JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC/GL/2024/36

06/11/2024

Joint Guidelines

on the oversight cooperation and information exchange between the ESAs and the competent authorities under Regulation (EU) 2022/2554

Status of the Guidelines

These Guidelines are issued pursuant to Article 16 of Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority); Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority); and Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority) (the ESAs' Regulations)[1].

The European Supervisory Authorities (ESAs) issue these Guidelines on the basis of Article 32(7) of Regulation (EU) 2022/2554 ("DORA")[2], according to which the ESAs shall issue guidelines on the cooperation between the ESAs and the competent authorities covering:

- the detailed procedures and conditions for the allocation and execution of tasks between competent authorities and the ESAs; and
- the details on the exchanges of information which are necessary for competent authorities to ensure the follow–up of recommendations addressed to ICT third party service providers to financial entities designated as critical.

Reporting requirements

In accordance with Article 16(3) of the ESAs' Regulations, competent authorities shall make every effort to comply with the Guidelines. Competent authorities must notify the respective ESA whether they comply or intend to comply with these Guidelines, or otherwise with reasons for non-compliance, within two months after the issuance of the translated versions of the Guidelines. In the absence of any notification by this deadline, competent authorities will be considered by the respective ESA to be non-compliant. Notifications should be sent to compliance@eba.europa.eu, CoE@eiopa.europa.eu and DORA@esma.europa.eu with the reference 'JC/GL/2024/36'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Notifications will be published on the ESAs' websites, in line with Article 16(3).

[1] 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.12-47). Regulation (EU) No 1094/2010 of the European Parliament and of the Council of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p.48-83).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. 84-119).

[2] Regulation (EU) No 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector amending Regulations (EC) No 1060/2009, (EU)No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p.01-79).

Section 1: General considerations

General aims and principles

These Guidelines aim at ensuring that the ESAs and the competent authorities have:

- an overview of the areas where cooperation and/or exchange of information between competent authorities and the ESAs is needed in accordance with Article 32(7) of the DORA;
- a coordinated and cohesive approach between the ESAs and competent authorities in the exchange of information and when cooperating for the purpose of oversight activities to ensure efficiency and consistency as well as to avoid duplications;
- a common approach to the rules of procedure and timelines that apply in relation to cooperation and information exchange, including roles and responsibilities and means for cooperation and information exchange.

These Guidelines constitute consistent, efficient and effective practices on the oversight cooperation and information exchange between ESAs and competent authorities in the context of Article 32(7) of the DORA. These Guidelines do not hinder the exchange of further information and extended oversight cooperation between ESAs and competent authorities. The practical details of the cooperation and information sharing between ESAs and competent authorities may be subject to bespoke target operating models.

The cooperation and information exchange set out in these Guidelines should take into account a preventive and risk-based approach which should lead to a balanced allocation of tasks and responsibilities between the three ESAs and competent authorities and should make the best use of the human resources and technical expertise available in each of the ESAs and competent authorities.

Unless otherwise specified in these Guidelines, ESAs refers to the three ESAs including the Lead Overseer.

Scope

The scope of these Guidelines relates only to Section II of Chapter V (Articles 31-44) of the DORA and does not cover articles related to:

- tasks that only apply to either one specific competent authority or ESA (e. g. Article 43 on Oversight fees, being a task for the LO only) or that apply to financial entities and critical ICT third-party service providers (e. g. under Article 35(5) , CTPPs are to cooperate in good faith with LO, and assist it in fulfilment of its tasks);
- the cooperation among competent authorities (e. g. under Article 48(1), CAs shall cooperate closely among themselves), among the ESAs (e. g. under Article 35(2)(a), the LO shall ensure

regular coordination within the Joint Oversight Network) and with other EU authorities (e. g. under Article 34(3), the LO may call on the ECB and ENISA to provide technical advice);

- the governance arrangements that are subject to the rules of procedure of the ESAs (e. g. under Article 32, the ESAs need to establish the OF and under Article 34, the LOs need to set up the Joint Oversight Network);
- the separate legal mandates (e. g. the criteria for determining the composition of the JET, their designation, tasks and working arrangements are covered by separate regulatory technical standards to be developed by the ESAs (Article 41(1)(c) of DORA).

Guideline 1: Language, communication means, contact points and accessibility

1.1 For cooperation and information exchange purposes, the ESAs and competent authorities should communicate in English, unless agreed otherwise.

1.2 The ESAs and competent authorities should make available the information referred to in these Guidelines by electronic means, unless agreed otherwise.

1.3 The ESAs and competent authorities should establish single points of contact in the form of a dedicated institutional/functional email address for information exchanges between the ESAs and competent authorities.

1.4 The single point of contact should only be used for exchanging non-confidential information. The ESAs and competent authorities may agree on a bilateral and/or multilateral basis on any applicable requirements concerning the secure transmission of information via the single point of contact (e.g. a requirement on electronic signatures of authorised persons).

1.5 The information on the contact points should be made available to the competent authorities by the ESAs. The competent authorities should make available and update the information about the contact points without undue delay according to the operational instructions defined by the ESAs.

1.6 The ESAs and competent authorities should use a dedicated secure online tool to share information amongst each other on a confidential and secure basis. The online tool should present technical information security measures to guarantee the confidentiality of data against unauthorised access by third-parties.

1.7 The information to be exchanged via the dedicated secure online tool should be limited to the information to be submitted according to points 5 to 12 and any additional information necessary for the Lead Overseer and competent authorities to carry out their respective duties under DORA.

1.8 The ESAs and competent authorities should ensure that communication and information exchange between the ESAs and competent authorities are accessible to, and inclusive for all parties involved, including those who may have language barriers or accessibility needs. In that context, the ESAs and competent authorities may use translation services or accessible communication tools, such as video conferencing software with closed captioning, provided data is protected from unauthorised use of third parties.

Guideline 2: Timelines

2.1 In the event of specific circumstances that require prompt action or additional time to complete the relevant task, the Lead Overseer may, in consultation with relevant competent authorities, reduce or extend the timelines described in points 5 to 12. The Lead Overseer should document the changes and the reasons for such changes.

Guideline 3: Difference of opinions between ESAs and competent authorities

3.1 In case of divergent views regarding the oversight cooperation and information exchange, the ESAs and competent authorities should strive to reach a mutually agreed solution. In cases where no such solution can be reached, the Lead Overseer should, in consultation with the Joint Oversight Network, present the difference of opinions to the Oversight Forum, which will present its views to find a mutually agreed solution.

Guideline 4: Information exchange between ESAs and competent authorities in the context of their respective cooperation with competent authorities designated or established in accordance with NIS2 (NIS2 authorities)

4.1 Where possible, competent authorities and the Lead Overseer should make available to each other relevant information stemming from their dialogue with NIS2 authorities responsible for the supervision of essential or important entities subject to that Directive, which have been designated as a critical ICT third-party service provider.

Section 2: Designation of critical ICT third-party service providers

Guideline 5: Information for the criticality assessment to be submitted by competent authorities to the ESAs

5.1 For the purposes of designating the ICT third-party service providers that are critical for financial entities in accordance with Article 31(1)(a) of the DORA, without undue delay following the receipt of the register of information referred to in Article 28(3) of the DORA, competent authorities should make available the full register of information to the ESAs in accordance with the formats and procedures specified by the ESAs.[3]

5.2 Competent authorities should also make available to the ESAs any relevant quantitative or qualitative information at their disposal to facilitate the criticality assessment envisaged in Article 31(2) of the DORA, taking into account the delegated act referred to in Article 31(6) of the DORA.

5.3 Upon request, competent authorities should make available to the ESAs additional available information acquired in their supervisory activities, in order to facilitate the criticality assessment.

Guideline 6: Information related to the designation of critical ICT third-party service providers to be submitted by the Lead Overseer or ESAs to competent authorities

6.1 Within 10 working days following the receipt from the ICT third-party service provider, the ESAs should make available to the competent authorities of the financial entities using the ICT services provided by a ICT third-party service provider, the legal name, identification code[4], country of the registered office of the ICT third-party service provider and, if it belongs to a group, of the parent group that submitted a request to be designated as critical according to Article 31(11) of the DORA.

6.2 The Lead Overseer should share with the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider:

a) Within 10 working days following the receipt from the critical ICT third-party service provider, the notification of the critical ICT third-party service provider about any changes to the structure of the management of the subsidiary established in the Union according to Article 31(13) of the DORA;

b) Within 10 working days after the submission of the notification of a decision to designate the ICT third party-party service provider as critical to the ICT third-party service provider, the legal name, identification code[7], country of the registered office of the ICT third-party service provider and, if it belongs to a group, of the parent group that has been designated as critical

[3] The ESAs will make use of Article 35(2) of the founding regulations of the ESAs to request the full register of information.

[4] "Identification code" refers to the identification code requested for ICT third-party service providers as established by the Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554

according to Article 31(5) and (11) of the DORA and the starting date as from which they will effectively be subject to oversight activities as referred to in Article 31(5) of the DORA.

Section 3: Core oversight activities

Guideline 7: Oversight plans

7.1 Prior to the finalisation of the annual oversight plan referred to in Article 33(4) of the DORA, the Lead Overseer should make available the draft annual oversight plan to the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider.

7.2 The draft annual oversight plan should include the following information on the envisaged general investigations or inspections:

a) type of oversight activity (general investigation or inspection);

b) high-level scope and objectives;

c) approximate timeframe.

7.3 Competent authorities may provide comments on the draft annual oversight plan within 30 working days following the receipt thereof.

7.4 Within 10 working days following the adoption, the Lead Overseer should make available to the competent authorities, the annual oversight plan and the multi-annual oversight plan[5].

7.5 The Lead Overseer should make available any material updates to the annual oversight plan and the multi-annual oversight plan to the competent authorities without undue delay following the adoption of the updates. Competent authorities may provide comments on the material updates to the annual oversight plan within 30 working days following the receipt.

Guideline 8: General investigations and inspections

8.1 At least 3 weeks before the start of the general investigation or inspection according to Articles 38(5), 39(3) and 36(1) of the DORA, or with the shortest possible delay in case of an urgent investigation or inspection, the Lead Overseer should inform the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider, the identity of the authorised persons for the general investigation or inspection.

8.2 The authorised persons include:

[5] See Recital 3 of draft Regulatory Technical Standards on the conduct of oversight activities in relation to the joint examination teams under DORA

- relevant staff members of the Lead Overseer; and
- the staff members of the Joint Examination Team as referred to in Article 40(2) of the DORA, appointed to carry out the general investigation or inspection.

8.3 The Lead Overseer should inform competent authorities of the financial entities using the ICT services provided by that critical ICT third-party service provider where the authorised persons find that a critical ICT third-party service provider opposes the inspection, including imposing any unjustified conditions to the inspection.

Guideline 9: Additional information exchanges between the Lead Overseer and competent authorities in relation to oversight activities

9.1 Within 10 working days following the adoption of the request for information to the critical ICT third-party service provider, the Lead Overseer should make available to the Joint Oversight Network and the competent authorities of the financial entities using ICT services provided by a critical ICT third-party service provider, the relevant scope of the request for information submitted to the critical ICT third-party service provider according to Articles 36(1)[6] and 37(1) of the DORA.

9.2 The Lead Overseer should inform competent authorities of the financial entities using ICT services provided by a critical ICT third-party service provider of any:

- major incidents with direct or indirect impact on financial entities within the Union when reported by the critical ICT third-party service provider, including relevant details to determine the significance of the incident on financial entities and assess possible cross-border impacts;[7]
- relevant changes in the strategy of the critical ICT third-party service provider on ICT third-party risk;
- events that could represent an important risk to the continuity and sustainability of the provision of ICT services;
- reasoned statement that may be submitted by the critical ICT third-party service provider evidencing the expected impact of the draft oversight plan on customers which are entities falling outside of the scope of DORA and where appropriate, formulating solutions to mitigate risks referred to in Article 33(4) of the DORA.

9.3 If a critical ICT third-party service provider liaises with the competent authorities for the purposes of all matters related to the oversight, the competent authorities should make available those communications to the Lead Overseer and remind the critical ICT third-party service provider that

[7] See Article 3(2), letter l of Draft regulatory technical standards on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) points (a), b) and (d) of Regulation (EU) 2022/2554

the Lead Overseer is its primary point of contact for the purposes of all matters related to the oversight.

Section 4: Follow-up of the recommendations

Guideline 10: General principles for follow-up

10.1 The following general principles should apply to the follow-up of the recommendations issued by the Lead Overseer:

- The competent authorities are the primary point of contact for financial entities under their supervision. The competent authorities are responsible for the follow-up concerning the risks identified in the recommendations concerning financial entities making use of the services of the critical ICT third-party service providers;
- The Lead Overseer is the primary point of contact for critical ICT third-party service providers for the purposes of all matters related to the oversight. The Lead Overseer is responsible for the follow-up of the recommendations addressed to the critical ICT third-party service provider.

Guideline 11: Information exchanges between the Lead Overseer and competent authorities to ensure the follow-up of recommendations

11.1 The Lead Overseer should make available to the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider, the following information:

a. Within 10 working days following the receipt by the Lead Overseer:
   - the notification of the critical ICT third-party service provider to follow the recommendations issued by the Lead Overseer and the remediation plan prepared by the critical ICT third-party service provider;
   - the reasoned explanation of the critical ICT third-party service provider for not following the recommendations;
   - the reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service provider according to Article 35(1)(c) of the DORA.

b. Within 10 working days after the expiration of the 60 calendar days according to Article 42(1) of the DORA:

- the fact that the critical ICT third-party service provider failed to send the notification within 60 calendar days after the issuance of recommendations to the critical ICT third-party service provider according to Article 35(1)(d) of the DORA.

c. Within 10 working days after the adoption by the Lead Overseer:

- the assessment as to whether the critical ICT third-party service provider's explanation for not following the Lead Overseer's recommendations is deemed sufficient and, if it is deemed sufficient, the Lead Overseer's decision concerning amendment of recommendations[8];
- the assessment of the reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service provider according to Articles 35(1)(c) of the DORA. In case the critical ICT third-party service provider has not adequately implemented the recommendations, the assessment should at least cover the criteria a) to d) of Article 42(8) of the DORA;
- the decision imposing a periodic penalty payment on the critical ICT third-party service provider according to Article 35(6) of the DORA. If the Lead Overseer opted not to disclose the periodic penalty payment to the public as per Article 35(10) of the DORA, the competent authorities receiving the information should not disclose it to the public;
- assessment as to whether the refusal of a critical ICT-third-party service provider to endorse recommendations, based on a divergent approach from the one advised by the Lead Overseer, could adversely impact a large number of financial entities, or a significant part of the financial sector.

11.2 In accordance with Article 42(10) of the DORA, the competent authorities should make available to the Lead Overseer the following information where critical ICT third party service providers have not endorsed in part or entirely recommendations addressed to them by the Lead Overseer:

a. Within 10 working days following the adoption by the competent authority:

- notification to the financial entity of the possibility of a decision being taken where a competent authority deems that a financial entity fails to take into account or to sufficiently address within its management of ICT third-party risk the specific risks identified in the recommendations issued by the Lead Overseer according to Article 42(4) of the DORA;
- individual warnings issued by competent authorities according to Article 42(7) of the DORA and relevant information which allows the Lead Overseer to assess whether such

[8] The Lead Overseer and the Joint Examination Team assess the critical ICT third party service provider's reasoned explanation for not following the recommendations. If the Lead Overseer decides that the explanation is deemed sufficient, the Lead Overseer may amend the respective recommendations.

warnings have resulted in consistent approaches mitigating the potential risk to financial stability.

b. Within 10 working days following the consultation:

- outcome of the consultation with NIS2 authorities prior to taking a decision, as referred to in Article 42(5) of the DORA , where possible.

c. Within 10 working days following the receipt of the information from financial entities:

- the material changes to existing contractual arrangements of financial entities with critical ICT third-party service providers which were made to address the risks identified in the recommendations issued by the Lead Overseer;
- the start of executing exit strategies and transition plans of the financial entities as referred to in Article 28(8) of the DORA.

11.3 The ESAs, in consultation with competent authorities, should develop a template to facilitate the transmission of the information as defined in point 11.2.

Guideline 12: Decision requiring financial entities to temporarily suspend the use or deployment of a service provided by the critical ICT third-party service provider or terminate the relevant contractual arrangements concluded with the critical ICT third-party service provider

12.1 The competent authorities should inform the Lead Overseer of their intention to notify a financial entity of the possibility of a decision being taken if the financial entity does not adopt appropriate contractual arrangements to address the specific risks identified in the recommendations, as referred to in Article 42(4) of the DORA . For the purpose of application of point 12.2, the competent authorities should make available to the Lead Overseer all relevant information regarding the possible decision and highlight if they intend to adopt an urgent decision.

12.2 After the receipt of the information, the Lead Overseer should assess the potential impact such decision might have for the critical ICT third-party service provider whose service would be temporarily suspended or terminated. Within 10 working days from the receipt of the information or with the shortest possible delay in case the competent authorities intend to adopt an urgent decision, the Lead Overseer should make that assessment available to the competent authorities concerned. Competent authorities should consider that non-binding assessment when deciding whether or not to issue the notification referred to in point 12.1.

12.3 Where two or more competent authorities plan to take or have taken decisions regarding financial entities making use of ICT services provided by the same critical ICT third-party service

provider, the Lead Overseer should inform them about any inconsistent or divergent supervisory approaches that could lead to an unlevel playing field where financial entities are using the ICT services provided by a critical ICT third-party service provider across Member States.

Section 5: Final provisions

These Guidelines apply from 17 January 2025.

These Guidelines will be subject to a review by the ESAs.

Annex: Table summarising information exchanges

The following table summarises the information exchanges between the LO/ESAs (marked grey) and CAs (marked green) as indicated by these Guidelines. The table is not intended to introduce any new guidance, but to reflect the guidance included in the Guidelines. If there are any differences between the Guidelines and this table, the information included in the Guidelines prevails.

Information exchange	Timeline	Related Article in the Level 1 text	GL
Section 1: General considerations			
LO, in consultation with relevant CAs, reduce or extend the timelines	-	-	2.1
LO, in consultation with the JON, to present to the OF difference of opinions regarding the oversight cooperation and information exchanges	-	-	3.1
Where possible, CAs and LO to make available to each other, relevant information from their dialogue with NIS2 authorities	-		4.1
Section 2: Designation of CTPPs			
CAs to make available the full register of information to the ESAs	Without undue delay following the receipt of the register of information	28(3)[9] 31(1)(a)[10], (2), (6)[11] and (10)[12] Article 35(2) of the ESAs' founding regulation[13]	5.1
CAs to make available to the ESAs any relevant	-		5.2

[9] Article 28(3): As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers…

[10] Article 31(1)(a): The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 32(1), shall designate the ICT third-party service providers that are critical for financial entities, following an assessment that takes into account the criteria specified in paragraph 2.

[11] Article 31(6): The Commission is empowered to adopt a delegated act in accordance with Article 57 to supplement this Regulation by specifying further the criteria referred to in paragraph 2 of this Article, by 17 July 2024.

[12] Article 31(10): For the purposes of paragraph 1, point (a), competent authorities shall, on a yearly and aggregated basis, transmit the reports referred to in Article 28(3), third subparagraph, to the Oversight Forum established pursuant to Article 32....

[13] Article 35(2) of the ESAs' founding regulation: The Authority may also request information to be provided at recurring intervals and in specified formats. Such requests shall, where possible, be made using common reporting formats.

Information exchange	Timeline	Related Article in the Level 1 text	GL
quantitative or qualitative information at their disposal to facilitate the criticality assessment			
Upon request, CAs to make available additional available information acquired in their supervisory activities	-		5.3
ESAs to make available to CAs information about the TPP that submitted a request to be designated as critical	Within 10 working days following the receipt from the TPP	31(5)[14], (11)[15] and (13)[16]	6.1
LO to share with CAs notification of the CTPP about any changes to the structure of the management of the subsidiary established in the Union	Within 10 working days following the receipt from the CTPP		6.2 (a)
LO to share with CAs information about the TPP that has been designated as critical and the starting date of designation	Within 10 working days after the submission of the notification		6.2 (b)
Section 3: Core oversight activities			
LO to make available to CAs the draft annual oversight plan	Prior to the finalisation of the annual oversight plan	33(4)[17] Recital 3 of draft Regulatory Technical Standards on the conduct of oversight activities	7.1
CAs may provide comments on the draft annual oversight plan	Within 30 working days following the receipt		7.3

[14] Article 31(5): … After designating an ICT third-party service provider as critical, the ESAs, through the Joint Committee, shall notify the ICT third-party service provider of such designation and the starting date as from which they will effectively be subject to oversight activities.

[15] Article 31(11): The ICT third-party service providers that are not included in the list referred to in paragraph 9 may request to be designated as critical in accordance with paragraph 1, point (a).

[16] Article 31(13): The critical ICT third-party service provider referred to in paragraph 12 shall notify the Lead Overseer of any changes to the structure of the management of the subsidiary established in the Union.

[17] Article 33(4): Based on the assessment referred to in paragraph 2, and in coordination with the Joint Oversight Network referred to in Article 34(1), the Lead Overseer shall adopt a clear, detailed and reasoned individual oversight plan describing the annual oversight objectives and the main oversight actions planned for each critical ICT third-party service provider. That plan shall be communicated yearly to the critical ICT third-party service provider.

Information exchange	Timeline	Related Article in the Level 1 text	GL
LO to make available to CAs, the annual oversight plan and the multi-annual oversight plan.	Within 10 working days following the adoption	in relation to the joint examination teams under DORA	7.4
LO to make available to CAs any material updates to the annual oversight plan and the multi-annual oversight plan	Without undue delay following the adoption of the updates		7.5
CAs may provide comments on the material updates to the annual oversight plan	Within 30 working days following the receipt		7.5
LO to confirm to the CAs of the identity of the authorised persons for the investigation or inspection	At least 3 weeks before the start of the investigation or inspection Or With the shortest possible delay in case of an urgent investigation or inspection	36(1), 38(5)[18] and 39(3)[19]	8.1
LO to inform CAs where the authorised persons find that a CTPP opposes an inspection, including imposing any unjustified conditions to the inspection	-	39(7)[20]	8.3

[18] Article 38(5): In good time before the start of the investigation, the Lead Overseer shall inform competent authorities of the financial entities using the ICT services of that critical ICT third-party service provider of the envisaged investigation and of the identity of the authorised persons.

[19] Article 39(3): In good time before the start of the inspection, the Lead Overseer shall inform the competent authorities of the financial entities using that ICT third-party service provider.

[20] Article 39(7): Where the officials and other persons authorised by the Lead Overseer find that a critical ICT third-party service provider opposes an inspection ordered pursuant to this Article, the Lead Overseer shall inform the critical ICT third-party service provider of the consequences of such opposition, including the possibility for competent authorities of the relevant financial entities to require financial entities to terminate the contractual arrangements concluded with that critical ICT third-party service provider.

Information exchange	Timeline	Related Article in the Level 1 text	GL
LO to make available to the JON and the CAs, relevant scope of the request for information submitted to the CTPP	Within 10 working days following the adoption of the request for information to the CTPP	36(1)[21],37(1)[22] and 37(5)[23]	9.1
LO to make available to CAs of: • major incidents with direct/indirect impact on FEs when reported by the CTPP (upon request by LO); • relevant changes in the strategy of the CTPP on ICT third-party risk; • events that could represent important risk to the provision of ICT services; • reasoned statement from the CTPP evidencing the expected impact of the draft oversight plan.	-	33(4)[24] Article 3(2), letter l of Draft regulatory technical standards on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) points (a), b) and (d) of Regulation (EU) 2022/2554	9.2
CAs to make available to the LO, communications of the CTPP with the CAs for the purposes of all	-	33(1)[25]	9.3

[21] Article 36(1): When oversight objectives cannot be attained by means of interacting with the subsidiary set up for the purpose of Article 31(12), or by exercising oversight activities on premises located in the Union, the Lead Overseer may exercise the powers, referred to in the following provisions, on any premises located in a third-country which is owned, or used in any way, for the purposes of providing services to Union financial entities, by a critical ICT third party service provider, in connection with its business operations, functions or services, including any administrative, business or operational offices, premises, lands, buildings or other properties…

[22] Article 37(1): The Lead Overseer may, by simple request or by decision, require critical ICT third-party service providers to provide all information that is necessary for the Lead Overseer to carry out its duties under this Regulation, including all relevant business or operational documents, contracts, policies, documentation, ICT security audit reports, ICT-related incident reports, as well as any information relating to parties to whom the critical ICT third-party service provider has outsourced operational functions or activities.

[23] The Lead Overseer shall, without delay, transmit a copy of the decision to supply information to the competent authorities of the financial entities using the services of the relevant critical ICT third-party service providers and to the JON.

[24] Article 33(4), third subparagraph: Upon receipt of the draft oversight plan, the critical ICT third-party service provider may submit a reasoned statement within 15 calendar days evidencing the expected impact on customers which are entities falling outside of the scope of this Regulation and where appropriate, formulating solutions to mitigate risks.

[25] Article 33(1): The Lead Overseer shall conduct the oversight of the assigned critical ICT third party service providers and shall be, for the purposes of all matters related to the oversight, the primary point of contact for those critical ICT third party service providers.

Information exchange	Timeline	Related Article in the Level 1 text	GL
matters related to the oversight			
Section 4: Follow-up of the recommendations			
LO to make available to CAs: • notification of CTPP to follow recommendations; • the CTPP's remediation plan; • the reasoned explanation of the CTPP for not following the recommendations; and • the report specifying the actions taken or remedies implemented by the CTPP	Within 10 working days following the receipt by the LO	35(1)(c)[26] and 42(1)[27]	11.1 a)
LO to make available to CAs, the fact that the CTPP failed to send the notification within 60 calendar days after the issuance of recommendations to the CTPP	Within 10 working days after the expiration of the 60 calendar days		11.1 b)
LO to make available to CAs: • assessment as to whether the CTPP's explanation for not following the LO's	Within 10 working days following the adoption by the LO	35(1)(c), 35(6)[28], 35(10)[29], 42(1), 42(8)(a-d)[30]	11.1 c)

[26] Article 35(1)(c): The Lead Overseer has the power to request, after the completion of the oversight activities, reports specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third party service provider in relation to the recommendations issued.

[27] Article 42(1): Within 60 calendar days of the receipt of the recommendations issued by the Lead Overseer, critical ICT third party service providers shall either notify the Lead Overseer of their intention to follow the recommendations or provide a reasoned explanation for not following such recommendations.

[28] Article 35(6): In the event of whole or partial non-compliance with the measures required to be taken pursuant to the exercise of the powers under paragraph 1, points (a), (b) and (c), and after the expiry of a period of at least 30 calendar days from the date on which the critical ICT third-party service provider received notification of the respective measures, the Lead Overseer shall adopt a decision imposing a periodic penalty payment to compel the critical ICT third-party service provider to comply with those measures.

[29] Article 35(10): The Lead Overseer shall disclose to the public every periodic penalty payment that has been imposed, unless such disclosure would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

[30] Article 42(8): Upon receiving the reports referred to in Article 35(1), point (c), competent authorities, when taking a decision as referred to in paragraph 6 of this Article, shall take into account the type and magnitude of risk that is not addressed by the critical ICT third-party service provider, as well as the seriousness of the non-compliance, having regard to the following criteria:

(a) the gravity and the duration of the non-compliance;

(b) whether the non-compliance has revealed serious weaknesses in the critical ICT third-party service provider's procedures, management systems, risk management and internal controls;

(c) whether a financial crime was facilitated, occasioned or is otherwise attributable to the non-compliance;

(d) whether the non-compliance has been intentional or negligent.

Information exchange	Timeline	Related Article in the Level 1 text	GL
recommendations is deemed sufficient and, if so, the LO's decision concerning amendment of recommendations; • assessment of the reports specifying the actions taken or remedies implemented by the CTPP; • decision imposing a periodic penalty payment on the CTPP; • assessment as to whether the refusal of a CTPP to endorse recommendations could adversely impact a large number of financial entities, or a significant part of the financial sector			
CAs to make available to LO: • notification to the financial entity of the possibility of a decision being taken; • individual warnings issued by CAs and relevant information which allows the LO to assess whether such warnings have resulted in consistent approaches mitigating the potential risk to financial stability	Within 10 working days following the adoption by the CA	42(4)[31], (7)[32] and (10)[33]	11.2 a)
Where possible, CAs to make available to LO, outcome of the consultation with NIS2 authorities prior to taking a decision.	Within 10 working days following the consultation	42(5)[34]	11.2 b)

[31] Article 42(4): Where a competent authority deems that a financial entity fails to take into account or to sufficiently address within its management of ICT third-party risk the specific risks identified in the recommendations, it shall notify the financial entity of the possibility of a decision being taken, within 60 calendar days of the receipt of such notification, pursuant to paragraph 6, in the absence of appropriate contractual arrangements aiming to address such risks.

[32] Article 42(7): Where a critical ICT third-party service provider refuses to endorse recommendations, based on a divergent approach from the one advised by the Lead Overseer, and such a divergent approach may adversely impact a large number of financial entities, or a significant part of the financial sector, and individual warnings issued by competent authorities have not resulted in consistent approaches mitigating the potential risk to financial stability, the Lead Overseer may, after consulting the Oversight Forum, issue non-binding and non-public opinions to competent authorities, in order to promote consistent and convergent supervisory follow-up measures, as appropriate.

[33] Article 42(10): Competent authorities shall regularly inform the Lead Overseer on the approaches and measures taken in their supervisory tasks in relation to financial entities as well as on the contractual arrangements concluded by financial entities where critical ICT third party service providers have not endorsed in part or entirely recommendations addressed to them by the Lead Overseer.

[34] Article 42(5): Upon receiving the reports referred to in Article 35(1), point (c), and prior to taking a decision as referred to in paragraph 6 of this Article, competent authorities may, on a voluntary basis, consult the competent authorities designated or established in accordance with Directive (EU) 2022/2555 responsible for the supervision of an essential or important entity subject to that Directive, which has been designated as a critical ICT third-party service provider.

Information exchange	Timeline	Related Article in the Level 1 text	GL
CAs to make available to LO: • the material changes to existing contractual arrangements of financial entities with CTPPs made to address the risks identified in the recommendations; • the start of executing exit strategies and transition plans of the financial entities	Within 10 working days following the receipt of the information from financial entities	28 and 42(10)[35]	11.2 c)
CAs to inform LO of: • intention to notify a financial entity of the possibility of a decision being taken if the financial entity does not adopt appropriate contractual arrangements to address the specific risks identified in the recommendations; • all relevant information regarding the decision; • whether they intend to carry out an urgent decision	-	42(4) and (10)	12.1
LO to make available to CAs, non-binding assessment of potential impact the decision might have for the CTPP whose service would be temporarily suspended or terminated	Within 10 working days from the receipt of the information referred to in GL 12.1 or With the shortest possible delay in case of an urgent decision		12.2

[35] Article 42(10): Competent authorities shall regularly inform the Lead Overseer on the approaches and measures taken in their supervisory tasks in relation to financial entities as well as on the contractual arrangements concluded by financial entities where critical ICT third-party service providers have not endorsed in part or entirely recommendations addressed to them by the Lead Overseer.