Council of the European Union

Brussels, 28 October 2024
(OR. en)

14984/24

EF 330
ECOFIN 1209
CYBER 296
TELECOM 309
DELACT 198

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	24 October 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	C(2024) 6913 final
Subject:	COMMISSION DELEGATED REGULATION (EU) …/... of 24.10.2024 supplementing Regulation (EU) 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

Delegations will find attached document C(2024) 6913 final.

Encl.: C(2024) 6913 final

EUROPEAN
COMMISSION

Brussels, 24.10.2024
C(2024) 6913 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 24.10.2024

supplementing Regulation (EU) 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)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to harmonise and streamline the regulatory requirements enabling the conduct of oversight activities in the European Union. To that end, DORA introduces new roles and responsibilities for the European Supervisory Authorities (ESAs) and competent authorities.

In that regard, Article 41(1) of DORA mandates the ESAs to develop through the Joint Committee, common draft regulatory technical standards (RTS) further specifying the following:

(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 Lead Overseer 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 Lead Overseer.

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). This draft RTS cover the areas included in points (a), (b) and (d) of Article 41(1) of Regulation (EU) 2022/2554 and was transmitted to the Commission on 17 July 2024.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

As part of developing the standards set out in this draft regulation, the ESAs published the draft RTS on 8 December 2023 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' final report provides a full overview of stakeholder responses.

The respondents to the public consultation commented on all aspects of the proposed draft RTS. The key points raised were the following:

– The scope of the information to be provided by ICT third-party service providers in the voluntary request to be designated as critical;

– The content of the information to be provided by the critical ICT third-party service providers in the context of the oversight framework including information about their subcontracting arrangements;

– Structure and format that has to be used by critical third-party service providers when delivering information to the Lead Overseer;

– Competent authorities' assessment of the risks identified in the recommendations of the Lead Overseer to the critical third-party service provider;

A total of 44 responses were received to the public consultation, covering all relevant stakeholders. The ESAs assessed the concerns raised and made changes to the draft RTS where relevant.

The main changes introduced to the draft RTS 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 ICT 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.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

Article 1 sets out the information to be provided by ICT third-party service providers in the application for a voluntary request to be designated as critical.

Articles 2-5 lay down the content of information to be provided by critical ICT third-party service providers to the Lead Overseer (Article 2), including the information to be provided after the issuance of recommendations (Article 3), the structure and format of the information (Article 4) and the information on subcontracting arrangements that will have to be provided (Article 5).

Article 6 covers the competent authorities' assessment of the measures taken by critical ICT third-party service providers based on recommendations of the Lead Overseer.

Article 7 contains the final provisions on entry into force.

COMMISSION DELEGATED REGULATION (EU) …/...

of 24.10.2024

supplementing Regulation (EU) 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) An ICT third-party service provider which decides to submit a voluntary request to be designated as critical should provide the receiving European Supervisory Authority (ESA) with all the necessary information to demonstrate its criticality according to the principles and criteria set out in Regulation (EU) 2022/2554. For this reason, the information to be included in the voluntary request application should be sufficiently detailed and complete to enable a clear and complete assessment of criticality under Article 31(11) of that Regulation. The relevant ESA should reject any incomplete application and request the missing information.

(3) The legal identification of ICT third-party service providers within the scope of this Regulatory Technical Standard 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.

(4) As a follow-up to the recommendations issued by the Lead Overseer to critical ICT third-party service providers, the Lead Overseer should monitor critical ICT third-party service providers' compliance with the recommendations. With a view to ensure 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

[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, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

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

(5) For the purpose of the assessment specified in Article 42(1) of Regulation (EU) 2022/2554, according to which Lead Overseer is obliged to evaluate whether the explanation provided by critical ICT third-party service 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 a description of the actions and measures that have been taken to mitigate the risks outlined in the recommendations, along with their respective deadlines. Such explanation should take the form of a remediation plan.

(6) 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.

(7) 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 any 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 service 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.

(8) 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 implementation of actions and remedies of the critical ICT third-party service providers.

(9) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[2] and delivered an opinion on 22 July 2024.

(10) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the ESAs.

(11) The Joint Committee of the ESAs has conducted open public consultations on the draft regulatory technical standards upon 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:

Article 1
Information to be provided by ICT third-party service provider in the application to be designated as critical

1. The information and communication technology (ICT) third-party service provider shall submit the following information in the reasoned application for a voluntary request under Article 31(11) of Regulation (EU) 2022/2554 to be designated as critical pursuant to Article 31(1), point (a), of Regulation (EU) 2022/2554:

   (a) name of the legal entity;

   (b) legal entity identification code;

   (c) name of contact person and contact details of the critical ICT third-party service provider;

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

---

2 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(e) description of the corporate structure including at least information on its parent company and other related undertakings providing ICT services to Union financial entities. That information shall include where applicable;

(i) name of the legal entities;

(ii) legal entity identification code;

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

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

(g) a description of each ICT service provided 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;

(h) 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 (EU) 2022/2554;

(iv) the geographic location from which the ICT services are provided to that specific legal entity;

(i) 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 where available;

(j) a self-assessment as regards the following:

(1) the degree of substitutability for each ICT service provided by the applicant considering the following:

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

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

– 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;

(2) 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;

(k) information on a future business strategy 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;

(l) identification of the subcontractors of the ICT third-party service provider which have been designated as critical ICT third-party service providers;

(m) any 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.

Article 2

Content, structure and format of the information to be submitted, disclosed or reported 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 that is necessary by the Lead Overseer to carry out its oversight duties in accordance with the requirements of Regulation (EU) 2022/2554.

2. The information referred to in paragraph 1 includes inter alia the following:

(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 of 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 any of the following :

(i) entities that 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) entities that 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;

(iii) entities that 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 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 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 information about compliance with all relevant regulations and national and international standards where applicable;

(h) information about technical and organisational measures to ensure data protection and data confidentiality, including personal and non-personal data, implemented control measures to protect sensitive data, access controls, encryption practices, data breach response plan; when in regards processing of personal data the ICT third-party service provider is subject to laws from third-countries, including third-country government access request, list of the countries and the laws applicable.

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

(j) information about the location of the data centres and ICT production centres used 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;

(k) 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 service provider;

(l) 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;

(m) 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, including 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;

(n) information about the change management framework, including policies, procedures, and controls of the critical ICT third-party service provider and its subcontractors;

(o) 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;

(p) 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;

(q) 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;

(r) 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 SLOs;

(s) 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) compliance and available 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 available 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;

(u) 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;

(v) information about any remediation plan to address recommendations pursuant to Article 3, and relevant related information to confirm remedies have been implemented;

(w) information about available employee training schemes and security awareness programs, including, where relevant, information on 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;

(x) 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 3

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

1. The critical ICT third-party service provider shall provide to the Lead Overseer a report containing a remediation plan in relation to the recommendations and remedies that the critical ICT third-party service provider plans to implement in order to mitigate the risks identified in the recommendations referred to in Article 35(1), point (d) of Regulation (EU) 2022/2254. The report 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 report provided by the critical ICT third-party service 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 4

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 and in the form set out by the Lead Overseer.

2. When providing information to the Lead Overseer, the critical ICT third-party service 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 a language customary in the sphere of international finance.

Article 5

Template for providing information on subcontracting arrangements

A critical ICT third-party service provider which is required to share information on subcontracting arrangements shall provide the information to the Lead Overseer according to the template set out in the Annex.

Article 6

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

1. As part of their supervision of financial entities, the competent authority shall assess the impact on the financial entities of the measures taken by the critical ICT third-party service provider based on the recommendations of the Lead Overseer in accordance with the principle of proportionality.

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

   (i) the adequacy and the coherence of the corrective and remedial measures implemented by the financial entities to mitigate the risks identified in the recommendations;

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

   (iii) the view of any other competent authorities who have been consulted in accordance with Article 42(5) of Regulation (EU) 2022/2554;

   (iv) 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 its 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 recommendations, including the cross-border impacts of these risks when impacting financial entities operating in more than one Member State.

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

Article 7

Entry into force

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

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 24.10.2024

For the Commission
The President
Ursula VON DER LEYEN