JC 2024 35

17 July 2024

Final Report

Draft Regulatory Technical Standards on harmonisation of conditions enabling the conduct of the oversight activities

Contents

1. Executive Summary

1. One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to harmonise the conditions enabling the oversight activities and create a new oversight framework for the oversight of critical third party service providers in Europe.
2. Article 41(1) of the DORA mandates the European Supervisory Authorities (ESAs) to develop through the Joint Committee common draft Regulatory Technical Standards further specifying:
    - the information to be provided by an ICT third-party service provider in the application for a voluntary request to be designated as critical under Article 31(11);
    - the content, structure and format of the information to be submitted, disclosed or reported by the ICT third-party service providers pursuant to Article 35(1), including the template for providing information on subcontracting arrangements;
    - the details of the competent authorities' assessment of the measures taken by critical ICT third-party service providers based on the recommendations of the Lead Overseer pursuant to Article 42(3)
3. This report follows a consultation paper (CP) which presented a first draft of the RTS and 8 questions and was open to comments from the public from 8 December 2023 to 4 March 2024.

4. A total of 44 responses were received to the public consultation, covering all sectors. The feedback received is presented in detail in Sections 5 and 6.

5. The ESAs assessed the concerns raised to decide which changes, if any, should be made to the draft RTS. In the light of the comments received, the ESAs agreed with some of the proposals and their underlying arguments and have introduced changes to the draft RTS.

6. The main changes are related to the scope of the information to be provided by an ICT third party service provider in the application to be designated as critical , the relevant identification code , the scope and content of the information to be provided by the critical third-party service providers to the Lead Overseer including information about their subcontracting arrangements and the competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer.

7. More information on the feedback received and how this was taken on board by the ESAs is provided in the "Feedback Statement".

Next steps

8. The ESAs will submit the final draft RTS to the European Commission for adoption. Following its adoption in the form of a Commission Delegated Regulation, it will then be subject to scrutiny of the European Parliament and the Council before publication in the Official Journal of the European Union.

9. The expected date of application of these technical standards is 17 January 2025.

2. Background and rationale

2.1 Introduction

1. The framework on digital operational resilience for the financial sector established by Regulation (EU) 2022/2554 introduces a Union oversight framework for the information and communication technology (ICT) third-party service providers (TPPs) to the financial sector designated as critical in accordance with Article 31 of that Regulation.

2. In this context, the ESAs have been mandated under Article 41(1) of Regulation (EU) 2022/2554 to develop draft regulatory technical standards (RTS) to harmonise the conditions enabling the conduct of oversight activities. According to the mandate, the draft RTS shall specify:

   (a) the information to be provided by an ICT third–party service provider in the application for a voluntary request to be designated as critical under Article 31(11);

   (b) the content, structure and format of the information to be submitted, disclosed or reported by the ICT third–party service providers to the Lead Overseer pursuant to Article 35(1), including the template for providing information on subcontracting arrangements;

   (c) the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the ESAs and from the relevant competent authorities, their designation, tasks, and working arrangements;

   (d) the details of the CAs' assessment of the measures taken by CTPPs based on the recommendations of the Lead Overseer.

3. While developing the draft RTS, the ESAs have decided to divide the mandate of Article 41(1) of Regulation (EU) 2022/2554 in two separate RTS: an RTS focusing on the areas of the mandate having a direct impact on financial entities and ICT third party service providers (points (a), (b) and (d) above) and another RTS on the requirements to be followed by the competent authorities in relation to the joint examination team (point (c) above). The reason of this decision is related to the different specific nature of the information included in the empowerment given by Article 41: the empowerments included in points (a), (b) and (d) have a clear impact on the market participants (either ICT third-party providers or financial entities), while the one included in point (c) has an impact only to the supervisory community.

4. These draft RTS cover the areas included in points (a), (b) and (d) of Article 41(1) of Regulation 2022/2554.

5. A Consultation paper (CP) on the draft RTS was published on 8 December for a three-month consultation period, which closed on 4 March 2024. The ESAs received 44 responses from a variety of market participants across the financial sector. The ESAs have assessed the responses from the public consultation and have made changes to the draft RTS where relevant. Feedback related to the full set of comments received can be found in the " Feedback Statement" section.

2.2 Rationale

6. The DORA oversight framework only applies to ICT third-party service providers that are critical to the European financial sector. CTPPs can either be designated by the ESAs via a designation mechanism under Article 31(1)(a) of the DORA or via a voluntary request from the ICT third-party service providers to be designated as critical under Article 31(11) of the DORA. Given the short timeframe introduced by the DORA for the ESAs to carry out the assessment of the voluntary request from the ICT third-party service providers, it is of paramount importance that the application submitted is complete. In case the application submitted is not complete, the ESAs will refuse the application asking the applicant ICT third-party service provider to re-submit a complete one.

7. Regulation 2022/2554 grants a number of powers to the Lead Overseer (LO) in respect of CTPPs, such as the possibility for the LO to request all relevant information and documentation from the CTPP which is necessary for the LO to carry out its duties.

8. According to Article 35(1)(c) of Regulation 2022/2554, the LO has the power to request, after the completion of the oversight activities, reports specifying the actions taken or remedies implemented by the CTPP in relation to the recommendations. In order to facilitate ongoing monitoring of the implementation of the recommendations, these reports should consist of interim and final progress reports as well as related supporting documents.

9. With regard to the follow-up to the issuance of recommendations, CAs and the LO have a complementary responsibility. While CAs are responsible for the follow-up with the relevant financial entities under their supervision concerning the risks identified in the recommendations, the LO is responsible for monitoring the implementation of the recommendations issued to the CTPP. In order to ensure a coordinated and cohesive approach between ESAs and CAs in the cooperation for the purpose of oversight activities, they should mutually exchange all relevant findings concerning CTPPs which are necessary for them to carry out their respective duties.

10. In particular, in case of severe risks which are shared among a large number of financial entities in several Member States, upon request by the LO, CAs should share relevant information about their assessment of the identified risks with the LO. Such information is intended to help the LO to evaluate the actions taken or remedies implemented by the CTPP in relation to the recommendations.

3. Draft Regulatory Technical Standards

COMMISSION DELEGATED REGULATION (EU) …/…

of DD Month YYYY

supplementing Regulation 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards on harmonisation of conditions enabling the conduct of the oversight activities

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

Having regard to 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[1], and in particular Article 41(2), second subparagraph, thereof,

Whereas:

(1) The framework on digital operational resilience for the financial sector established by Regulation (EU) 2022/2554 introduces a Union oversight framework for the information and communication technology (ICT) third-party service providers to the financial sector designated as critical in accordance with Article 31 of that Regulation.

(2) Considering that Article 31(11) of Regulation (EU) 2022/2554 grants a limited time period of 6 months from the receipt of the application, it is crucial that the European Banking Authority, European Insurance and Occupational Pensions Authority, and European Securities and Markets Authority (collectively European Supervisory Authorities or ESAs), receive a voluntary request to be designated as critical from a ICT third-party service provider, that is complete. In case the application submitted is not complete, the relevant ESA should reject the application and request the missing information.

(3) Regulation (EU) 2022/2554 mandates the Lead Overseer to carry out a comprehensive assessment of the ICT risks that ICT third party service providers pose to financial entities. In order to carry out this assessment, Regulation (EU) 2022/2554 equips the Lead Overseer with power to request information covering areas directly or indirectly related to the ICT services the critical ICT third-party service providers provide to the financial entities.

[1] OJ L 333, 27.12.2022, p. 1.

(4) The request to critical ICT third-party service providers to transmit to the Lead Overseer information that is necessary to carry out its duties, including the one on subcontracting arrangements, should be done considering the second subparagraph of Article 33(2) of Regulation (EU) 2022/2554.

(5) The legal identification of ICT third-party service providers within the scope of this Regulatory Technical Standards should be aligned with the identification code set out in Commission Implementing Regulation adopted in accordance with Article 28(9) from Regulation (EU) 2022/2554.

(6) As a follow-up to the recommendations issued by the Lead Overseer to critical ICT third-party providers, the Lead Overseer should monitor critical ICT third party service providers' compliance with the recommendations. With a view to ensure a level playing field and an efficient and effective monitoring of the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service providers in relation to these recommendations, the Lead Overseer should be able to require the reports referred to in Article 35(1), point (c), of Regulation (EU) 2022/2554, which should be intended as interim progress reports and final reports.

(7) Also for the purpose of assessment specified in Article 42(2) of Regulation (EU) 2022/2554, according to which Lead Overseer is obliged to evaluate whether explanation provided by critical ICT third-party provider is sufficient, the notification to the Lead Overseer by the critical ICT third-party service provider of its intention to follow the recommendations received should be complemented by such explanation in the form of a remediation plan. In such remediation plan the critical ICT third-party service provider describes the actions and the measures planned to mitigate the risks of the recommendations, along with their respective timelines.

(8) As the information submitted to the Lead Overseer by critical ICT third-party service providers may be of confidential nature, the Lead Overseer should provide the critical ICT third-party service provider with secure electronic channels for information submission.

(9) The critical ICT third-party service provider should always provide information in a clear, concise and complete manner. Considering the unified nature of the European oversight framework, information should be submitted, disclosed or reported by the ICT third-party service providers pursuant to Article 35(1) in English.

(10) As the Lead Overseer is expected to assess the subcontracting arrangements of the critical ICT third-party service provider, a template needs to be developed for providing information on those arrangements. The template should take into account the fact that the critical ICT third-party service providers have different structures than financial entities. The templates should therefore not fully mirror the templates of the register of information referred to in Article 28(3) of Regulation (EU) 2022/2554.

(11) Once the recommendations to a critical ICT third-party service provider are issued by the Lead Overseer, and competent authorities have informed the relevant financial entities of the risks identified in that recommendations, the Lead Overseer should monitor and assess the implementation by the critical ICT third-party service provider

of the actions and remedies to comply with the recommendations. Competent authorities should monitor and assess the extent to which the financial entities are exposed to the risks identified in these recommendations. With a view to maintain a level playing field while carrying out their respective tasks, particularly when the risks identified in the recommendations are severe and shared among a large number of financial entities in multiple Member States, both the competent authorities and the Lead Overseer should share among each other relevant findings which are necessary for them to carry out their respective tasks. The objective of the information sharing is to ensure that the feedback of the Lead Overseer to the critical ICT third-party provider in relation to the actions and remedies the latter is implementing takes into account the impact on the risks of the financial entities, and that the supervisory activities performed by the competent authorities are informed by the assessment carried out by the Lead Overseer.

(12) To allow for an efficient and effective sharing of information, the competent authorities should assess, as part of their supervisory activities, the extent to which the financial entities supervised by them are exposed to the risks identified in the recommendations. This assessment should be carried out in a proportionate and risk-based manner. Lead Overseer should request the competent authorities to share the results of this assessment in the specific cases when the risks associated with the recommendations are severe and shared among a large number of financial entities in multiple Member States. To make the best use of the resources of the competent authorities, when asking to provide the results of this assessment, the Lead Overseer should always take into account that the objective of these requests is to evaluate the actions and remedies of the critical ICT third-party providers.

(13) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Supervisory Authorities.

(14) The Joint Committee of the European Supervisory Authorities has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council[2], the Insurance and Reinsurance Stakeholder Group and the Occupational Pensions Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council[3], and the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[4].

---

[2] 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).

[3] Regulation (EU) No 1094/2010 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).

[4] 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).

HAS ADOPTED THIS REGULATION:

CHAPTER I

INFORMATION TO BE PROVIDED BY ICT THIRD-PARTY SERVICE PROVIDERS IN THE APPLICATION FOR A VOLUNTARY REQUEST TO BE DESIGNATED AS CRITICAL

Article 1

Information to be provided by ICT third-party service provider in the application for a voluntary request to be designated as critical

1. For the purpose of Article 31(11) of Regulation (EU) 2022/2554, the information to be provided by an ICT third-party service provider in the reasoned application for a voluntary request to be designated as critical in accordance with Article 31(1), point (a), of Regulation (EU) 2022/2554 shall include all of the following:

   (a) name of the legal entity;

   (b) legal entity identification code;

   (c) country where the legal entity has registered office;

   (d) description of the corporate structure including at least the following information on its parent company and other related undertakings to the applicant ICT third-party service providers providing ICT services to Union financial entities, where applicable;

      (i) name of the legal entities;

      (ii) legal entity identification code,;

      (iii) country where the legal entity has registered office;

   (e) an estimation of the market share of the ICT third-party service provider in the Union financial sector and estimation of market share per type of financial entity as referred to in Article 2(1) of Regulation (EU) 2022/2554 as of the year of application and the year before application;

   (f) a clear description of each ICT service provided by the ICT third-party service provider to Union financial entities including:

      (i) a description of the nature of business and the type of ICT services provided to financial entities;

      (ii) a list of the functions of financial entities supported by the ICT services provided, where available;

(iii) information whether the ICT services provided to financial entities support critical or important functions, where available;

(g) a list of financial entities that make use of the ICT services provided by the ICT third-party service provider, including the following information for each of the financial entity serviced, where available:

(i) name of the legal entity;

(ii) legal entity identification code, where known to the ICT third-party service provider;

(iii) type of financial entity as specified in Article 2(1) of Regulation 2022/2554;

(iv) the geographic location of the legal entity, from which ICT services are provided, where available;

(h) a list of the critical ICT third-party service providers included in the latest available list of such providers published by the ESAs pursuant to Article 31(9) of Regulation (EU) 2022/2554 that rely on the services provided by the applicant ICT third-party service provider, where available;

(i) a self-assessment by the ICT third-party service provider including the following:

(i) the degree of substitutability for each ICT service provided by the ICT third-party service provider considering:

1. the market share of the ICT third-party service provider in the Union financial sector;

2. the number of known relevant competitors per type of ICT services, or group of ICT services;

3. description of specificities relating to the ICT services offered, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;

(ii) knowledge about the availability of the alternative ICT third-party service providers to provide the same ICT services as the ICT third-party service provider submitting the application;

(j) information on future strategy and investment plans in relation to the provision of ICT services and infrastructure to financial entities in the Union, including any planned changes in the group or management structure, entry into new markets or activities;

(k) information on subcontractors which have been designated as critical ICT third-party service providers pursuant to Article 31(1), point (a), of Regulation (EU) 2022/2554;

(l) other reasons relevant for the ICT third-party service provider's application to be designated as critical.

2. Where the ICT third-party service provider belongs to a group, the information referred to in paragraph 1 shall be provided in relation to the ICT services provided by the group as a whole.

3. As part of their review of the application received from the ICT third-party service provider, the ESAs may request clarifications of the information submitted.

Article 2

Assessment of completeness of application

1. The ICT third-party service provider shall submit its complete reasoned application, which contains all information necessary for the purpose of designation as critical in Article 1 of this Regulation, to the relevant ESA, via means determined by the ESAs.

2. Where the relevant ESA considers that information provided in the application is incomplete, it shall reject the application and request the missing information.

CHAPTER II

INFORMATION FROM CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS TO THE LEAD OVERSEER

Article 3

Content of information provided by critical ICT third-party service providers

1. Critical ICT third-party service providers shall provide to the Lead Overseer, upon its request, any information deemed necessary by the Lead Overseer to carry out its oversight duties in accordance with the requirements of Regulation (EU) 2022/2554. Critical ICT third-party service providers shall transmit this information according to the structure and format described in Article 5 of this Regulation, within the time limits and with the frequency set by the Lead Overseer.

2. Without prejudice to paragraph 1, upon Lead Overseer request, the critical ICT third-party service provider shall submit all of the following information:

(a) information about the arrangements, and copies of contractual documents, between:

(i) the critical ICT third-party service provider and the financial entities referred to in Article 2(1) of Regulation (EU) 2022/2554;

(ii) the critical ICT third-party service provider and its subcontractors with a view to capture the technological value chain that effectively underpins the ICT services provided to the financial entities in the Union

(b) information about the organisational and group structure of the critical ICT third-party service provider, including identification of all entities belonging to the same group that directly or indirectly provide ICT services to financial entities in the Union;

(c) information about the major shareholders, including their structure and geographical spread, of the entities that:

(i) without prejudice to Article 3(2), point (b), of this Regulation, hold, solely or jointly with their linked entities, 25% or more of the capital or voting rights of the critical ICT third-party service provider;

(ii) hold the right to appoint or remove a majority of the members of the administrative, management, or supervisory body of the critical ICT third-party service provider; or

(iii) control, pursuant to an agreement, a majority of shareholders' or members' voting rights in the critical ICT third-party service provider;

(d) information about the critical ICT third-party service provider's own estimation of its market share, per type of services, in the relevant markets where it operates;

(e) information about the internal governance arrangements of the critical ICT third-party service provider, including the structure with lines of governance responsibility and accountability rules;

(f) the meeting minutes of the critical ICT third-party service provider's management body and any other internal relevant committees, which relate in any way to activities and risks concerning ICT third-party services supporting functions of financial entities within the Union;

(g) information about the ICT security and data protection frameworks, including personal and non-personal data, of the critical ICT third party service provider, including relevant strategies, objectives, policies, procedures, protocols, processes, control measures to protect sensitive data, access controls, encryption practices, incident response plans, and compliance with all relevant regulations and national and international standards where applicable;

(h) information about the mechanisms the critical ICT third-party service provider offers to the Union financial entities for data portability, application portability and interoperability;

(i) information about the exact location of the data centres and ICT production centres used in any way for the purposes of providing services to the financial entities, including a list of all relevant premises and facilities of the critical ICT third-party service provider, including outside the Union;

(j) information about provision of services by the critical ICT third-party service provider from third countries, including information on relevant legal provisions applicable to personal and non-personal data processed by the ICT third-party provider in different jurisdictions;

(k) information about measures taken to address risks arising from the provision of ICT services by the critical ICT third-party service provider and their subcontractors from third-countries;

(l) information about the risk management framework and the incident management framework, including policies, procedures, tools, mechanisms, and governance arrangements of the critical ICT third-party service provider and of its subcontractors. Information shall also include list and description of major incidents with direct or indirect impact on financial entities within the Union, including relevant details to determine the significance of the incident on financial entities and assess possible cross-border impacts. Information about the change management framework, including policies, procedures, and controls of the critical ICT third-party service provider and its subcontractors

(m) information about the overall response and recovery framework of the critical ICT third-party service provider, including business continuity plans and related arrangements and procedures, software development lifecycle policy, response and recovery plans and related arrangements and procedures, backup policies arrangements and procedures;

(n) information about performance monitoring, security monitoring, and incident tracking as well as information about reporting mechanisms related to service performance, incidents, and compliance with agreed-upon service level agreements (SLAs) and service level objectives (SLOs) or similar arrangements between critical ICT third-party service providers and financial entities in the Union;

(o) information about the ICT third-party management framework of the critical ICT third-party service provider, including strategies, policies, procedures, processes, and controls including details on the due diligence and risk assessment performed by the critical ICT third-party service provider on its subcontractors before entering into an agreement with them and to monitor the relationship covering all relevant ICT and counterparty risks;

(p) extractions from the monitoring and scanning systems of the critical ICT third-party service provider and of its subcontractors, covering but not limited to network monitoring, server monitoring, application monitoring, security monitoring, vulnerability scanning, log management, performance monitoring,

incident management and measurements against reliability goals, such as Service Level Objectives;

(q) extractions from any production, pre-production and test system or application used by the critical ICT third-party service provider and its subcontractors, to provide directly or indirectly services to financial entities in the Union;

(r) compliance and audit reports as well as any relevant audit findings, including audits performed by national authorities in the Union and outside the Union where cooperation agreements with the relevant authorities provide for such information exchange, or certifications achieved by the critical ICT third-party service provider or its subcontractors, including reports from internal and external auditors, certifications, or compliance assessments with industry-specific standards. This includes information about any type of independent testing of the resilience of the ICT systems of the critical ICT third-party service provider, including any type of threat led penetration testing carried out by the ICT third-party service provider;

(s) information about any assessments carried out by the critical ICT third-party service provider upon its request or on its behalf evaluating the suitability and integrity of individuals holding key positions within the critical ICT third-party service provider;

(t) information about the remediation plan to address recommendations according to Article 4 of this Regulation, and relevant related information to confirm remedies have been implemented;

(u) information about employee training schemes and security awareness programs, which shall include information about the investments, resources and methods of the critical ICT third-party service provider in training its staff to handle sensitive financial data and maintain high levels of security;

(v) information about the activities of the critical ICT third-party service provider and financial statements, including information on the budget and resources related to ICT and security.

Article 4

Information from critical ICT third-party providers after the issuance of recommendations

1. In accordance with Article 35(1), point (c), of Regulation (EU) 2022/2554 and as part of the notification to the Lead Overseer of its intention to comply with the recommendations pursuant to Article 42(1) of that Regulation, the critical ICT third-

party service provider shall provide to the Lead Overseer a remediation plan outlining the actions and remedies that the critical ICT third-party service provider plans to implement in order to mitigate the risks identified in the recommendations. The remediation plan shall be consistent with the timeline set by the Lead Overseer for each recommendation.

2. To enable the monitoring of the implementation of 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 received, the critical ICT third-party service provider shall share with the Lead Overseer upon request:

   (a) interim progress reports and related supporting documents specifying the progress of the implementation of the actions and measures set out in the remediation plan provided by the critical ICT third party provider to the Lead Overseer within the timeline defined by the Lead Overseer;

   (b) final reports and related supporting documents specifying the actions that have been taken or the remedies that have been implemented by the critical ICT third-party service provider in order to mitigate the risks identified in the recommendations received.

Article 5

Structure and format of information provided by critical ICT third-party service providers

1. The critical ICT third-party service provider shall provide the requested information to the Lead Overseer through the dedicated secure electronic channels indicated by the Lead Overseer in its request.

2. When providing information to the Lead Overseer, the critical ICT third-party providers shall:

   (a) follow the structure indicated by the Lead Overseer in its information request;

   (b) clearly locate the relevant piece of information in the submitted documentation.

3. Information submitted, disclosed or reported to the Lead Overseer by the critical ICT third-party service provider shall be in English.

Article 6

Information on subcontracting arrangements provided by critical ICT third-party service providers

A critical ICT third-party service provider which is required to share information on subcontracting arrangements shall provide the information according to the structure and the template set out in Annex I of this Regulation.

CHAPTER III

COMPETENT AUTHORITIES' ASSESSMENT OF THE MEASURES TAKEN BY CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS BASED ON RECOMMENDATIONS OF THE LEAD OVERSEER

Article 7

Competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer

1. As part of their supervision of financial entities, competent authorities shall assess the impact on the financial entities of the measures taken by critical ICT third-party service providers based on the recommendations of the Lead Overseer. This assessment shall reflect a risk-based approach and the principle of proportionality.

2. When conducting the assessment referred to in paragraph 1, competent authorities shall take into account all of the following:

   (a) the adequacy and the coherence of the corrective and remedial measures implemented by the financial entities under their remit to mitigate those risks, if any;

   (b) the assessment made by the Lead Overseer of the compliance with the measures and actions included in the remediation plan by the critical ICT third-party service provider where it has impacts on the exposure of the financial entities under their remit to the risks identified in the recommendations;

   (c) the view of competent authorities designated or established in accordance with Directive (EU) 2022/2555, where those competent authorities have been consulted in accordance with Article 42(5) of Regulation (EU) 2022/2554;

   (d) whether the Lead Overseer has considered the actions and remedies implemented by the critical ICT third-party service provider as adequate to mitigate the exposure of the financial entities under their remit to the risks identified in the in recommendations.

3. Upon request from the Lead Overseer, the competent authority shall provide in reasonable time the results of the assessment set out in paragraph 1. When requesting the

results of this assessment, the Lead Overseer shall consider the principle of proportionality and the magnitude of risks associated with the recommendation, including the cross-border impacts of these risks when impacting financial entities operating in more than one Member State.

4. Where relevant, competent authorities shall request to financial entities any information necessary to carry out the assessment specified in paragraph 1.

CHAPTER IV

FINAL PROVISIONS

Article 8

Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 17 January 2025. This Regulation shall be binding in its entirety and directly applicable in all Member States.

ANNEX

Annex I

Template for sharing information on subcontracting arrangements

Information Category	Key Information Elements
General Information	• Name of the critical ICT third-party service provider • Identification code of the critical ICT third-party service provider • Name of contact person and contact details of the critical ICT third-party serice provider • Date of sharing the information
Overview of Subcontracting Arrangements	• Mapping of the subcontracting arrangements, including a short description of the purpose and scope of the subcontracting relationships (including an indication on the level of criticality or importance of the subcontracting arrangements for the critical ICT third-party provider) • Specification and description of the types of ICT services subcontracted and their significance to the ICT services provided to financial entities, in line with *ITS to establish the templates composing the register of information*. • When specifying the types of ICT services, please refer to the list in Annex IV of the *ITS to establish the templates composing the register of information*
Subcontractors' Information	• Name and legal entity details (including identification code) of each subcontractor involved • Contact information of key staff responsible for each of the subcontracting relationships in the critical ICT third-party provider management structure • Overview for each subcontractor of the expertise, experience and qualifications related to the contracted ICT services
Description of Services Provided by Subcontractors	• Detailed description of the specific ICT services provided by each subcontractor • Breakdown of the responsibilities and tasks allocated to subcontractors • Information on the level of access subcontractors have to sensitive data or systems regarding the ICT services provided to financial entities

Information Category	Key Information Elements
	• Information on the sites from which the services of subcontractors are provided and on the measures taken to address risks arising from services provided outside the Union
Subcontracting Governance and Oversight	• Description of the contractual and governance framework in place to manage subcontracting relationships, including clauses restricting the usage of sensitive data • Explanation of the processes for selecting, engaging and monitoring subcontractors • Overview of performance metrics, service level objectives and agreements, and key performance indicators used to assess subcontractors' performance and reliability monitoring
Risk Management and Compliance	• Assessment of the subcontractors' risk profiles and potential impact on the ICT services provided to financial entities • Explanation of the risk mitigation measures implemented to address subcontracting-related risks • Details of subcontractors' compliance with relevant regulations, data protection requirements and industry standards
Business Continuity and Contingency Planning	• Overview of the subcontractors' business continuity and response and recovery plans • Description of the arrangements in place to ensure service continuity in case of disruptions or termination by the subcontractor • Frequency of tests of the business continuity plans and response and recovery plans by the subcontractors, dates of the latest tests over the past 3 years, and specification if the critical ICT third-party service provider has been involved in those tests
Reporting	• Description of the reporting mechanisms and frequency of reporting between the critical ICT third-party service provider and its subcontractors
Remediation and Incident Management	• Outline of the procedures for addressing subcontractor-related incidents, breaches or non-compliance
Certifications and Audits	• Information on any certifications, independent audits or assessments conducted on subcontractors to validate their security controls, quality standards or regulatory compliance

Information Category	Key Information Elements
	• Date and frequency of the audits of the subcontractors conducted by the critical ICT third-party service provider

4. Impact assessment

1. In accordance with Article 10(1) of Regulation (EU) No 1093/2010 (EBA Regulation), of Regulation (EU) No 1094/2010 (EIOPA Regulation) and Regulation (EU) No 1095/2010 (ESMA Regulation), any draft regulatory technical standards developed by the ESAs shall be accompanied by an Impact Assessment (IA) to analyse 'the potential related costs and benefits' of the technical standard.
2. The following paragraphs present the IA of the main policy options included in this Consultation Paper (CP) on the harmonization of conditions enabling the conduct of oversight activities under Article 41(1) points (a), (b) and (d), of Regulation (EU) 2022/2554 (DORA).

Problem identification

3. DORA introduces an oversight framework for the ICT third-party service providers designated as critical according to Article 31(1)(a) of that Regulation. In this context, Article 41(1) points (a), (b) and (d) of the DORA mandates the ESAs to develop draft regulatory technical standards (RTS) to specify:
    - the information to be provided by an ICT third–party service provider in the application for a voluntary request to be designated as critical under Article 31(11) of the DORA;
    - the content, structure and format of the information to be submitted, disclosed or reported by the ICT third–party service providers to the Lead Overseer pursuant to Article 35(1) of the DORA, including the template for providing information on subcontracting arrangements;
    - the details of the competent authorities' assessment of the measures taken by critical ICT third–party service providers based on the recommendations of the LO pursuant to Article 42(3) of the DORA.
4. Article 41(1) (c) of the DORA mandates the ESAs to harmonise through an RTS another element of the conditions enabling the conduct of the oversight activities, namely "*the criteria for determining the composition of the joint examination team […], their designation, tasks, and working arrangements*". As further detailed in the section dedicated to policy options and outlined in the introductory part of this consultation paper, the ESAs have decided to develop a dedicated RTS covering that part of the mandate of Article 41.
5. This impact assessment does not cover the requirements set out in DORA in relation to the areas covered by the draft RTS, but it focuses only on the specific provisions of the draft RTS and assesses the implications of the policy issues considered by the ESAs while developing the draft RTS.

Policy Objectives

6. The objective of the draft RTS is threefold:
    - as any application by an ICT third-party provider for a voluntary request to be designated as critical shall be reasoned, the objective of the regulatory technical standards is to enable the Lead Overseer to carry out a detailed assessment of all the criteria set out in Article 31(2) of the DORA;

- as the Lead Overseer has the mandate to perform a risk assessment of the ICT third-party provider designated as critical according to Article 31(1)(a) of the DORA, the objective of the regulatory technical standards is to provide clarity to all involved parties on the information to be exchanged and the process for such information exchange including information to be exchanged according to Article 35 of the DORA; and
- as following the execution of the oversight activities, the Lead Overseer may issue recommendations to the ICT third-party providers designated as critical, the objective of the regulatory technical standards is to enable the Lead Overseer and competent authorities to carry out appropriate follow-up activities.

Baseline scenario

7. DORA establishes a Union oversight framework of critical ICT third-party service providers for the financial sector that allows for a continuous monitoring of the activities of ICT third-party service providers that are critical to financial entities, while ensuring that the confidentiality and security of customers other than financial entities is preserved. Hence, the baseline scenario for the areas in scope of the present regulatory technical standards is very limited.
8. However, it is important to note that certain potential third-party service providers designated as critical under DORA may already be subject to supervision at national level in the context of existing outsourcing regulations. In this regard some information-sharing arrangements might already be in place. The knowledge and expertise of the supervisory community has been factored in the definition of the list of information for the ICT third-party service providers designated as critical considering the tasks of the Lead Overseer.
9. In relation to the oversight, the baseline scenario are the roles and responsibilities of the DORA and the principle of cooperation between Lead Overseers and competent authorities in the oversight of ICT third-party service provides designated as critical to achieve the overall aim of the oversight framework, namely to ensure financial stability and market integrity in the digital age.

General policy options

POLICY ISSUE 1: STRUCTURE OF THE DRAFT RTS

Options considered

10. Option A: including in a single regulatory technical standard all the areas referred to in Article 41(1) of the DORA, i.e., covering those that have a direct impact on financial entities and ICT third party service providers (Article 41(1) points (a), (b) and (d) of the DORA) and the one that must be followed by the ESAs and the relevant competent authorities in relation to the joint examination team (Article 41(1) point (c) of the DORA).
11. Option B: dividing the mandate of Article 41(1) of the DORA in two separate RTS: one focusing on the areas of the mandate having a direct impact on financial entities and ICT third-party service providers (Article 41(1) points (a), (b) and (d) of the DORA) and the other one on the requirements

to be followed by the supervisory community in relation to the joint examination team (Article 41(1)(c) of the DORA).This principle was established by the EBA in a previous RTS[5].

Cost-benefit analysis

12. The empowerment given by Article 41(1) of the DORA contains two different sets of requirements in terms of market impacts: the empowerments included in points (a), (b) and (d) have a clear impact on the market participants (either ICT third-party providers or financial entities), while the one included in point (d) has an impact only to the supervisory community. In light of the above considerations, in order to give the necessary time to the market stakeholders to participate to this public consultation, the ESAs have decided to give priority to the empowerments included in points (a), (b) and (d).

Preferred option

13. Option B has been retained.

Policy options relating to Chapter II – Information from critical ICT third-party service providers to the Lead Overseer

POLICY ISSUE 2: LIST OF INFORMATION TO BE PROVIDED BY CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS

Options considered

14. Option A: ICT third-party service providers designated as critical should submit a specific, defined set of information to the Lead Overseer that is exhaustive and comprehensive in its nature.

15. Option B: ICT third-party service providers designated as critical to submit information to the Lead Overseer that is not predetermined but can be expanded as needed to accommodate emerging needs.

Cost-benefit analysis

16. As ICT and technology risks are continuously evolving, circumstances change on an ongoing basis and new trends emerge, an open list of information is considered more appropriate as it allows for flexibility and adaptation, making it easier to incorporate new trends as they become relevant. This adaptability is considered crucial for staying responsive to evolving market conditions. Such a list should not prevent the possibility for the Lead Overseer to ask any additional relevant information needed by the Lead Overseer to monitor the provision of the ICT services provided by the critical ICT third party providers and to carry out its oversight duties in accordance with the requirements of the DORA. The Annex provides a mapping between the minimum required topics covered by the assessment of the Lead Overseer (Article 33(3)of the DORA) and article 3(2) of the present RTS.

Preferred option

17. Option B has been retained.

[5] EBA Regulatory Technical Standards on Own Funds: https://www.eba.europa.eu/regulation-and-policy/own-funds/draft-regulatory-technical-standards-on-own-funds.

POLICY ISSUE 3: REMEDIATION PLAN

18. Option A: A critical ICT third-party service provider to provide the Lead Overseer only with information about implemented actions or remedies in relation to the recommendations received from the Lead Overseer.

19. Option B: A critical ICT third-party service provider to provide the Lead Overseer not only with information about implemented actions or remedies in relation to the recommendations received from the Lead Overseer, but also with information about the envisaged actions or remedies during their implementation.

Cost-benefit analysis

20. In accordance with Article 35(1) point (c) of the DORA and as part of the notification to the Lead Overseer of its intention to comply with the recommendations received pursuant to Article 42(1) of the same Regulation, the critical ICT third-party service provider shall provide to the Lead Overseer a remediation plan outlining the actions and the measures, and respective timeline, that the critical ICT third-party service provider plans to implement in order to mitigate the risks identified in the recommendations. To enable end-to-end monitoring of the implementation of the actions or the remedies by the critical ICT third-party service provider in relation to the recommendations received and to facilitate continuous communication between the critical ICT third-party service provider and the Lead Overseer, it is considered important that the critical ICT third-party service provider shares information about the envisaged actions or remedies already during the implementation phase and not only via a final report, i.e., when the actions and remedies have been implemented.

Preferred option

21. Option B has been retained.

POLICY ISSUE 4: INFORMATION ON SUBCONTRACTING ARRANGEMENTS

22. Option A: Include a requirement for a critical ICT third-party service provider to provide information on their subcontracting arrangements by using the same templates of the register of information to be maintained and updated by financial entities as referred to in Article 28(3) of Regulation 2022/2554.

23. Option B: Have a specific template to be used by a critical ICT third-party service for providing information on subcontracting arrangements.

Cost-benefit analysis

24. Subcontracting is one of the areas where the Lead Overseer is expected to assess the ICT third-party service provider designated as critical. It is therefore expected a material exchange of information between the involved stakeholders on this subject which should be facilitated by the development of a specific template. Taking into account the fact that structures of ICT third-party service providers differ significantly from the structures of financial entities, the template to be used by critical ICT third-party service providers to submit relevant information should not mirror or be based on the templates of the register of information referred to in Article 28(3) of the DORA. Instead, a new, flexible template is needed which takes into account the specificities of ICT third-party service provider structures.

Preferred option

25. Option B has been retained.

Policy options relating to Chapter III – Assessment of the measures taken by critical ICT third-party service providers based on recommendations of the Lead Overseer

POLICY ISSUE 5: CHANNELS DEDICATED TO THE TRANSMISSION OF INFORMATION FROM THE CTPPS TO THE LEAD OVERSEER

26. Option A: Provide the full detail in the RTS of the communication channel to be used by the critical ICT third-party service providers to share information with the Lead Overseer.
27. Option B: Indicate in the RTS that the Lead Overseer shall specify in its information request the communication channel to be used by the ICT third-party service providers to share information with the Lead Overseer.

Cost-benefit analysis

28. Secure information sharing between the CTPPs and the LO is key to ensure the proper functioning of the oversight framework. In order to achieve its oversight objectives, the Lead Overseer can ask the critical ICT third-party service providers to submit a diverse range of information either through simple request or request by decision. The Lead Overseer has the responsibility to ensure that the security measures applied to the information shared from the CTPP is commensurate to the type of information shared and its risk. In order to achieve it, the ESAs will establish a dedicated online tool where information shared by the critical ICT-third party service providers can be confidentially, securely shared and stored. Furthermore, on a case by case basis, for example in case of ad-hoc requests, the Lead Overseer may decide to access information provided by the critical ICT third-party service providers directly on the systems of the ICT third-party service providers. For these reasons, it has been decided to retain flexibility in the draft RTS.

Preferred option

29. Option B has been retained.

POLICY ISSUE 6: ASSESSMENT PERFORMED BY COMPETENT AUTHORITIES

30. Option A: The regular assessment of the risks addressed in the recommendations of the Lead Overseer is an ad hoc task of the competent authorities, which should be performed for each recommendation issued by Lead Overseer to a critical ICT third-party service provider. The results of this assessment should be shared with the Lead Overseer on a continuous basis.
31. Option B: The regular assessment of the risks addressed in the recommendations of the Lead Overseer is a task which is part of the supervisory tasks of the competent authorities and it is their decision when to carry it out applying a risk based and proportionate approach. The results of this assessment should be shared with the Lead Overseer upon its request.

Cost-benefit analysis

32. Once recommendations to a critical ICT third-party service provider are issued by the Lead Overseer and competent authorities have informed the relevant financial entities of the risks identified in

that recommendations, the Lead Overseer should be in charge to monitor and assess the implementation by the critical ICT third-party service provider of the actions and remedies to comply to that recommendations and the competent authorities to monitor and assess the extent to which the financial entities are exposed to the risks identified in these recommendations.

33. With a view at maintaining a level playing field, while carrying out their respective tasks, particularly when the risks identified in the recommendations are severe and shared among a large number of financial entities in multiple Member States, it is considered important that both the competent authorities and the Lead Overseer share among each other relevant findings of their tasks. This information sharing should be carried out with the objective to ensure that the feedback of the Lead Overseer to the critical ICT third-party provider in relation to the actions and remedies the latter is implementing takes into account the impacts on the risks of the financial entities, and that the supervisory activities performed by the competent authorities are informed by the assessment carried out by the Lead Overseer.

34. In order to allow for the cooperation described in the previous paragraph to be efficient and effective, it is vital that competent authorities assess, as part of their supervisory activities, the extent to which the financial entities supervised by them are exposed to the risks identified in the recommendations. This assessment should be carried out by the competent authority in a proportionate and risk-based manner.

Preferred option

35. Option B has been retained.

Costs and benefits of the RTS

Stakeholder groups affected	Costs	Benefits
Financial entities	Additional compliance efforts for financial entities as they might need to invest in new systems and processes to ensure compliance with the regulatory requirements set out in the regulatory technical standards. Increased administrative burden as financial entities must review the information provided about critical ICT third-party service providers and cooperate with competent authorities.	Enhanced security and risk management as financial entities benefit from a structured framework for assessing and monitoring the ICT services they rely on. This helps ensure the security and resilience of their operations. Deeper market insights as financial entities receive information about critical ICT third-party service providers allowing financial entities to assess the actions/remedies taken by critical ICT third-party service providers to address identified risks.
ICT TPP	Gathering and submitting extensive information to competent authorities can be resource-intensive and may require additional internal processes. Being designated as critical subjects ICT third-party service providers to more	While being designated as critical may enhance the status and credibility of ICT third-party service providers, the provisions set out in the regulatory technical standards may support ICT third-party service providers

Stakeholder groups affected	Costs	Benefits
	rigorous oversight, which can be costly in terms of compliance and addressing the recommendations issues by the Lead Overseers.	designated as critical in gaining a better understanding of the market, their market share, and the competition through the information they provide. Through the opportunity to engage with competent authorities, ICT third-party service providers designated as critical can benefit from improved risk management practices.
Competent authorities	Processing and evaluating the information provided can be labour-intensive and costly and may require additional internal processes and systems. New information provided by the market may oblige competent authorities to invest in relevant staff training and additional resources with a different skill set than existing staff.	Competent authorities gain access to comprehensive information about critical ICT third-party service providers and the services those are providing to financial entities, ultimately helping competent authorities assess and monitor risks. The detailed reporting can allow competent authorities to identify potential issues early and take corrective action. Supervisory efforts can be prioritised based on the risk assessment of critical ICT third-party service providers.
European Supervisory Authorities	The ESAs must review and manage the information provided by ICT third-party service providers and extensively coordinate with competent authorities and ICT third-party service providers. This has resource implications. The ESAs bear the responsibility of ensuring consistency and effectiveness in the application of the provisions set out in the regulatory technical standards across EU Member States.	ESAs to receive valuable new data, which enhances existing oversight and ultimately helps increasing the stability of the EU financial sector.

Annex to the impact assessment - high-level mapping between Article 33(3) DORA and Article 3(2) RTS

Article 33(3) DORA	**Article 3(2) RTS**
(a) ICT requirements to ensure, in particular, the security, availability, continuity, scalability and quality of services which the critical ICT third-	(a) information about the arrangements between the CTPP, the FEs and its subcontractors.

Article 33(3) DORA	Article 3(2) RTS
party service provider provides to financial entities, as well as the ability to maintain at all times high standards of availability, authenticity, integrity or confidentiality of data	(g) information about the ICT security and data protection frameworks (k) information about measures taken to address risks arising from the provision of ICT services (n) information about performance monitoring, security monitoring, and incident tracking as well as information about reporting mechanisms related to service performance, incidents, and compliance with agreed-upon service level agreements (SLAs) or similar arrangements (o) information about the ICT third-party management framework of the CTPP, including strategies, policies, procedures, processes, and controls including details on the due diligence and risk assessment performed by the CTPP on its subcontractors (q) extractions from any production, pre-production and test system or application used by the critical ICT third-party service provider and its subcontractors to provide directly or indirectly services to financial entities in the Union (t) information about the remediation plan to address recommendations according to Article 4 of this Regulation, and relevant related information to confirm remedies have been implemented
(b) the physical security contributing to ensuring the ICT security, including the security of premises, facilities, data centres	(g) information about the ICT security and data protection frameworks (i) information about the exact location of the data centres and ICT production centres (o) information about the ICT third-party management framework of the CTPP, including strategies, policies, procedures, processes, and controls including details on the due diligence and risk assessment performed by the CTPP on its subcontractors
(c) the risk management processes, including ICT risk management policies, ICT business continuity policy and ICT response and recovery plans	(k) information about measures taken to address risks arising from the provision of ICT services (l) information about the risk management framework and the incident management framework (m) information about the overall response and recovery framework of the critical ICT third-party service provider (n) information about performance monitoring, security monitoring, and incident tracking as well as information about reporting mechanisms related to service performance, incidents, and compliance with agreed-upon service level agreements (SLAs) or similar arrangements (o) information about the ICT third-party management framework of the CTPP, including strategies, policies, procedures, processes, and controls including details on the due diligence and risk

Article 33(3) DORA	Article 3(2) RTS
	assessment performed by the CTPP on its subcontractors (v) information about the activities of the critical ICT third-party service provider and financial statements, including information on the budget and resources related to ICT and security
(d) the governance arrangements, including an organisational structure with clear, transparent and consistent lines of responsibility and accountability rules enabling effective ICT risk management	(a) information about the arrangements between the CTPP, the FEs and its subcontractors (b) information about the organisational and group structure of the CTTP (c) information about the major shareholders of the CPP (d) information about the CTPP market share in the relevant markets where it operates in terms of types of services where it operates (e) information about the internal governance arrangements of the CTPP, including the structure with lines of governance responsibility and accountability rules; (f) the meeting minutes of the CTPP management body and any other internal relevant committees (j) information about provision of services by CTPP from third-countries (o) information about the ICT third-party management framework of the CTPP, including strategies, policies, procedures, processes, and controls including details on the due diligence and risk assessment performed by the CTPP on its subcontractors (s) information about any assessments carried out by the ICT third-party service provider upon its request or on its behalf evaluating the suitability and integrity of individuals holding key positions within the critical ICT third-party service provider; (u) information about employee training schemes and security awareness programs (v) information about the activities of the critical ICT third-party service provider and financial statements, including information on the budget and resources related to ICT and security
(e) the identification, monitoring and prompt reporting of material ICT-related incidents to financial entities, the management and resolution of those incidents, in particular cyber-attacks;	(l) information about the risk management framework and the incident management framework (n) information about performance monitoring, security monitoring, and incident tracking as well as information about reporting mechanisms related to service performance, incidents, and compliance with agreed-upon service level agreements (SLAs) or similar arrangements
(f) the mechanisms for data portability, application portability and interoperability, which ensure an effective exercise of termination rights by the financial entities	h) information about the mechanisms the CTPP offers to customers for data portability, application portability and interoperability

Article 33(3) DORA	Article 3(2) RTS
(g) the testing of ICT systems, infrastructure and controls	m)information about the overall response and recovery framework of the critical ICT third-party service provider, including business continuity plans and related arrangements and procedures, response and recovery plans and related arrangements and procedures, backup policies arrangements and procedures; (n) information about performance monitoring, security monitoring, and incident tracking as well as information about reporting mechanisms related to service performance, incidents, and compliance with agreed-upon service level agreements (SLAs) or similar arrangements (p) extractions from the monitoring and scanning systems of the critical ICT third-party service provider and of its subcontractors, covering but not limited to network monitoring, server monitoring, application monitoring, security monitoring, vulnerability scanning, log management, performance monitoring, and incident management
m) the ICT audits	(k) information about measures taken to address risks arising from the provision of ICT services (p) extractions from the monitoring and scanning systems of the critical ICT third-party service provider and of its subcontractors, covering but not limited to network monitoring, server monitoring, application monitoring, security monitoring, vulnerability scanning, log management, performance monitoring, and incident management (r) compliance and audit reports (s) information about any assessments carried out by the ICT third-party service provider upon its request or on its behalf evaluating the suitability and integrity of individuals holding key positions within the critical ICT third-party service provider;
n) the use of relevant national and international standards applicable to the provision of its ICT services to the financial entities	(g) information about the ICT security and data protection frameworks (n) information about performance monitoring, security monitoring, and incident tracking as well as information about reporting mechanisms related to service performance, incidents, and compliance with agreed-upon service level agreements (SLAs) or similar arrangements

5. Feedback from the Public Consultation

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
Content of information to be provided by ICT third party providers in the application for a voluntary request to be designated as critical	One stakeholder requested clarification whether the voluntary requests to be designed as critical, will be accepted starting 17/01/25, and related to this, when the CTPP list will be published by the ESAs, since the list is a pre-requisite for the voluntary request based on Article 1(h).	The mandate is not about the starting date of the opt-in process, but about the requested information. However, it is acknowledged that the information requested as per Article 1(1)(h) can only be provided when the list of CTPPs is available.	"where available" added to Article 1(1)(h).
	One Stakeholder suggested to complement the list of information by several items, which are: a) the existence and date of the most recent review of internal policies, e.g.: Code of Conduct, Software Development Lifecycle Policy, Disaster Recovery & Business Continuity Plan, b) inclusion of detailed information about the capabilities of third-party providers in the field of monitoring, reporting, etc. c) the company's reliability monitoring efforts, e.g. like the active measurement of Service Level Objectives (and/or Service Level Agreements) in daily operations. Effective SLO/SLA monitoring is essential for maintaining high levels of service performance and availability, which are critical components of digital operational resilience. Objectives should include assessments of the capability to restore service with specific time and quality goals	The ESAs decided to discard these additional elements to be requested as they are not necessary for the assessment of their criticality to the financial sector (in comparison with the criticality criteria of DORA article 31(2)). These are all elements that can be analysed once an ICT TPP is designated as critical and subject to the oversight of a Lead Overseer.	No change

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
	based on measurement of recovery systems and tests. d) the entity's compliance with any certifications, independent audits, assessments, compliance with frameworks, date and frequency of the audits (e.g. ISO27001, SOC 2 Type 1/2/3)		
	Some stakeholders were unsure about the willingness of the potential CTPP to provide the required information, particularly Article 1(1)(i) and (1)(j). Instead, providers should only provide information on strategy and investment plans to the extent it is relevant to the assessment of whether they are "critical". 3 stakeholders noted that not all information in the Article would be well-suited for the criticality assessment. They recommended that Article 1(1)(k) of the RTS is deleted, and that at the end of Article 1(1)(j), the following text is inserted:", insofar as these plans are relevant to the factors set out in Article 31(2) of Regulation (EU) 2022/2554";"	A self-assessment by the ICT Third-party service provider regarding their criticality will feed the ESAs assessment providing information the ESAs may not find in information reported by the financial entities through their registers of information. The elements requested under (1)1(i) will be used as additional information supporting the self-assessment of said ICT provider as being critical for the European Financial sector. No amendment has been introduced since the scope of DORA is the European financial sector and the objective of the application is the criticality assessment. Regarding Article 1(1)(k), a similar approach is followed for the designation of the critical third party ICT service providers based on the Delegated Act specifying the criteria for the designation of ICT third-party service providers as critical for financial entities (see Article 2(5)(b))	No change regarding article 1(1)(i) and (k)

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
	Some stakeholders shared their worry that the extensive amount of information requested requires many additional resources and may therefore lead to adverse effects on financial entities. They suggest aligning the content of the information provided by the ICT third-party provider with the financial entities' register of information, in order to avoid the need for financial entities to request additional information. The ESAs are suggested to share the information received from the CTPPs with financial entities. Consequently, financial entities would only need to collect information related to "regular" ICT third-party providers and not the CTPPs	The register of information under Article 1(1) will address other information needs (eg. ICT risk management of the financial entities and supervisory needs of the competent authorities), so it is not possible to fully align the register and the information requested from the applicant TPPs. In addition, the information requested in article 1(1) will complement the register of information to give the opportunity to the applicant ICT TPPs to justify their criticality with information not already available in the register. The requested information in Article 1(1) will have to be provided by applicant ICT TPPs and not by CTPPs.	No change
LEI	2 stakeholders underlined that not all third-country ICT providers may possess or provide trading venues with an LEI, requiring a strong consideration of additional criteria, such as Tax ID for instance.	For alignment purposes it is proposed to make a cross reference to the "identification code" as defined in the upcoming Commission Implementing Regulation adopted in accordance with Article 28(9) of Regulation (EU) 2022/2554.	A specific recital has been included accordingly.
	These 2 stakeholders pointed out the scope of information needed for a voluntary request to be designated as critical appears too broad and may discourage ICT third-party service providers from applying to preserve their business secrets. The proposed solution would be to divide the application process into two steps - the first step would require a	The ESAs took into account the request to specify whether all services or only services in relation to financial entities are required in point f. The items of information requested to be designated as critical are based on the elements listed in DORA L1.	No change An amendment to article 1(1)(e) was made clarifying the" Union" financial sector is targeted An amendment to article 1.(1)(f)

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
	narrower scope of information and only the second step would require the full scope. Additionally, some specific items in the list were deemed problematic, such as item (e) (suggestion to clarify how license-based models should be treated in more detail), (f) (suggestion to specify whether all services or only services in relation to financial entities are required) and (j) (providers would be unwilling to share this information, which might also not even be relevant).	The ESAs would like to remind that the possibility to voluntarily apply to be designated as critical is not meant to be seen as a certifying process or as a way to obtain a supervisory seal of approvement. The ESAs consider the proposal to add more items or make this a 2 step process would complexify the process.	was added clarifying that this concerns services provided to" Union financial entities"
Assessment of the completeness of opt-in application	Three stakeholders highlighted the provision of Article 2(3) explaining the ICT TPPs which would not provide all the necessary information on time would see their application discarded and this may lead to inequalities and errors in interception of critical providers. Two of them suggested to extend the time to provide this information (or allowing the applying provider to ask more time), the third suggested to simply warn the providers without discarding their application. One of them also raised an erroneous cross reference in this article (reference to a paragraph 5 which does not exist).	- Regarding the comments on article 2(3), the ESAs are of the view the information to apply are clearly listed in article 1, so the applying ICT TPPs have time to prepare for the application, hence the proposed process to manage incomplete application is adapted. The process will be the same for all ICT TPPs applying and nothing prevents them for applying once again if their application was rejected because it was considered incomplete. The erroneous cross-reference has been rectified. - Following the designation of a ICT third party provider as critical through this specific process, the list of critical ICT third party providers published by the ESAs will be updated on their website	-Article 2 was amended as follows: paragraph 3 was deleted. - The new paragraph 2(2) states "*Where the relevant ESA considers that information provided in the application is incomplete, it shall reject the application and request the missing information.* "

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
		and after each designation.	
	One stakeholder requested clarification on if submitting a complete application would be enough for an ICT TPP to be designated as CTPP	The ESAs clarify that submitting a complete application only allows the application to be assessed by the ESAs but does not guarantee designation per se (DORA article 31(11) second subparagraph states that the ESAs "*shall decide whether to designate that ICT third-party service provider as critical*").	No change
	One stakeholder requested to clarify what the ESAs mean by "*market share*" in Article 1(1)(e) assuming that the ICT TPP cannot calculate this without having an overview of the clients in the financial sector and what the ESAs mean by "*market share*" and "*known relevant competitors*" in Article 1(1)(i)(i)	Regarding the reference to "*market shares*", the ESAs acknowledge the ICT TPPs may not have an overview of the market, so may not be in position to estimate such shares with accuracy, but such type of information is inherent to the criticality of the CTPPs and the applicants should try to estimate it to the extent possible to justify their application. Regarding the "known relevant competitors", the ESAs assume the ICT TPPs are able to identify their main competitors on their markets, though such estimate may not take into account all and every ICT TPPs providing the same ICT services.	No change

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
The list of information to be provided by critical ICT third-party service providers to the Lead Overseer based on Article 3	On the content to be provided by ICT third-party providers, is concerned by the high level of administrative burden this will generate, especially for SMEs. Content of the information to be provided by ICT TPP should be aligned with the FE's register of information.	The ESAs would like to remind that the information requested and listed in article 3 are provided by ICT TPPs which have been designated as critical in the context of the Oversight Framework - The information requested by the Lead Overseer may be any information that is deemed necessary by the Lead Overseer to efficiently carry out its oversight duties. Not all of the information has the same scope or can be aligned with the FE's register of information since this is requested from the CTPPs	Article 3(1) was amended as follows: "*Critical ICT third-party service providers shall provide to the Lead Overseer, upon its request, any information deemed necessary by the Lead Overseer to carry out its oversight duties in accordance with the requirements of Regulation (EU) 2022/2554. Critical ICT third-party service providers shall transmit this information according to the structure and format described in Article 5 of this Regulation, within the time limits and with the frequency set by the Lead Overseer*". -Article 3(2)(w) was deleted .
	One stakeholder suggested to complement Article 3(2)(c) , to be consistent with the terms of Commission Recommendation 2003/361/EC, identifying shareholders	This proposal was deemed valuable for the ESAs who introduced the proposed elements	Article 3(2)(c) was amended so as to better capture information about major stakeholders and geographical spreads and entities *"(i) hold, solely or jointly with their linked entities 25% or more of the capital or voting rights of the critical*

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
			ICT third-party service provider; *(ii) hold the right to appoint or remove a majority of the members of the administrative, management, or supervisory body of the critical ICT third-party service provider; or* *(iii) control, pursuant to an agreement, a majority of shareholders' or members' voting rights in the critical ICT third-party service provider*"
	Several stakeholders suggested CTPPs might not be in possession of information requested under Article 3(2)(d)	While the ESAs acknowledge that the CTPP may not hold , what is requested in this case is their own estimation	Amendment was inserted in Article 3(2)(d) specifying *"service provider's own estimation* of its market share,.."
	The requested information includes sensitive details about the ICT third-party service provider's operations, security frameworks, financial entities and employee training and security awareness programmes.	The ESAs believe these are all information the LO is entitled to request according to article 33(3) of Regulation (EU) 2022/2554	No change
	One stakeholder suggested that reference in Article 3(2)(f) to management body meeting minutes is overbroad. Nothing in DORA warrants unlimited access to all of service provider's board meetings minutes and internal	The ESAs believe that although this information pertains to very confidential topics, depending on the subjects discussed by the MB the information provided	Amendment proposed stating that the MB meeting minutes that are requested here are the ones

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
	committee meetings, which may discuss a wide range of sensitive commercial information	under Article 3(2)(f) could lead to General Investigations or deep dives. The scope of this information is specified in the Article.	"*which relate in any way to activities concerning ICT third-party services supporting functions of financial entities within the Union*"
	Several stakeholders highlighted the fact that ensuring the secure handling and transmission of this sensitive data presents a significant challenge, requiring robust data protection measures.	The ESAs recognise the sensitive nature of some of the Data that the CTPPs are requested the provide to the LO. To this end, the ESAs intend to put in place an information transmission tool that has all the necessary security controls in place to ensure data privacy, confidentiality and data storage. The necessary security requirements of the tool will be evaluated during the development phase of the tool and will be commensurate to the sensitivity of the data.	An amendment in Article 5(1) was introduced based on this proposal: "The critical ICT third-party service provider shall provide the requested information to the Lead Overseer through the dedicated secure electronic channels indicated by the Lead Overseer in its request. "
	Several stakeholders suggested that in the interest of proportionality, the authority of the lead overseer (LO) under article 3 to request information about the CTPP's subcontracting arrangements should be limited to arrangements that effectively underpin ICT services supporting critical or important functions or a material part thereof.	The Lead Overseers will determine in the course of the oversight activities what are the relevant information they need in relation to the subcontracting arrangements of the CTPPs to achieve their oversight objectives, taking into account the information shared by the CTPPs based on Article 6 and the Annex of this draft RTS.	Based on this proposal a new recital (4) was introduced stating: "The request to critical ICT third-party service providers to transmit to the Lead Overseer information that is necessary to carry out its duties, including the one on subcontracting arrangements, should be done considering the

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
			second subparagraph of Article 33(2) of Regulation (EU) 2022/2554.
	Several stakeholders highlighted that Articles 3(2)(p) and (q) cover "extractions" from service provider and subcontractor system scans and monitoring and any production, pre-production, and test system or application used to provide services to financial entities. "Extractions" is unclear. It could include any data relating to such functions and technology. There is no general legitimate basis under DORA for acquiring such a broad set of data, much of which is highly sensitive, and the draft RTS offers none.	The term extractions depicts the most accurately what the LO may request in the exercise of his oversight powers in accordance with Article 33(3) of DORA.	No change
	Some stakeholders raised the fact that Article 3(2)(i) requires CTPP to submit info upon request about exact location of its data centres. Disclosing this would create physical security risks to said facilities. Request removing this requirement or amend it so that only general location of relevant facilities is required. It was proposed Article 3(2)(i) should be amended as it presently includes data centres that are out of scope of the DORA Regulation	Article 33(3)(b) of DORA request the LO to oversee various assets of the CTPPs, including data centres, hence their exact location is a relevant information to achieve their oversight objectives. The ESAs consider that this information is needed in order to determine the geographical spread of the CTPP as well as where the data of the EU financial entities making use of said provider is backed up. In no way the LOs plan to "disclose" such information, neither any other information provided by the CTPPs.	- No change

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
	One stakeholder pointed Article 3 lists info that CTPP must submit to its LO including sensitive & confidential information, such as: "ICT security and data protection frameworks" (Art3(2)(g));risk management and incident response (Art3(2)(l)) & info from production & monitoring systems of service provider (Art3(2)(p) and (q)). If this info were managed insecurely, may affect security of CTPP systems & financial system. It was suggested,CTPPs should provide the Lead Overseer with sufficient information to enable oversight activities, but: (i) not result in the creation of new vulnerabilities that may be exploited through the leakage of sensitive data; or (ii) exceed the scope of Regulation (EU) 2022/2554's focus on financial entities and their use of ICT services. Highly sensitive security information CTPPs disclose is most secure when it remains with the CTPP.	the LOs do not plan to "disclose" any information provided by the CTPPs.	No change
	Some stakeholders suggested the scope of the information requested may be overbroad. Lack of scope limitation to ICT services supporting critical or important functions is a recurring flaw. Article 3(2) demands production of various information on a service providers' service and technology in general, regardless of whether they support critical or important functions. See, e.g., Art 3(2)(a)-(o), (p)-(s), (v). At the very least, these provisions should be scoped to relevant services	The ESAs do not consider the scope of the information requested to be overbroad as they aim at allowing the LOs to achieve the assessment requested in Article 33(3). In addition, Article 33(2) mandates the LO to assess all relevant risks, extending the assessment to functions other than those that are critical or important if necessary.	However, amendments were introduced in Articles 3(2)(h) and (i) specifying that the information requested concerns CTPPs offer to "Union *financial entities for data portability,…"* and "*information about the exact location of the data centres and ICT production centres used and being used to provide services to financial entities*" And in Article 3(2) the sentence "*and*

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
			outside the Union where cooperation agreements with the relevant authorities provide for such information exchange" was added
r	One stakeholder suggested it would be beneficial to include reliability monitoring: a) inclusion of detailed information about the capabilities of third-party providers in the field of monitoring, reporting, etc. is crucial because it directly impacts the reliability and performance of the services provided to financial entities. b) information about company's reliability monitoring efforts, e.g. like the active measurement of Service Level Objectives (and/or Service Level Agreements) in daily operations. Effective SLO/SLA monitoring is essential for maintaining high levels of service performance and availability, which are critical components of digital operational resilience. Article 3, point 2p – it was recommended that this specifically mentions measurement against reliability goals (e.g. Service Level Objectives)	The ESAs agree on the importance of having access to appropriate evidence of reliable monitoring from the CTPPs.	Amendments were inserted in Articles 3(2)(m), (n) and (p) based on this proposal.
Remediation plan and progress reports	Some stakeholders requested clarification with regards to the frequency of the remediation plans A limited set of stakeholders expressed the view that Article 35(1)(c) does not always require	As remediation plans are part of the recommendations issued after the completion of oversight activities, there is no pre-determined frequency. Article 4(1) of the draft RTS on the harmonisation of	The title of Article 4 was amended to "Information from critical ICT third-party providers after the issuance of recommendations"

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
	remediation and that a CTPP is not compelled to remediate and proposed to revise Paragraph 1. 2 stakeholders commented on the timeline of the execution of the remediation plan. One had the wrong reading that the FE are to implement such plan. A limited number of stakeholder suggested to discard point 2(i) where CTPP are requested to share interim reports and related supporting documents. It was of view that these exchanges should be managed through the ongoing oversight relationship between the LO and CTPP and there is no need to specify as step. 1 stakeholder suggested that remediation plans should be managed by independent party to ensure objectiveness of the process.	conditions enabling the conduct of the oversight activities under Article 41(1), (a), (b) and (d) of DORA foresee that, as part of the notification of its intention to comply with the recommendations, the CTPP provides the LO with a remediation plan. The remediation plan is requested from the CTPP in accordance with Article 37 and 35 1(c) of DORA which allows the LO to require the CTPP to provide all information necessary for the LO to carry out its duties under DORA. The ESAs note that the remediation plan is an integral part of the recommendation. The LO's recommendations will always come with the need for the CTPP to provide a remediation plan or reasoned explanation for not following the recommendations. Therefore, when a recommendation is issued, it will include a request for a remediation plan illustrating how the findings will be addressed and the respective timeline. LO - as part of its oversight activities - may establish an on-going dialogue with the CTPP, interim reports will facilitate the monitoring of the actions taken to address the recommendation, therefore a necessary step. The DORA L1 sets the ESAs as the responsible of the oversight of the CTPPS and thus the review of the remedial plans lay with the LO and cannot be delegated to a third party.	furthermore paragraph 2(b) of the same article has been amended to specify that the actions and the remedies included in the final reports shared by the CTPP with the lead overseer are aimed at mitigating the risks identified in the recommendations.

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
Structure and format of information provided by the critical ICT third-party service provider	Some stakeholders, while flagging that the draft RTS should state that the lead overseer assumes full responsibility for losses occurring from intrusion or leaks of data occurring through the use of the secure channel it provides, proposed amendments regarding the secure channel of communication to be provided by the Lead overseer for the CTTPs to submit mandatory information: Given the highly sensitive nature of said information, RTS should state that relevant secure channel should meet minimum technical standards for safety and confidentiality and be jointly agreed upon by the lead overseer and the CTTP. Several stakeholders disagreed with the proposal to require all information to be submitted to the lead overseer in English as the burden of providing all information in English is disproportionate for smaller European FEs with European ICT providers, for which the original documents are not created in English; in addition, stakeholders flagged that translating those contracts would result in an extremely resource-intensive if it is to be notarized and legally binding.	The ESAs recognise the sensitive nature of some of the Data that the CTPPs are requested the provide to the LO. To this end, the ESAs intend to put in place an information transmission tool that has all the necessary security controls in place to ensure data privacy, confidentiality and data storage. The necessary security requirements of the tool will be evaluated during the development phase of the tool which will be commensurate to the sensitivity of the data. The RTS on Oversight is not the document which should state the relevant secure standards applied to the information transmission tool as this is not in the mandate specified in L1. The English language requirement is set out in Level 1 text.	Paragraph 1 of Article 5 has been amended as follows: "*The critical ICT third-party service provider shall provide the requested information to the Lead Overseer through the dedicated secure electronic channels indicated by the Lead Overseer in its request*" Paragraph 2 of Article 5 was modified to clarify that , when providing information to the Lead Overseer, the critical ICT third-party providers shall: "*clearly locate the relevant piece of information in the submitted documentation*" Finally, the impact assessment has been updated with a new policy option to describe the choice related to the channels dedicated to the transmission of information from the CTPPs to the Lead Overseer
Information to be provided by the critical ICT third-party service provider to the Lead Overseer	Stakeholders flagged that maintaining a database containing each subcontractor's qualifications might not be feasible and that building the framework to	Regarding the suggestion to rely on a central team/function to coordinate contacts, the key staff information is helpful to have an ownership and responsibility guarantee, but	In the context of Annex I complementing the provisions laid out in Article 6, the information category

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
regarding subcontracting	monitoring performance metrics will need time. - A limited number of stakeholders proposed to allow all contacts to be coordinated through a central team/function, instead of identifying a specific staff member, to reduce key person risk. - Some respondents proposed to amend the 3rd bullet point of section *Subcontracting Governance and Oversight* in Annex I as: "*Overview of performance metrics, service level objectives and agreements, and key performance indicators used to assess subcontractor performance and reliability monitoring*". A limited number of stakeholders proposed to amend Article 6 to include a focus on arrangements which effectively underpin ICT services supporting critical or important functions or a material part thereof. - Some stakeholders proposed to remove the mapping of sub-contractors and the specification and description of types of ICT services subcontracted and their significance to the ICT services provided to financial entities from the Annex and proposed to substitute this information with a short description of the purpose/scope of the sub-contracting arrangement. - 1 stakeholder has several re-drafting proposals on Article 3, which should also apply to the Annex of Article 6: o Art 3(2)(a)-(o), (p)-(s), (v) should be at least	this does not exclude the use of shared communication services (e.g. functional mailboxes) when contacting the key staff or the respective team. Since the financial entities define the critical and important functions in the DORA context, it will be difficult for the potential CTPP to filter the data points for services that effectively underpin ICT services supporting critical or important functions […], and this classification might also evolve regularly so it is important to be cautious with such limitations.	on subcontracting governance and oversight was amended including information on Service Level Objectives (SLOs) as follows: "[…]*Overview of performance metrics, service level objectives and agreements, and key performance indicators used to assess subcontractor performance and reliability monitoring.*

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
	scoped to relevant services for FEs or critical or important functions. o Art 3(2)(d-e) seem out of scope of DORA. Some stakeholders flagged the need to align the wording of Article 3(2)(l) with the NIS 2 vocabulary to ensure clarity and consistency.		
Competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer	Some stakeholders suggested to further clarify the roles of the CA and the LO. Some stakeholders flagged that requiring FEs to assess the impact of the measures of the remediation plan and the check regarding adherence to timelines go more into the direction of a task to be assigned to CAs. On the other hand, stakeholders also flagged that FEs are best placed to determine how to address the identified CTPP risks within their own risk management assessment. Several stakeholders suggested to clarify how FEs should report to CAs on the measures implemented to mitigate risks identified by the LO (pursuant to Article 42(3)). In addition, stakeholders complemented the feedback highlighting that this reporting task would have administrative costs and this should be taken into account in the impact assessment accompanying the draft RTS. Several stakeholders suggested to clarify how FEs should report to CAs on the measures implemented to mitigate risks identified by the LO (pursuant to Article 42(3)). In addition, stakeholders complemented the feedback highlighting that this reporting task would have administrative costs and that this	The role of CAs and LO are defined in L1, the CAs will use the information provided by the LOs for the supervision of the financial entities, and will assess the measures taken by the CTPPs through the supervision of the financial entities relying on these CTPPs, while the Lead Overseers will directly assess the measures taken by the CTPPs. Article 7(2)(b) already states that CA will have to take in consideration the assessment made by the LO (of the compliance with the measures and actions included in the remediation plan by the CTPP, where it has impact on the exposures of the FEs under their remit). -Under Article 42(3) of DORA competent authorities shall inform the relevant financial entities of the risks identified in the recommendations addressed to critical ICT third-party service providers by the LO in accordance with Article 35(1), point (d). In this regard, FEs will be able to report to CAs on the adequacy and the coherence of the remediation measures implemented to mitigate those risks during ongoing supervisory activities. Any additional suggestions or	Article 7(1) has been amended as follows "As part of their supervision of financial entities, competent authorities shall assess the impact on the financial entities […]" Article 7(3) has been amended as follows: "Upon request from the Lead Overseer, the competent authority shall provide in reasonable time the results of the assessment set out in paragraph When requesting the results of this assessment, the Lead Overseer shall consider the principle of proportionality and the magnitude of risks associated with the recommendatio

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
	aspect should be taken into account in the impact assessment accompanying the draft RTS. -Some stakeholders proposed, in order to avoid further EU-fragmentation and potential market disruption, that LO and OF should be able prevented from taking unilateral decision that could disrupt operation of FE beyond a MS.	proposals by FE will be discussed accordingly. The ESAs note that Article 42(6) establishes that CAs "may require financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the CTPP". While the LO is not empowered to prohibit such a decision, it is noted that Article 42(10) requires that CAs "shall regularly inform the LO 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 CTPPs have not endorsed in part or entirely recommendations". In addition, the joint guidelines on the oversight cooperation and information exchange between the ESAs and the competent authorities under Regulation (EU) 2022/2554 GL 12.2) require that the LO should assess the potential impact such decision might have for the CTPP whose service would be temporarily suspended or terminated and should share this assessment with the competent authorities concerned. The same GL12 also indicates that where two or more CAs plan to take or have taken decisions regarding financial entities making use of ICT services provided by the same CTPP, the LO should inform them about any inconsistent or divergent supervisory approaches that could lead to an unlevel playing field.	n, including the cross-border impacts of these risks when impacting financial entities operating in more than one Member State."

Topic	Summary of responses received	ESAs' analysis	Amendments to the proposal
Impact assessment and the main conclusions stemming from it	One stakeholder welcomed the inherent flexibility of the provisions, especially the fact the information requested to the CTPPs can be expanded as needed to accommodate oversight needs. On the contrary, another stakeholder suggested to define a common request delivered on a regular basis allowing the CTPPs to anticipate. Six stakeholders stressed the implementation of the RTS would impose additional burden and compliance costs on financial entities and would want more transparency about this in the impact assessment (especially regarding the remediation measures). One of them also reminded that financial entities with international activities may have to comply with similar obligations in other jurisdictions. One stakeholder would have expected further guidance on the information that can be requested (without specifying to who) and advocated for proportionality in this respect. One stakeholder stated that the timeline for the implementation of the new requirements is too short.	Regarding the comment on the potential burden on financial entities in case of potential remediation measures, the ESAs are not in a position to elaborate on this given this will be the consequence of potential supervisory decisions taken by Competent Authorities to follow-up on oversight activities. Hence, this will also depend on the inherent proportionality of the supervisory activities. In addition, it is reminded that the Competent Authorities are mandated to follow-up on the Lead Overseers' recommendations based on Article 42 of DORA (this is not a proposal introduced by the ESAs in this draft RTS), so they have to take them into account when supervising the financial entities using the CTPPs. Regarding the comment on the information to be requested to the CTPPs, the ESAs do not exclude the possibility to identify information that may be collected from the CTPPs on a regular basis, but such potential regular reporting cannot be considered as sufficient to cover any type of oversight needs. Regarding the comment on the timeline to comply with the new requirements, the ESAs are not in a position to discuss this, the deadline to deliver their Final Report is determined in Article 41(2) of DORA.	No change