recommendation A(1), and in consultation with the ECB and the ESRB, the addressee has undertaken a mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF, and has provided a sufficiently clear and adequate level of mapping and analytical explanations of those impediments, including legal and other operational barriers. More analytically, the addressee has adequately described the hurdles, elaborated on the obstacles impeding the full and effective functioning of the EU-SCICF, and engaged in substantial analysis, presenting their consequences, the benefits of their removal and, as the case may be, actionable suggestions. Given that the report is meant to provide feedback for the European Commission, the ESAs have provided a clear and sufficiently adequate and analytical mapping of the obstacles identified.
	Sufficiently explained (SE) – No actions were taken but the addressee provided sufficient justification	The addressee has not yet undertaken a mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF, in consultation with the ECB and the ESRB, but has provided sufficient justification.
	Largely compliant (LC) – Actions taken implement almost all of the Recommendation	In view of sub-recommendation A(1), and in consultation with the ECB and the ESRB, the addressee has undertaken a mapping and subsequent analysis of current impediments, legal and other operational barriers to the effective development of the EU-SCICF, and has provided a clear mapping and analytical explanation of the current impediments, including legal and other operational barriers, to the further effective development of the EU-SCICF. However, the report remains at a higher level of mapping and analysis and lacks the extra depth and detail that could be leveraged by the addressee at this stage.
Mid-grade	**Partially compliant (PC)** – Actions taken implement only part of the Recommendation	The addressee has undertaken a mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF. However, the actions and analysis undertaken so far do not provide adequate assurance that a sufficiently adequate mapping with clear explanations of the impediments are provided by the time of the final report.
	Materially non-compliant (MNC) – Actions taken implement only a small part of the Recommendation	The addressee has undertaken a mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF. However, the actions taken do not provide sufficient assurance that a wide enough analysis of the impediments to the framework's development, as envisaged under sub-recommendation A(2), has been undertaken, and the analysis provided lacks clear explanations of the impediments detected.
Negative grades	**Non-compliant (NC)** – Actions taken are not in line with the nature of the Recommendation	The addressee has undertaken a mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF. However, based on the actions taken, it does not seem likely that the analysis of the impediments to the framework's development, and the explanations given, provide any adequate and actionable feedback as envisaged in the report. Significant aspects/areas of potential impediments to the network's development have not been examined 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 addressee has not yet undertaken a mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF, and has failed to provide any justification for its inaction.

Table A2

Reporting as regards sub-recommendation A(2)

	Reporting by 16 July 2025	
Positive grades	**Fully compliant (FC)** – Actions taken fully implement the Recommendation	The addressee has provided a final report which, in line with sub-recommendation A(2), provides details of the mapping and subsequent analysis of current impediments, including legal and other operational barriers, to the effective development of the EU-SCICF for the ESAs, the ECB, the ESRB and relevant national authorities. Therefore, the addressee submitted the fully completed template or an alternative report to the ESRB via the ESRB Secretariat by 16 July 2025. Alternatively, the addressee has collaborated with the other addressees and submitted a joint report or an alternative joint report to the ESRB via the ESRB Secretariat by 16 July 2025.
	Sufficiently explained (SE) – The report was delayed, but the addressee provided sufficient justification	The addressee submitted the fully completed (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat later than 16 July 2025, but has provided a sufficient explanation for the delay.
	Largely compliant (LC) – Actions taken implement almost all of the Recommendation	While the addressee submitted the (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat by 16 July 2025, some non-material information is missing.
Mid-grade	**Partially compliant (PC)** – Actions taken implement only part of the Recommendation	In the course of the preparations, the addressee has demonstrated the actions taken to date in response to the Recommendation and compliance criteria and has provided sufficient assurance that most of the compliance criteria were met by the time the final report was due.
	Materially non-compliant (MNC) – Actions taken implement only a small part of the Recommendation	While the addressee has submitted the (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat by 16 July 2025, much of the essential information is missing.
Negative grades	**Non-compliant (NC)** – Actions taken are not in line with the nature of the Recommendation	While the addressee submitted the (joint) template or an alternative (joint) report to the ESRB via the ESRB Secretariat by 16 July 2025, most of the essential information is missing.
	[Inaction] Insufficiently explained (IE) – No action was taken and the addressee failed to provide sufficient justification	The addressee did not submit a final report to the ESRB Secretariat by 16 July 2025 and failed to provide any justification for its inaction, or the addressee failed to submit its report to the ESRB Secretariat by 16 July 2025, but provided justification for its inaction which, however, proved to be inadequate.

Annex III: Overall table of results

Table A3

Sub-recommendation A(2) – analysis of the impediments and barriers to the development of a pan-European systemic cyber incident coordination framework (EU-SCICF) (final report)

Addressee	Sub-Recommendation A(2)	Reporting	Overall assessment grade
ESAs	Largely compliant	Fully compliant	Largely compliant

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

Jari Friebel (Chair of the assessment team)
Deutsche Bundesbank

Pascal Jourdain
Banque de France

Joana Vaz Baptista
ESRB Secretariat

Elpis Pentheroudaki
ESRB Secretariat

Maximilian Liegler
ESRB Secretariat

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

The cut-off date for the data included in this report was 10 December 2025

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

PDF ISBN 978-92-9472-443-4, ISSN 2529-3273, doi:10.2849/1640899, DT-01-26-007-EN-N