JC 2023 71

27 November 2023

Consultation Paper

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

Contents

1. Responding to this consultation

The European Supervisory Authorities (the ESAs) invite comments on all proposals put forward in this paper and in particular on the specific questions summarised on page 7.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed / rationale proposed; and
- describe any alternative regulatory choices the ESAs should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 04 March 2024. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Your responses will be published on the ESA websites unless: you request to treat them confidential, or they are unlawful, or they would infringe the rights of any third party. Please indicate clearly and prominently in your submission any part you do not wish to be publicly disclosed.

A confidential response may be requested from us in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the ESAs' Board of Appeal and the European Ombudsman.

Data protection

Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published. EIOPA, as a European Authority, will process any personal data in line with Regulation (EU) 2018/1725. More information on how personal data is processed can be found under the Legal notice sections on the ESAs' websites.

2. Executive Summary

Introduction and scope

Regulation (EU) 2022/2554 ("DORA")[1] introduces a pan-European oversight framework of ICT third-party service providers designated as critical (CTPPs). As part of this oversight framework, the ESAs and competent authorities (CAs) have received new roles and responsibilities. For example, on the one hand, the ESA, as Lead Overseer (LO), will be responsible to exercise oversight activities on the CTPPs, issue recommendations and follow up with the CTPPs on these recommendations. On the other hand, CAs, for example, will participate in the LO's oversight of the CTPP as part of the Joint Examination Team (JET) and follow up with financial entities concerning the risks identified in the recommendations.

In order to ensure a consistent and convergent supervisory approach and a level playing field where financial entities are using the ICT services provided by a CTPP across Member States, it is important to have close cooperation between CAs and ESAs through a mutual exchange of information and provision of assistance in the context of relevant supervisory activities. Moreover, a coordinated approach in the context of oversight activities is important to avoid duplications and overlaps in conducting measures aimed at monitoring the CTPPs' risks.

In this context, the ESAs have been mandated under Article 32(7) of the DORA to issue guidelines on the cooperation between the ESAs and the CAs covering the detailed procedures and conditions for the allocation and execution of tasks between CAs and the ESAs and the details on the exchanges of information which are necessary for CAs to ensure the follow-up of recommendations addressed to CTPPs.

In terms of scope, the draft guidelines in this Consultation Paper cover the cooperation and information exchange between ESAs and CAs only. Hence, the cooperation with financial entities, CTPPs, among relevant CAs, among the ESAs and with other EU institutions is outside the scope of the guidelines.

Contents

The draft guidelines have the following five sections as well as an Annex with a table summarising the information exchanges for the LO/ESAs and CAs as indicated by these Guidelines.

1. General considerations: this section covers topics, such as language, communication means, contact points and difference of opinions between ESAs and CAs.

2. Designation of CTPPs: this section covers the information exchanges between the LO, CAs and the Oversight Forum (OF) related to the designation of CTPPs.

[1] EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu)

3. Oversight activities: this section covers the procedures and information exchanges related to the annual oversight plan, general investigations and on-site inspections as well as the measures CAs can take concerning CTPPs only in agreement with the LO.

4. Follow-up of the recommendations: this section covers the general principles for the follow-up of the recommendations and the information exchanges between the LO and CAs to ensure the follow-up of recommendations. It also encompasses information exchanges in case of the last resort decision of CAs to require financial entities to suspend / terminate their contract with the CTPP.

5. Final provisions: this section covers the application date of the full set of guidelines and a guideline providing a review by the ESAs of the application of the guidelines within four years after publication.

In order to guide and support the reader during the public consultation, the guidelines have been complemented with footnotes reporting the relevant legal text of the DORA. These footnotes will be removed in the text of the final guidelines.

Next steps

The consultation period will run until 04 March 2024. The ESAs will consider the responses they received to this Consultation Paper and will finalise the draft guidelines to issue them by 17 July 2024.

3. Introduction and scope

3.1 Introduction

1. The Digital Operational Resilience Act (DORA)[2] entered into force on 16 January 2023 and will apply from 17 January 2025.
2. DORA introduces an oversight framework to the financial sector for all designated CTPPs in accordance with Article 31(1)(a) of the DORA. According to Recital 76, the oversight framework is set up with a view to:
    - promote convergence and efficiency in relation to supervisory approaches when addressing ICT third–party risks in the financial sector;
    - strengthen the digital operational resilience of financial entities which rely on CTPPs for the provision of ICT services that support the supply of financial services;
    - contribute, thereby, to the preservation of the Union's financial system stability and the integrity of the internal market for financial services.
3. The main actors of the DORA oversight framework are:
    - the LO, one of the European Supervisory Authorities – (ESAs) appointed according to Article 31(1)(b) and responsible to carry out the oversight tasks and to be the single point of contact for the CTPPs;
    - the CAs, identified in Article 46 and responsible to supervise the compliance of financial entities to DORA and to the various applicable relevant financial regulations; and
    - the other two ESAs that have not been appointed as LOs for a particular CTPP, being involved in the DORA oversight activities through their participation in the Joint Examination Teams (JET) as defined in Article 40 and in the Joint Oversight Network as defined in Article 34.
4. Representatives from all those actors are members of the OF as defined in Article 32(4) which also includes authorities such as the ESRB, ENISA, the ECB and, where applicable, the CAs designated or established according to Directive (EU) 2022/2555 supervising the essential and important entities ("NIS 2") to be appointed as observers.
5. To ensure the timely and successful results of the oversight framework, also in light of the obligation stemming from Article 40 for both the ESAs not appointed as LO and the relevant CAs to provide resources to the JET, the application of oversight framework should be facilitated by close cooperation among relevant CAs and consultation with the ESAs through the mutual exchange of information and the provision of assistance in the context of relevant supervisory activities (Recital 97).

[2] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)

6. In addition, as referred to in Recital 93, a coordinated approach between the ESAs and CAs in the context of the exercise of tasks in the oversight framework is important to avoid duplications and overlaps in conducting measures aimed at monitoring the CTPP's risks. As indicated in recital 88, such duplications and overlaps could prevent financial supervisors from obtaining a complete and comprehensive overview of ICT third-party risk in the Union, while also creating redundancy, burden and complexity for critical ICT third-party service providers if they were subject to numerous monitoring and inspection requests.

3.2 Scope

7. According to Article 32(7) of the DORA, in accordance with Article 16 of Regulation (EU) No 1093/2010 (EBA Regulation), of Regulation (EU) No 1094/2010 (EIOPA Regulation) and Regulation (EU) No 1095/2010 (ESMA Regulation), *"the ESAs shall issue, for the purposes of this Section [i. e. Chapter V – Section II "Oversight framework of critical ICT third party service providers"], 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 pursuant to Article 35(1), point (d), addressed to critical ICT third–party service providers."*

8. Since the Section II of Chapter V is composed by Articles 31 to 44, the scope of the Guidelines relates to these Articles. Hence, other Articles which are related to the cooperation between ESAs and CAs (e. g. Article 49 on "Financial cross-sector exercises, communication and cooperation") are not covered by the Guidelines.

9. Articles which cover tasks that only apply to either one specific CA or ESA (e. g. Article 43 on Oversight fees, being a task for the LO only) or that apply to financial entities and CTPPs (e. g. under Article 35(5), CTPP to cooperate in good faith with LO, and assist it in fulfilment of its tasks), are outside the scope of the Guidelines given that for such tasks, cooperation between the CAs and the ESAs is not required.

10. These Guidelines cover the cooperation between the ESAs and CAs, which are defined in Article 46. Hence, these Guidelines do not cover:

    - the cooperation among CAs (e. g. under Article 48(1), CAs shall cooperate closely among themselves),
    - the cooperation between CAs and CAs under NIS 2 excluded by Article 46 (e. g. under Article 42(5), CAs may consult, on a voluntary basis, CAs under NIS 2, prior to temporarily suspending the use or deployment of services provided by the CTPP),
    - the cooperation among the ESAs (e. g. under Article 35(2)(a), the LO shall ensure regular coordination within the Joint Oversight Network) and
    - the cooperation between the ESAs and other EU authorities (e. g. under Article 34(3), the LO may call on the ECB and ENISA to provide technical advice).

11. Articles 31 to 44 also cover the governance arrangements that need to be set up by the ESAs to ensure cooperation and take decisions (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 cooperation between CAs and ESAs in the context of these governance arrangements – including for specific tasks such as the collective assessment of the results and findings of the oversight activities (Article 32(2)) or the preparation of benchmark of CTPPs (Article 32(3)) – are not covered by the Guidelines given that they are subject to the rules of procedure (to be) established by the Joint Committee of the ESAs. However, the Guidelines would specify the information CAs need to submit to the OF for the purposes of designating the ICT third-party service providers that are critical for financial entities.

12. Where the ESAs or the European Commission have a legal mandate in DORA to provide further details (e. g. through delegated acts) to any aspects concerning the coordination between the ESAs and CAs as referred to in Article 32(7), the Guidelines do not cover such aspects. For example, the following aspects are not covered by the Guidelines:

    - Criteria for designation of CTPPs (Article 31(6)) – i. e. the Guidelines do not further specify such criteria given that the European Commission will adopt a delegated act on this;
    - Criteria for determining the composition of the JET, their designation, tasks and working arrangements (Article 41(1)(c)) – i. e. the allocation and execution of tasks between CAs and the ESAs within the JET are not covered by the Guidelines, but by a separate regulatory technical standards to be developed by the ESAs (Article 41(1)).

4. Overview of questions for consultation

1. For each guideline, do you consider the Guideline to be clear, concise and comprehensible? If your answer is no, please refer to the specific point(s) of the guideline which is/are not sufficiently clear, concise or comprehensible.
2. Taking into account the specific scope of these Guidelines, do you consider that these Guidelines cover all the instances where cooperation and information exchange between CAs and the LO is necessary? If your answer is no, please propose additional areas that should be covered.
3. Do you consider that the implementation of these Guidelines will contribute to adequate cooperation and information exchange between the ESAs and CAs in the conduct of oversight activities? If your answer is no, please propose an alternative approach how this could be achieved.
4. What are your main expectations regarding the impact on financial entities and CTPPs of the application of these Guidelines?

5. Draft Guidelines on ESAs-competent authorities oversight cooperation

Status of these Guidelines

This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (EBA); Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (EIOPA); and Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (ESMA)) - 'the ESAs' Regulations'[3]. In accordance with Article 16(3) of the ESAs' Regulations, competent authorities shall make every effort to comply with the guidelines.

These Guidelines are based on Article 32(7) of Regulation (EU) 2022/2554 ("DORA")[4], 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 according to Article 31(1) point (a).

Reporting requirements

In accordance with Article 16(3) of the ESAs' Regulations, competent authorities must notify the respective ESA whether they comply or intend to comply with these Guidelines, or otherwise with reasons for non-compliance, by [two months after issuance 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, compliance@eiopa.europa.eu and compliance@esma.europa.eu with the reference 'JC/GL/2024/xx'. 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).

[3] 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).

[4] 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:

a) 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);

b) a coordinated and cohesive approach between 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;

c) 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). 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 comprises the three ESAs including the Lead Overseer.

Scope

The scope of these Guidelines relates only to Section II of Chapter V (Articles 31-44)[5] of the DORA and does not cover Articles related to:

- tasks that only apply to either one specific competent authority or ESA or that apply to financial entities and critical ICT third-party service providers[6];

[5] According to Article 32(7), "the ESAs shall issue, for the purposes of this Section [i. e. Chapter V – Section II "Oversight framework of critical ICT third party service providers"], guidelines on the cooperation between the ESAs and the competent authorities. Hence, other Articles which are related to the cooperation between ESAs and competent authorities (e. g. Articles 47-48 on "Cooperation with structures and authorities established under NIS 2" and "Cooperation between authorities") are not covered by the guidelines

[6] Articles which cover tasks that only apply to either one specific competent authority or ESA (e. g. Article 43 on Oversight fees, being a task for the Lead Overseer only) or that apply to financial entities and critical ICT third party service providers (e. g. under Article 35(5), critical ICT third party service provider shall cooperate in good faith with the Lead Overseer, and assist it in fulfilment of its tasks), are outside the scope of the guidelines given that for such tasks, cooperation between the competent authorities and the ESAs is not required

- the cooperation among competent authorities, among the ESAs and with other EU authorities[7];
- the governance arrangements that are subject to the rules of procedure of the ESAs[8];
- the separate legal mandates[9].

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 transmit the information referred to in these Guidelines by electronic means, unless agreed otherwise.

1.3 The ESAs and competent authorities should establish a single point 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. requirement on electronic signatures of authorised persons).

---

[7] The cooperation among relevant competent authorities (e. g. under Article 42(5), competent authorities may consult, on a voluntary basis, 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, prior to temporarily suspending the use or deployment of services provided by the critical ICT third party service providers), among the ESAs (e. g. under Article 35(2)(a), the Lead Overseer shall ensure regular coordination within the Joint Oversight Network (JON)) and with other EU authorities (e. g. under Article 34(3), the Lead Overseer may call on the European Central Bank and the European Union Agency for Cybersecurity to provide technical advice) are not covered by the guidelines

[8] Articles 31 to 44 also cover the governance arrangements that need to be set up by the ESAs to ensure cooperation and to take decisions (e. g. under Article 32, the ESAs need to establish the Oversight Forum and under Article 34, the Lead Overseer needs to set up the Joint Oversight Network). The cooperation between competent authorities and ESAs in the context of these governance arrangements – including for specific tasks such as the collective assessment of the results and findings of the oversight activities (Article 32(2)) or the preparation of benchmark of critical ICT third party service providers (Article 32(3)) – are not covered by the guidelines given that they are subject to the rules of procedure (to be) established by the Joint Committee of the ESAs (Chapter IV of ESAs founding regulations). Also, the guidelines do not aim to cover the practical details of the cooperation and information sharing between ESAs and competent authorities that will be subject to bespoke target operating models.

[9] Where the ESAs or the European Commission have a separate legal mandate in DORA to provide further guidance (e. g. through delegated acts or draft regulatory technical standards) in relation to any aspects concerning the coordination between the ESAs and competent authorities as referred to in Article 32(7), in order to avoid overlaps with such separate guidance, the guidelines do not cover such aspects. For example, the following aspects are not covered by the guidelines:

Criteria for designation of critical ICT third party service providers critical ICT third party service providers (Article 31(6)) – i. e. the guidelines would not further specify such criteria given that the European Commission will adopt a delegated act on this;

Criteria for determining the composition of the joint examination team, their designation, tasks and working arrangements (Article 41(1)(c)) – i. e. the allocation and execution of tasks between competent authorities and the ESAs within the joint examination team would not be covered by the guidelines, but by separate draft Regulatory Technical Standards to be developed by the ESAs (Article 41(1)).

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

1.6 The ESAs should establish a dedicated online tool where the information to be submitted in line with Sections 2, 3 and 4 of these Guidelines can be confidentially and securely shared among the ESAs and competent authorities. The online tool should present technical information security measures to guarantee the confidentiality of data against unauthorised third-parties.

1.7 Without undue delay after receiving the information to be submitted in line with Sections 2, 3 and 4 of these Guidelines, the Lead Overseer and competent authorities should acknowledge receipt of such information.

1.8 The ESAs and competent authorities should ensure that communication and information exchange between the ESAs and competent authorities are accessible 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 Lead Overseer may, in consultation with relevant competent authorities, reduce or extend the timelines described in Sections 2, 3 and 4 of these Guidelines. 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 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 NIS 2 (NIS 2 authorities)

4.1 Where possible, competent authorities and the Lead Overseer should share with each other, relevant information stemming from their dialogue with NIS 2 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.[10]

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 Oversight Forum

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)[11], without undue delay following the receipt of the register of information referred to in Article 28(3), competent authorities should transmit the full register of information[12] to the Oversight Forum in accordance with the formats and procedures specified by the ESAs.[13]

5.2 Competent authorities should also submit to the Oversight Forum any relevant quantitative or qualitative information at their disposal to facilitate the criticality assessment envisaged in Article 31(2), taking into account the delegated act referred to in Article 31(6)[14].

5.3 Upon request, competent authorities should provide the Lead Overseer 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 to competent authorities

6.1 The Lead Overseer should transmit to the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider, the following information related to the designation of critical ICT third-party service providers:

---

[10] Article 48(2): Competent authorities and the Lead Overseer shall, in a timely manner, mutually exchange all relevant information concerning critical ICT third-party service providers which is necessary for them to carry out their respective duties under this Regulation, in particular in relation to identified risks, approaches and measures taken as part of the Lead Overseer's oversight tasks.

[11] 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.

[12] 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…

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

[14] 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.

a) Within 10 working days following the receipt from the critical ICT third-party service provider:

- the legal name, LEI code, country of establishment 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)[15];
- 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)[16].

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, LEI code, country of establishment of the ICT third-party service provider and, if it belongs to a group, of the parent group that has been designated as critical according to Article 31(5)[17] and (11) and the starting date as from which they will effectively be subject to oversight activities as referred to in Article 31(5).

Section 3: Core oversight activities

Guideline 7: Annual oversight plan

7.1 Within 10 working days following its adoption in [September/October], the Lead Overseer should transmit to the competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider, the annual oversight plan referred to in Article 33(4)[18].

7.2 The Lead Overseer should transmit any updates to the annual oversight plan to the competent authorities concerned without undue delay following the adoption of the updates.

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

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

[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).

For the purpose of the first subparagraph, the ICT third-party service provider shall submit a reasoned application to EBA, ESMA or EIOPA, which, through the Joint Committee, shall decide whether to designate that ICT third-party service provider as critical in accordance with paragraph 1, point (a).

The decision referred to in the second subparagraph shall be adopted and notified to the ICT third-party service provider within 6 months of receipt of the application.

[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 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.

[18] 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.

- high-level scope and objectives;
- approximate timeframe;
- human resources expressed in full-time equivalents needed (this information would not be included in the annual oversight plan to be notified to the critical ICT third-party service provider according to Article 33(5)[19]);
- expected profile of staff to carry out the oversight activity (this information would not be included in the annual oversight plan to be notified to the critical ICT third-party service provider according to Article 33(5)).

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)[20], 39(3)[21] and 36(1) or with the shortest possible delay in case of an urgent investigation or inspection, the Lead Overseer should inform competent authorities of the financial entities using the ICT services provided by a critical ICT third-party service provider, of the identity of the authorised persons for the general investigation or inspection.

8.2 The authorised persons include:

- relevant staff members of the Lead Overseer; and
- the staff members of the Joint Examination Team as referred to in Article 40(2)[22] 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: Measures by competent authorities concerning critical

[19] Article 33(5): Once the annual oversight plans have been adopted and notified to the critical ICT third party service providers, competent authorities may take measures concerning such critical ICT third party service providers only in agreement with the Lead Overseer.

[20] 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.

[21] 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.

[22] Article 40(2): The joint examination team referred to in paragraph 1 shall be composed of staff members from:

(a) the ESAs;

(b) the relevant competent authorities supervising the financial entities to which the critical ICT third-party service provider provides ICT services;

(c) the national competent authority referred to in Article 32(4), point (e), on a voluntary basis;

(d) one national competent authority from the Member State where the critical ICT third-party service provider is established, on a voluntary basis.

Members of the joint examination team shall have expertise in ICT matters and in operational risk. The joint examination team shall work under the coordination of a designated Lead Overseer staff member (the 'Lead Overseer coordinator').

ICT third-party service providers

9.1 Within 30 working days following the receipt of the annual oversight plan according to point 7.1, competent authorities should submit to the Lead Overseer a list of measures concerning critical ICT third-party providers which they plan to take during the period covered by the annual oversight plan.

9.2 Where competent authorities intend to take measures concerning the critical ICT third-party provider in addition to those included in the list referred to in point 9.1, competent authorities should submit to the Lead Overseer an updated list of measures concerning critical ICT third-party providers.

9.3 The list of measures referred to in points 9.1 and 9.2 should include the following information for every envisaged measure:

- the name of the relevant critical ICT third-party provider;
- the name of the financial entity using the relevant critical ICT third-party provider;
- description and envisaged reasonable timeline of the measure;
- reasoned explanation for the need to take such measure;
- other additional information as deemed useful by competent authorities.

9.4 The measures included in the lists referred to in points 9.1 and 9.2 have been agreed with the Lead Overseer, if competent authorities do not receive feedback in relation to those measures from the Lead Overseer:

- within 30 calendar days after the submission of the list referred to in point 9.1; and
- within 3 working days after the submission of the updated list referred to in point 9.2.

Guideline 10: Additional information exchanges between the Lead Overseer and competent authorities in relation to oversight activities

10.1 Within 10 working days following the adoption of the request for information to the critical ICT third-party service provider, the Lead Overseer should transmit 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)[23] and 37(1)[24].

[23] 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…

[24] 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.

10.2 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 ICT-related incidents reported by the critical ICT third-party service provider including description of incident, impact on critical ICT third-party service provider and on the financial entities it provides services to, resolution/closure of incident;
- 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)[25].

10.3 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 transmit those communications to the Lead Overseer and remind the critical ICT third-party service provider that the Lead Overseer is its primary point of contact for the purposes of all matters related to the oversight[26].

Section 4: Follow-up of the recommendations

Guideline 11: General principles for follow-up

11.1 The following general principles should apply to the follow-up to 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[27] making use of the services of the critical ICT third-party service providers;

[25] 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.

[26] 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.

[27] For example, the competent authorities have the following powers to follow up concerning the financial entities:

- Article 42(3): Competent authorities shall inform the relevant financial entities of the risks identified in the recommendations addressed to critical ICT third party service providers;
- Article 42(6): Competent authorities may, as a measure of last resort, following the notification and, if appropriate, the consultation as set out in DORA, take a decision requiring financial entities to temporarily suspend, either in part or completely, the use or deployment of a service provided by the critical ICT third party service provider until the risks identified in the recommendations addressed to critical ICT third party service providers have been addressed.

- 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[28].

Guideline 12: Information exchanges between the Lead Overseer and competent authorities to ensure the follow-up of recommendations

12.1 The Lead Overseer should transmit 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[29]:

- the notification of the critical ICT third-party service provider to follow the recommendations 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)[30].

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

- 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)[31].

---

[28] For example, the Lead Overseer has the following powers to follow up concerning the critical ICT third party service provider:

- 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 providers in relation to the recommendation;
- 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(a)(b)(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;
- Article 42(2): The Lead Overseer shall publicly disclose where a critical ICT third-party service provider fails to notify the Lead Overseer in accordance with paragraph 1 or where the explanation provided by the critical ICT third-party service provider is not deemed sufficient;
- Article 42(7): In case the critical ICT third party service provider refuses to endorse recommendations, 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.

[29] 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.

[30] 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.

[31] Article 35(1)(d): For the purposes of carrying out the duties laid down in this Section, the Lead Overseer shall have the power to issue recommendations...

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[32];
- 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). In case the critical ICT third-party service provider has not adequately implemented the recommendations, the assessment should at least cover the criteria a)-d) of Article 42(8)[33];
- the decision imposing a periodic penalty payment on the critical ICT third-party service provider according to Article 35(6)[34]. If the Lead Overseer opted not to disclose the periodic penalty payment to the public as per Article 35(10)[35], 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[36].

12.2 For the purpose of application of point 12.3, critical ICT third party service providers should be considered as not having endorsed in part or entirely recommendations addressed to them by the Lead Overseer in at least the following cases:

---

[32] 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.

[33] 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;

[34] 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.

[35] 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.

[36] 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.

- the critical ICT third-party service provider notified intention to comply with the recommendations, but they have not been adequately implemented by the critical ICT third-party service provider;
- the reasoned explanation of the critical ICT third-party service provider for not following the recommendations is not deemed sufficient by the Lead Overseer;
- the critical ICT third-party service provider failed to notify the Lead Overseer of its intention to follow the recommendations or provide a reasoned explanation for not following such recommendations.

12.3 In accordance with Article 42(10)[37], the competent authorities should transmit 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;
   - individual warnings issued by competent authorities according to Article 42(7)[38] and relevant information which allows the Lead Overseer to assess whether such 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 NIS 2 authorities prior to taking a decision, as referred to in Article 42(5)[39], 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;

[37] 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.

[38] 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.

[39] 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.

- the start of executing exit strategies and transition plans of the financial entities as referred to in Article 28(8)[40].

12.4 The ESAs, in consultation with competent authorities, should develop a template to facilitate the transmission of the information as defined in point 12.3.

Guideline 13: 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

13.1 The competent authorities should inform the Lead Overseer[41] 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)[42]. For the purpose of application of point 13.2, the competent authorities should provide the Lead Overseer with all relevant information regarding the possible decision and highlight if they intend to adopt an urgent decision.

13.2 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 share this assessment with the competent authorities concerned. Competent authorities should consider this non-binding assessment when deciding whether or not to issue the notification referred to in point 13.1.

13.3 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.

---

[40] Article 28(8): For ICT services supporting critical or important functions, financial entities shall put in place exit strategies…

Financial entities shall identify alternative solutions and develop transition plans enabling them to remove the contracted ICT services and the relevant data from the ICT third-party service provider and to securely and integrally transfer them to alternative providers or reincorporate them in-house.

[41] 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.

[42] 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.

Section 5: Final provisions

These Guidelines apply as from the date of the reporting requirement referred to on page 9.

The ESAs will undertake a review of the application of these Guidelines within four years after their publication.

6. Draft cost-benefit analysis / impact assessment

1. As per Article 16(2) of the founding regulation of the ESAs, the ESAs shall, where appropriate, analyse the related potential costs and benefits of issuing guidelines (impact assessment) and that analysis shall be proportionate in relation to the scope, nature and impact of the guidelines.
2. This analysis presents the impact assessment (IA) of the main policy options included in this Consultation Paper (CP) on the oversight cooperation and information exchange between the ESAs and CAs under DORA.

Problem identification

3. DORA introduces an oversight framework to the financial sector for all CTPPs designated in accordance with Article 31(1)(a).
4. In order to ensure a consistent and coherent supervisory approach and a level playing field where financial entities are using the ICT services provided by a CTPPs across Member States, it is important to have close cooperation between CAs and the ESAs through the mutual exchange of information and the provision of assistance in the context of relevant supervisory activities.
5. Moreover, as highlighted in Recital 93, a coordinated approach between the ESAs and CAs in the context of the exercise of tasks in the oversight framework is important to avoid duplications and overlaps in conducting measures aimed at monitoring the CTPP's risks.
6. In this context, the ESAs have been mandated under Article 32(7) to issue guidelines on the cooperation between the ESAs and the CAs covering the detailed procedures and conditions for the allocation and execution of tasks between CAs and the ESAs and the details on the exchanges of information which are necessary for CAs to ensure the follow-up of recommendations addressed to CTPPs.

Policy objectives

7. The Guidelines aim at ensuring that the ESAs and the CAs have:
    a) an overview of the areas where cooperation and/or exchange of information between CAs and the ESAs is needed in accordance with Article 32(7);
    b) a coordinated and cohesive approach between ESAs and CAs 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;

c) 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.

Baseline scenario

8. Recitals 93 and 97 as well as Article 48(2) highlight the importance of close cooperation and information exchange between the ESAs and CAs in the conduct of oversight activities. However, DORA does not include detailed provisions on the cooperation and exchanges of information necessary for the purpose of oversight activities.
9. In the absence of further clarifications on details on the exchanges of information and the allocation and execution of tasks between CAs and ESAs, there is a risk of lack of coordination and information exchange between CAs and ESAs, resulting potentially in duplications/overlaps in the measures directed at CTPPs and financial entities using ICT services of CTPPs and inconsistent/divergent supervisory approaches by CAs.

POLICY ISSUE 1 – GUIDELINE 5: INFORMATION FOR THE CRITICALITY ASSESSMENT TO BE SUBMITTED BY CAS TO THE OVERSIGHT FORUM

Options considered

10. For the purposes of designating the ICT third-party service providers that are critical for financial entities, CAs should transmit to the Oversight Forum:
    - Option A: Only the reports referred to in Article 31(10);
    - Option B: Only the register of information referred to in Article 28(3); or
    - Option C: The register of information referred to in Article 28(3) and any relevant additional information at the disposal of CAs.

Cost benefit analysis

11. The information referred to in Options A and B is not sufficient for the purpose of designating the ICT third-party service providers that are critical for financial entities. In order to assess the criticality, the Oversight Forum needs additional input from CAs, including, relevant quantitative or qualitative information to determinate/calculate the indicators for the criticality criteria set out in Article 31(2) (Option C). In order to avoid costs and burden for financial entities and CAs, CAs are not required gather any additional information from financial entities, but use the information they already have at their disposal.

Preferred option

12. Option C has been retained.

POLICY ISSUE 2 – GUIDELINE 13: 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

Options considered

13. CAs should inform the LO:

- Option A: After taking the decision as referred to in Article 42(6);
- Option B: After notifying the financial entity of the possibility of a decision being taken as referred to in Article 42(4); or
- Option C: Before notifying the financial entity of the possibility of a decision being taken as referred to in Article 42(4).

Cost benefit analysis

14. If CAs inform the LO of their decision only after it has been taken (Option A) or the financial entity has been notified of the possibility of a decision being taken (Option B), the CAs will not be able to consider at an early stage of the decision-making process, the LO's assessment of the potential impact of such decision on the CTPP and the LO's information about any inconsistent or divergent supervisory approaches where applicable. Options A and B could result in an unlevel playing field where financial entities are using the ICT services provided by CTPPs across Member States.
15. If CAs inform the LO before notifying the financial entity of the possibility of a decision being taken (Option C), CAs will be able to adequately consider the LO's assessment/information in their supervisory approaches, resulting in a more coordinated approach and a level playing for financial entities from a very early stage.

Preferred option

16. Option C has been retained.

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 deviations between the Guidelines and this table, the information included in the Guidelines apply.

Information exchange	Timeline	Related Article in the Level 1 text	GL
Section 1: General considerations			
LO and CAs to acknowledge receipt of information	Without undue delay after receiving the information	-	1.7
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 share with each other, relevant information from their dialogue with NIS 2 authorities	-		4.1
Section 2: Designation of CTPPs			
CAs to transmit the full register of information to the OF	Without undue delay following the receipt of the register of information	28(3)[43] 31(1)(a)[44], (2), (6)[45] and (10)[46] Article 35(2) of the ESAs' founding regulation[47]	5.1
CAs to also submit to the OF any relevant	-		5.2

[43] 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…

[44] 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.

[45] 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.

[46] 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....

[47] 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 provide additional available information acquired in their supervisory activities	-		5.3
LO to transmit to CAs information about the TPP that submitted a request to be designated as critical and 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	31(5)[48], (11)[49] and (13)[50]	6.1 (a)
LO to transmit to 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		6.1 (b)
Section 3: Core oversight activities			
LO to transmit to CAs the annual oversight plan and updates to the annual oversight plan	Within 10 working days following its adoption in September/October	33(4)[51]	7.1 and 7.2
LO to inform 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	36(1), 38(5)[52] and 39(3)[53]	8.1

[48] 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.

[49] 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).

[50] 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.

[51] 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.

[52] 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.

[53] 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.

Information exchange	Timeline	Related Article in the Level 1 text	GL
	case of an urgent investigation or inspection		
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)[54]	8.3
CAs to submit to the LO list of measures concerning CTPP which they plan to carry out during the period covered by the annual oversight plan	Within 30 working days following the receipt of the annual oversight plan	33(5)[55]	9.1
Where CAs intend to take measures concerning the CTPP in addition to those included in the list, CAs to submit to the LO, the updated list of measures concerning CTPPs	-		9.2
LO to transmit 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)[56],37(1)[57] and 37(5)[58]	10.1

[54] 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.

[55] Article 33(5): Once the annual oversight plans have been adopted and notified to the critical ICT third party service providers, competent authorities may take measures concerning such critical ICT third party service providers only in agreement with the Lead Overseer.

[56] 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…

[57] 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.

[58] 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.

Information exchange	Timeline	Related Article in the Level 1 text	GL
LO to inform CAs of: • major ICT-related incidents reported by the CTPP; • 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)[59]	10.2
CAs to transmit to the LO, communications of the CTPP with the CAs for the purposes of all matters related to the oversight	-	33(1)[60]	10.3
Section 4: Follow-up of the recommendations			
LO to transmit 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)[61] and 42(1)[62]	12.1 a)
LO to transmit 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		12.1 b)

[59] 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.

[60] 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.

[61] 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.

[62] 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.

Information exchange	Timeline	Related Article in the Level 1 text	GL
LO to transmit to CAs: • assessment as to whether the CTPP's explanation for not following the LO's 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	Within 10 working days following the adoption by the LO	35(1)(c), 35(6)[63], 35(10)[64], 42(1), 42(8)(a-d)[65]	12.1 c)
CAs to transmit to LO: • notification to the financial entity of the	Within 10 working days following the	42(4)[66], (7)[67] and (10)[68]	12.3 a)

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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.

[68] 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.

Information exchange	Timeline	Related Article in the Level 1 text	GL
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	adoption by the CA		
Where possible, CAs to transmit to LO, outcome of the consultation with NIS 2 authorities prior to taking a decision.	Within 10 working days following the consultation	42(5)[69]	12.3 b)
CAs to transmit 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)[70]	12.3 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; • provide all relevant information regarding the decision; • highlight if they intend to carry out an urgent decision	-	42(4) and (10)	13.1
LO to share with 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 13.1		13.2

[69] 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.

[70] 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.

Information exchange	Timeline	Related Article in the Level 1 text	GL
	or With the shortest possible delay in case of an urgent decision		