JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2023 69

27 November 2023

Consultation Paper

Draft regulatory technical standard on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) points (a), (b) and (d) of Regulation (EU) 2022/2554

Contents

1. Responding to this consultation

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

Comments are most helpful if they:

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

Submission of responses

The ESAs will consider all comments received by 04 March 2024**.**

Comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Your responses will be published on the ESAs' website unless: you request to treat them confidential, or they are unlawful, or they would infringe the rights of any third-party. Please, indicate clearly and prominently in your submission any part you do not wish to be publicly disclosed. ESAs may also publish a summary of the survey input received on their website.

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

Declaration by the contributor

By sending your contribution to EIOPA you consent to publication of all non-confidential information in your contribution, in whole/in part – as indicated in your responses, including to the publication of the name of your organisation, and you thereby declare that nothing within your response is unlawful or would infringe the rights of any third party in a manner that would prevent the publication.

Data protection

Please note that personal contact details (such as name of individuals, email addresses and phone numbers) will not be published.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

2. Executive Summary

Introduction and scope

Regulation (EU) 2022/2554[1] ("DORA") introduces a pan-European oversight framework of ICT third-party service providers designated as critical (CTPPs). As part of this oversight framework, the ESAs and competent authorities (CAs) have received new roles and responsibilities.

In this context, the ESAs have been mandated under Article 41(1) 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;

b) the information to be submitted by the ICT third–party service providers that is necessary for the LO to carry out its duties;

c) the criteria for determining the composition of the joint examination team, their designation, tasks, and working arrangements;

d) the details of the competent authorities' assessment of the measures taken by CTPPs based on the recommendations of the LO.

This consultation paper and the included draft RTS cover the draft technical standards aimed at specifying the areas of (a), (b) and (d) indicated above. Point (c) related to the joint examination team will be specified in a separate draft RTS which will be consulted on at a later stage.

Next steps

The ESAs will consider the feedback received when finalising the draft RTS following this public consultation. The ESAs expect to submit the RTS by 17 July 2024 to the European Commission for adoption.

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

3. Background and rationale

Background

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 this consultation paper and the draft RTS, the ESAs have decided to divide the mandate of Article 41(1) of Regulation (EU) 2022/2554 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 (points (a), (b) and (d) above) and the other one 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. 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 taken the decision as described above.
4. This consultation paper and the included draft RTS cover the areas included in points (a), (b) and (d) of Article 41(1) of Regulation 2022/2554.

Rationale

5. 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.
6. 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.
7. 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.
8. 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.
9. 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.

4. Overview of questions for consultation

1. Do you agree with the content of information to be provided by ICT third party providers in the application for a voluntary request to be designated as critical? Please, provide comments on information to be added or removed including the rationale (Article 1)
2. Is the process to assess the completeness of opt-in application clear and understandable? (Article 2)
3. Is the list of information to be provided by critical ICT third-party service providers to the Lead Overseer that is necessary to carry out its duties clear and complete? Please, provide comments on information to be added or removed including the rationale (Article 3)
4. Do you agree with the content of Article 4 on remediation plan and progress reports?
5. Is the article on the structure and format of information provided by the critical ICT third-party service provider appropriate and structured? (Article 5)
6. Is the information to be provided by the critical ICT third-party service provider to the Lead Overseer complete, appropriate and structured? (Article 6 and Annex I)
7. Is Article 7 on competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer clear?
8. Do you agree with the impact assessment and the main conclusions stemming from it?

5. 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 to harmonise the 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[2], and in particular the second subparagraph of of Article 41(2) 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 6 months of time to the European Supervisory Authority (ESA) recipient of the voluntary request to be designated as critical from a ICT third-party service provider, the latter should submit an application that is complete and accurate. In case the application submitted is not complete, the recipient ESA should reject the application and should ask to the applicant ICT third-party service provider to re-submit a complete one.

(3) Regulation (EU) 2022/2554 mandates the Lead Overseer to carry out a comprehensive assessment of ICT risks that ICT TPPs 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.

(4) As a follow-up to the recommendations issued by the Lead Overseer to critical ICT third-party providers, the Lead Overseer will monitor 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 will be able to require the reports referred

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

to in Article 35(1) point (c) of Regulation (EU) 2022/2554,which should be intended as interim progress reports and final reports.

(5) With the same objective and as part of the information that critical ICT third-party providers should submit according to Article 35(1) of Regulation (EU) 2022/2554, the notification to the Lead Overseer by the critical ICT third-party service provider of its intention to follow the recommendations received needs to be complemented by a remediation plan where 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.

(6) 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.

(7) 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.

(8) 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. Such a template should take into account the fact that the ICT third party service providers have different structures than financial entities and therefore the templates should not fully mirror the templates of the register of information referred to in Article 28(3) of Regulation (EU) 2022/2554.

(9) 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 monitors and assesses the implementation by the critical ICT third-party service provider of the actions and remedies to comply with the recommendations. Competent authorities 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.

(10) 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. The 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.

(11) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Banking Authority, the European Insurance and Occupational Pensions Authority, the European Securities and Markets Authority (European Supervisory Authorities).

(12) 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[3], 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[4], 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[5].

HAS ADOPTED THIS REGULATION:

CHAPTER I

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

Article 1

Information to be provided by Information and Communication Technology 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 Information and Communication Technology (ICT) third-party service provider in the reasoned application for a voluntary request to be designated as critical in accordance with Article 31(1)(a) shall include all of the following:

[3] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

[4] 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).

[5] 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).

a) name of the legal entity;

b) a Legal Entity Identifier, which is a 20-character, alpha-numeric code based on the ISO 17442 standard (LEI code);

c) country of establishment;

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 EU financial entities, where applicable;

   i) name of the legal entities;

   ii) LEI code, where available;

   iii) registered office;

e) an estimation of the market share of the ICT third-party service provider in the financial sector and estimation of market share per type of financial entity as provided in Article 2 of Regulation 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 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 in the Union 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) LEI codes, where known to the ICT third-party service provider;

   (iii) type of financial entities determined in accordance with Article 2(1) of Regulation 2022/2554;

   (iv) the geographic location of the legal company, 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;

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 EU 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) 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 European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), collectively European Supervisory Authorities (ESA) may request clarifications of the information submitted.

Article 2

Assessment of completeness of application

1. The ICT third-party service provider shall submit its reasoned application to the EBA, ESMA or EIOPA including all information listed in Article 1 of this Regulation via means determined by ESA.

2. A complete application contains all information necessary for the assessment in Article 1 of this Regulation.

3. Where the recipient ESA considers that information provided in the application is incomplete, it shall request the missing information. If the ICT third-party service provider does not provide missing information by a date specified in the request, the recipient ESA shall not designate the applicant as a critical ICT third-party service provider. Within 30 working days of the receipt of the missing information, the recipient ESA shall inform the applicant ICT third-party service provider that the reasoned application is complete for the purpose of paragraph 5 of this Article.

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. The Lead Overseer may request critical ICT third-party service providers to provide information that is necessary to carry out its duties, transmitted 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 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 as defined in Article 2(2) of Regulation (EU) 2022/2554;

        (ii) the critical ICT third-party service provider and its subcontractors with a view to capture the entire technological value chain;

    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 its geographical spread;

    d) information about the critical ICT third-party service provider 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 management body and any other internal relevant committees;

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 customers for data portability, application portability and interoperability;

i) information about the exact location of the data centres and ICT production centres, including a list of all relevant premises and facilities of the critical ICT third-party service provider, including outside of 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, 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 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, and incident management;

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, 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 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;

w) any other 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 Regulation (EU) 2022/2554.

Article 4

Remediation plan and progress reports

1. In accordance with Article 35(1)(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:

    i) 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;

    ii) 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 relation to 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 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. provide a clear indication of where in the requested documentation the relevant piece of information can be found.

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 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 remediation 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 line 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 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.

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 • LEI 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 CTPP) • 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 LEI) of each subcontractor involved • Contact information of key staff responsible for each of the subcontracting relationships in the CTPP 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 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

Information Category	Key Information Elements
	relationships, including clauses restricting the usage of sensitive data • Explanation of the processes for selecting, engagingand monitoring subcontractors • Overview of performance metrics, service level agreements, or key performance indicators used to assess subcontractor performance
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 • Date and frequency of the audits of the subcontractors conducted by the critical ICT third-party service provider

6. Draft cost-benefit analysis / impact assessment

1. As per 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 next 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.

Problem identification

3. Regulation (EU) 2022/2554 (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 a 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;
- 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 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 one 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[6].

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.

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

Preferred option

17. Option B has been retained.

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: ASSESSMENT PERFORMED BY COMPETENT AUTHORITIES

26. 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.
27. 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

28. 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.
29. 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.
30. 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

31. 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 rigorous oversight, which can be costly in terms of compliance and addressing the recommendations issues by the Lead Overseers.	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 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	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

Stakeholder groups affected	Costs	Benefits
	training and additional resources with a different skill set than existing staff.	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.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Annex to the draft cost-benefit analysis - 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-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	(a) information about the arrangements between the CTPP, the FEs and its subcontractors. (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

Article 33(3) DORA	Article 3(2) RTS
	(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 (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

Article 33(3) DORA	**Article 3(2) RTS**
(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
(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;

Article 33(3) DORA	**Article 3(2) RTS**
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