JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Consultation Paper

on Draft Regulatory Technical Standards

to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. Responding to this consultation

The ESAs invite comments on all matters in this paper and on the specific questions summarised in Paragraph 6.

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 EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 11.09.2023. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with the ESAs' rules on 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 ESAs' Boards of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of EBA, EIOPA and ESMA websites respectively.

2. Executive Summary

Article 28(2) of Regulation (EU) 2022/2554 requires from financial entities that they adopt and regularly review, as part of their ICT risk management framework, a strategy on ICT third-party risk. The strategy on ICT third-party risk shall include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. The ESAs are mandated to develop jointly draft regulatory technical standards to further specify the detailed content of this policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.

In line with Regulation (EU) 2022/2554, the draft RTS sets out requirements for the policy of financial entities on their use of ICT third-party service providers, including ICT intragroup providers and concerns all ICT services provided by them that support critical or important function. The RTS applies to all such ICT services and is not limited to outsourcing arrangements.

The financial entity's policy on the use of ICT third-party service providers is defining crucial parts of the financial entities' governance arrangements, risk management and internal control framework with regard to the use of ICT services provided by ICT third-party service providers and should ensure that the financial entity remains in control of its operational risks, information security and business continuity throughout the life cycle of contractual arrangements with such providers.

It is crucial that financial entities perform risks assessments and due diligence processes before they enter in contractual arrangements with ICT third-party service providers and that they ensure that they can exit from such arrangements where necessary and ensure business continuity for the supported critical or important function, e.g. where a service is not provided appropriately, external ICT systems fail or where a service cannot be received any longer following imposed sanctions.

The ESAs will finalise the draft RTS following its public consultation and aims to submit it in January 2024 to the European Commission for adoption.

Next steps

The ESAs will finalise the draft RTS following its public consultation and aims to submit it in January 2024 to the European Commission for adoption.

3. Background and rationale

1. Article 28(2) of DORA requires from financial entities that: “as part of their ICT risk management framework, financial entities [...] shall adopt, and regularly review, a strategy on ICT third-party risk […]The strategy on ICT third-party risk shall include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers and shall apply on an individual basis and, where relevant, on a sub-consolidated and consolidated basis…”.

2. In accordance with Article 28 (10) of DORA, “the ESAs shall, through the Joint Committee, develop draft regulatory technical standards to further specify the detailed content of the policy … in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers”.

3. The draft RTS has been developed considering already existing specifications provided in Guidelines on outsourcing arrangements published by the European Supervisory Authorities (EBA, ESMA and EIOPA) and other relevant specifications provided in the EBA Guidelines on ICT and security risk management.

4. Furthermore, when developing those draft regulatory technical standards, the ESAs have taken into account the size and the overall risk profile of the financial entities, and the nature, scale and complexity of their services, activities and operations.

5. In line with DORA, the draft RTS sets out requirements for the policy of financial entities on their use of ICT third party service providers, including ICT intra group service providers and concerns all ICT services provided by them that support critical or important function.

6. The draft RTS deals with ICT third party services providers and ICT intragroup service providers in the same way. The risks towards those services providers may be different but the requirements applicable to them are similar. Intra group service providers are considered to form a subcategory of ICT third party service providers as DORA is also applied on an individual basis.

7. The use of ICT service providers cannot reduce the responsibility for the financial entities and their management bodies to manage their risks and to comply with legislative requirements, especially when critical and important functions are supported by ICT third party service providers. The draft RTS includes provisions that ensure that financial entities clearly assign the internal responsibilities for the approval, management, control, and documentation of contractual arrangements on the use of ICT services provided by ICT third-party service providers to support their critical or important functions. Such provisions strengthen the accountability within the involved business areas within financial institutions.

8. The draft RTS further specify the requirements for the application in a group context where this is applicable. In this context, the EU parent undertaking or the parent undertaking in a Member State shall ensure that the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as referred to in Article 28 (2) of Regulation (EU) 2022/2554, is implemented consistently in their subsidiaries and adequate for the effective application of the RTS at all relevant levels. This is to ensure that, where applicable, a group wide management of ICT risks can be provided for.

9. The financial entity's policy on the use of ICT third party service providers defines crucial parts of the financial entities governance arrangements, risk management and internal control framework with regard to the use of ICT services provided by ICT third party providers. This policy should thus ensure that the financial entity remains in control of its operational risks, information security and business continuity throughout the life cycle of contractual arrangements with such providers. To be effective, the RTS covers the whole life cycle of such arrangements and starts with the planning phase of the buy in of ICT services, including risk assessments and due diligence processes, covers the ongoing service delivery, monitoring and auditing, and ends with the exit from such arrangements.

10. In order to ensure that the ICT services are provided with the needed quality and that there are no additional material operational or reputational risks, financial entities shall assess the business reputation of the ICT third party service provider and shall ensure that it has available the resources, including expertise and adequate financial, human and technical resources, information-security arrangements, an appropriate organisational structure, including risk management and internal controls and is able to comply with the contractual and regulatory requirements.

11. The draft RTS needs to be read together with Regulation (EU) 2022/2554 which defines what are ICT services, what is critical and important function and includes provisions on mandatory contractual arrangements with ICT third party providers. While this RTS set out requirements for ICT services supporting critical or important functions, Regulation (EU) 2022/2554 sets also risk management requirements for ICT services supporting other functions that are not considered critical or important. The draft RTS also needs to be read in conjunction with other draft RTS, e.g. on sub-outsourcing, the register of ICT services provided and business continuity planning.

Next Steps

The ESAs will finalise the draft RTS following its public consultation and submit it to the European Commission for adoption.

4. Draft regulatory technical standards

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards for specifying the detailed content of the policy on the contractual arrangements regarding on the use of ICT services supporting critical or important functions provided by ICT third-party service providers

(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 and, in particular Article 28(10) thereof,

Whereas:

(1) The framework on digital operational resilience for the financial sector established by Regulation (EU) 2022/2554 requires that financial entities set out certain key principles to manage ICT third-party risk, which are of particular importance when financial entities engage with ICT third-party service providers to support their critical or important functions.

(2) To ensure the sound monitoring of ICT third-party risk in the financial sector, financial entities, as part of their ICT risk management framework, should adopt, and regularly review, a strategy on ICT third-party risk. In accordance with Article 28(2) of Regulation (EU) 2022/2554, the strategy on ICT third-party risk should include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers and should apply on an individual and, where relevant, on a sub-consolidated and consolidated basis.

(3) To ensure a consistent and uniform application by financial entities and supervisory convergence across the European Union, it is necessary to further specify the content of the policy referred to in Article 28(2) of Regulation (EU) 2022/2554.

(4) Financial entities vary widely in their size, structure, and internal organisation and in the nature and complexity of their activities. It is therefore necessary to take into account that diversity while imposing certain fundamental regulatory requirements which are appropriate for all financial entities when developing the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions by ICT third party providers (here after “relevant contractual arrangements”).

(5) Where belonging to a group, financial entities should ensure that the policy on the use of ICT services supporting critical or important functions by ICT third party providers is applied in a consistent and coherent way within the group.

(6) When applying the policy on the use of ICT services supporting critical or important functions, ICT intra-group service providers, where applicable, including those fully or collectively owned by financial entities within the same institutional protection scheme, undertaking the provision of ICT services, should be considered as ICT third party services providers. The risks posed by those ICT services providers may be different but the requirements applicable to them are the same in accordance with Regulation (EU) 2022/2054. In a similar way, this policy should apply to subcontractors to ICT third-party service providers where this is relevant in case a chain of ICT third-party service providers exists.

(7) The ultimate responsibility of the management body in managing a financial entity's ICT risk is an overarching principle which is also applicable regarding the use of ICT third-party service providers. This responsibility should be further translated into the continuous engagement of the management body in the control and monitoring of ICT risk management, including in the adoption and review, at least once per year, of the policy on the use of ICT services supporting critical or important functions by ICT third-party service providers.

(8) To ensure appropriate reporting to the management body, the policy should clearly specify and identify the internal responsibilities for the approval, management, control and documentation of contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.

(9) In order to take into account all possible risks that could arise when contracting ICT services supporting critical or important function, the structure of this policy should follow all the steps of the life cycle regarding contractual arrangements for the use of ICT services supporting critical or important functions provided by ICT third-party service providers.

(10) To mitigate the risks identified, this policy should specify the planning of relevant contractual arrangements, including the risk assessment, the due diligence, and the approval process for new or material changes to those third-party contractual arrangements. In addition, in order to manage all risks that could arise before entering into an arrangement with an ICT third-party service provider, the policy should specify an appropriate and proportionate process to select and assess the suitability of prospective ICT third-party service providers and prescribe that the financial entity assesses a non-exhaustive list of aspects related to the business reputation, the resources including expertise and adequate financial, human and technical resources, information-security, appropriate organisational structure, including risk management, and internal controls that the ICT third party service providers should have in place.

(11) For the purpose of ensuring a sound risk management in the provision of ICT services supporting critical or important functions by ICT third-party service providers through contract management, this policy should contain information with regard to the implementation, monitoring and management of contractual arrangements for the use of ICT services supporting critical or important functions including at consolidated and sub-

consolidated level where applicable. This includes requirements on the contractual clauses on mutual obligations of the financial entities and the ICT third-party service providers that should be set out in a written agreement. This policy should ensure the financial entities' or appointed third parties' and competent authorities' rights to inspections and access to information and should also further specify the exit strategies and termination processes.

(12) The European Supervisory Authorities have 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 ESA's Stakeholder Groups established in accordance with Article 37 of Regulation (EU) No 1093/2010, Article 37 of Regulation (EU) No 1094/2010 and Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council.

HAS ADOPTED THIS REGULATION:

Article 1

Complexity and risk considerations

1. The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall take into account, for the purpose of Articles 3 to 11, elements of increased complexity or risk, including elements relating to the location of the ICT third-party service provider or its parent company, the nature of data shared with the ICT third-party service providers, the location of data processing and storage, whether the ICT third-party service providers are part of the same group of the financial entity and the potential impact of the related risks and disruptions on the continuity and availability of the financial entity's activities.

Article 2

Group application

2. Where this Regulation applies on a sub-consolidated or consolidated basis, the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial statements for the group shall ensure that the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as referred to in Article 28 (2) of Regulation (EU) 2022/2554, is implemented consistently in their subsidiaries and is adequate for the effective application of this Regulation at all relevant levels.

Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?

Article 3

Governance arrangements regarding the policy on the use of ICT services supporting critical or important functions

1. As part of the strategy on ICT third-party risk referred to in Article 28(2) of Regulation (EU) 2022/2554, and taking into account the multi-vendor strategy referred to in Article 6(9), the management body of a financial entity shall adopt a written policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers, and ensure its implementation on an individual and, as applicable, on a sub-consolidated and consolidated basis.
2. The management body shall review the policy referred to in paragraph 1 at least once a year and update it where necessary. Changes made to the policy shall be implemented in a timely manner and where appropriate also to the relevant contractual arrangements.
3. The policy referred to in paragraph 1 shall define or refer to a methodology for determining which ICT services support critical or important functions. The policy shall also specify when this assessment should be conducted and reviewed.
4. The policy referred to in paragraph 1 shall clearly assign the internal responsibilities for the approval, management, control, and documentation of relevant contractual arrangements and shall ensure that appropriate skills, experience and knowledge are maintained within the financial entity to effectively oversee relevant contractual arrangements.
5. Without prejudice to the final responsibility of the financial entity to effectively oversee relevant contractual arrangements, the policy referred to in paragraph 1 shall foresee that the financial entity assesses that the ICT third party service provider has sufficient resources to ensure that the financial entity complies with all its legal and regulatory requirements.
6. The policy referred to in paragraph 1 shall clearly identify, in accordance with Article 5(3) of Regulation (EU) 2022/2554, the role or member of senior management responsible for monitoring the relevant contractual arrangements. This policy shall define how this role or member of senior management shall cooperate with the control functions where it is not part of it and define the reporting lines to the management body, including the nature and frequency of the documents to report.
7. The policy referred to in paragraph 1 shall ensure that the relevant contractual arrangements are consistent with the financial entity's ICT risk management framework referred to in Article 6(1), the information security policy under Article 9(4), the business continuity policy under Article 11 and the requirements on incident reporting under Article 19 of Regulation (EU) 2022/2554.
8. The policy referred to in paragraph 1 shall require that ICT services supporting critical or important functions provided by ICT third party service providers are subject to independent review and included in the financial entity's audit plan.

9. The policy referred to in paragraph 1 shall explicitly specifies that the relevant contractual arrangements:
    a. do not relieve the financial entity and its management body of its regulatory obligations and its responsibilities to its clients;
    b. shall not hinder effective supervision of a financial entity and shall not contravene any supervisory restrictions on services and activities;
    c. have provisions in place that ensure that the ICT third party service providers cooperate with the competent authorities; and
    d. have provisions in place that ensure that the financial entity, its auditors, and competent authorities have effective access to data and premises relating to the use of IT services supporting critical or important functions.

Question 2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?

Article 4

ICT third-party service providers and ICT services supporting critical or important functions

1. As part of the ICT third-party risk strategy referred to in Article 28 (2) of Regulation (EU) 2022/2554, and taking into account the multi-vendor strategy referred to in Article 6(9), where applicable, and the overall ICT risk management framework, the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall differentiate, including for sub-contractors, between the:
    (a) ICT third-party service providers that are authorised or registered by a competent authority in a Member State or subject to the oversight framework under Section II of Chapter V of Regulation (EU) 2022/2554 or ICT third-party service providers that are authorised or registered by a supervisory authority from a third country and are subject to supervision or oversight and those that are not;
    (b) provision of ICT services supporting critical or important functions by ICT intra-group service providers and by ICT third-party service providers that are outside the group;
    (c) provision of ICT services supporting critical or important functions by ICT third-party service providers located within a Member State and the ones located in third countries, also considering the location where the ICT services are actually provided from and the location where the data is actually processed and stored.

Question 3: Is article 4 appropriate and sufficiently clear?

Article 5

Main phases of the life cycle for the use of ICT services supporting critical or important functions provided by ICT third- party service providers

1. The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall specify the requirements, including principles, responsibilities, and procedures, for each main phase of the lifecycle of the use of such ICT services, covering at least:

   (d) the responsibilities of the management body in line with Article 5(2) of Regulation (EU) 2022/2554, including its involvement, as appropriate, in the decision-making process on the use of ICT services supporting critical or important functions provided by ICT third-party service providers;

   (e) the planning of contractual arrangements for the use of ICT services supporting critical or important functions provided by ICT third-party service providers including the risk assessment, the due diligence and the approval process of new or material changes to relevant third-party contractual arrangements;

   (f) the involvement of business units, internal controls and others relevant units in respect of contractual arrangements for the use of ICT services supporting critical or important functions provided by ICT third-party service providers;

   (g) the implementation, monitoring and management of contractual arrangements for the use of ICT services supporting critical or important functions including at consolidated and sub-consolidated level, where applicable;

   (h) the documentation and record-keeping, taking into account the requirements on the register of information in accordance with Article 28(3) of Regulation (EU) 2022/2554;

   (i) the exit strategies and termination processes.

Question 4: Is article 5 appropriate and sufficiently clear?

Article 6

Ex-ante risk assessment

1. The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall include the requirement to define the business needs of the financial entity before entering into contractual arrangements on the use of ICT services provided by prospective third-party service providers, supporting critical or important functions.

2. The policy referred to in paragraph 1 shall require that, before entering into a contractual arrangement with an ICT third-party service provider a risk assessment shall be conducted at financial entity level and, where applicable, at consolidated and sub-consolidated level, taking into account all the relevant requirements under of Regulation (EU) 2022/2554 and applicable sectoral legislations and regulations. This risk assessment shall consider, in particular, the impact of the provision of ICT services supporting critical or important functions by ICT third-party service providers on the financial entity and all its risks, including operational risks, legal risks, ICT risks, reputational risks, risks to the protection of confidential or personal data, risks linked to the availability of data, risks linked to where the location of the data is processed and stored and the location of the ICT third-party service provider as well as ICT concentration risks at entity level in accordance with Article 29 of Regulation (EU) 2022/2554.

Article 7

Due diligence

1. In accordance with Article 28 (4) of Regulation (EU) 2022/2554, the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall specify an appropriate and proportionate process for selecting and assessing the prospective ICT third-party service providers taking into account whether or not the ICT third party service provider is an intragroup ICT service provider and prescribe that the financial entity assesses, before entering into a contractual arrangement, at least whether the ICT third-party service provider:

    (a) has the business reputation, sufficient abilities, expertise and adequate financial, human and technical resources, information security standards, appropriate organisational structure, including risk management and internal controls and, if applicable, the required authorisation(s) or registration(s) to provide the ICT services supporting the critical or important function in a reliable and professional manner, the ability to monitor relevant technological developments and identify ICT security leading practices and implement them where appropriate to have an effective and sound digital operational resilience framework;

    (b) uses or intends to use ICT sub-contractors to perform material part of their services;

(c) is located, processes or stores the data in a third country and if this is the case, if this practice elevates the level of operational risks, reputational risks or the risk of being affected by sanctions that may impact the ability of the ICT third-party service provider to provide the ICT services or the financial entity to receive those ICT services;

(d) consents to arrangements that ensure that it is effectively possible to conduct audits, including onsite, by the financial entity itself, appointed third parties, and competent authorities at the ICT service provider,

(e) acts in an ethical and socially responsible manner and adheres to human and children's rights, applicable principles on environmental protection, and ensures appropriate working conditions including the prohibition of child labour.

2. The policy referred to in paragraph 1 shall specify the required level of assurance concerning the effectiveness of ICT third-party service providers' risk management framework for the ICT services to be provided by ICT third-party providers to support critical or important functions. This policy shall require that the due diligence process shall include the assessment of the existence of risk mitigation and business continuity measures and how their functioning within the ICT third-party service provider is ensured.

3. The policy referred to in paragraph 1 shall:

(a) determine the due diligence process for selecting and assessing the prospective ICT third-party service providers, including which of the elements listed in paragraph 1 points (a) to (e) shall be used for the required level of assurance.

(b) determine that the element listed in paragraph 1 point (a) shall be used, where the selected elements in paragraph 1 points (b) to (e) are not sufficient to ensure an appropriate assessment of the ICT third-party service providers suitability. The assessment of the ICT third-party provider's suitability shall always include at least one of the elements listed in paragraph 1 points (a) and (c).

(c) consider at least, the following elements to be used as part of the process for selecting and assessing the prospective ICT third-party service providers:

i. audits performed by the financial entity itself or on its behalf;
ii. the use by the financial entity of relevant appropriate third party certifications;
iii. the use by the financial entity of independent audit reports made on behalf of the ICT third-party service provider;
iv. the use by the financial entity of audit reports of the internal audit function of the ICT third-party provider;
v. the use by the financial entity of other relevant publicly available information.

Question 5: Are articles 6 and 7 appropriate and sufficiently clear?

Article 8

Conflict of interest

1. The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall specify the appropriate measures to identify, prevent and manage actual or potential conflicts of interest arising from the use of ICT third party service providers before entering relevant contractual arrangements and provide for an ongoing monitoring of conflicts of interests.

2. Where ICT services are provided by ICT intra-group service providers, the policy referred to in paragraph 1 shall specify the conditions, including the financial conditions, for the ICT services supporting critical or important functions to be set at arm's length.

Question 6: Is article 8 appropriate and sufficiently clear?

Article 9

Contractual clauses for the use of ICT services supporting critical or important functions

1. The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall specify that the relevant contractual arrangement shall be written and shall include all the elements set out by Article 30(2) of Regulation (EU) 2022/2554. The policy shall also include elements regarding ICT requirements, in accordance with that Regulation, as well as other relevant European and national regulations as appropriate.

2. The policy referred to in paragraph 1 shall specify that the relevant contractual arrangements shall include information access, inspection, audit, and ICT testing rights. The policy shall foresee that without prejudice to the final responsibility of the financial entity, the financial entity shall use for this purpose:

   (a) its own internal audit or an appointed third party;

   (b) pooled audits and pooled ICT testing, including threat-led penetration testing, organised jointly with other contracting financial entities or firms that use ICT services of the same ICT third-party service provider, that are performed by them and these contracting financial entities or firms or by a third party appointed by them;

(c) third-party certifications and third-party or internal audit reports made available by the ICT third-party service provider.

3. The policy referred to in paragraph 1 shall specify whether third-party certifications and reports as referred to in paragraph 2 (c) are adequate and sufficient to comply with their regulatory obligations and shall not rely solely on these reports over time. In this regard, the policy shall require that the financial entity shall use of the methods referred to paragraph 2 (c) only if it:

(a) is satisfied with the audit plan for the relevant contractual arrangements;

(b) ensures that the scope of the certifications or audit reports cover the systems and key controls identified by the financial entity and the compliance with relevant regulatory requirements;

(c) thoroughly assesses the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;

(d) ensures that key systems and controls are covered in future versions of the certification or audit report;

(e) is satisfied with the aptitude of the certifying or auditing party;

(f) is satisfied that the certifications are issued, and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;

(g) has the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; whereby the number and frequency of such requests for scope modification shall be reasonable and legitimate from a risk management perspective; and

(h) retains the contractual right to perform individual and pool audits at their discretion with regard to the relevant contractual arrangements and activate them according to a predefined frequency.

4. The policy referred to in paragraph 1 shall ensure that material changes to the relevant contractual agreement shall be formalised in a written document, dated, and signed by all parties and shall specify the renewal process for contractual arrangements.

Question 7: Is article 9 appropriate and sufficiently clear?

Article 10

Monitoring of the contractual arrangements for the use of ICT services supporting critical or important functions

1. The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall ensure that the relevant contractual arrangements specify the measures and key indicators to monitor, on an ongoing basis, the performance of ICT third party service providers, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial entity's relevant policies and procedures. The policy should also specify measures that apply when service levels are not met including, where appropriate penalties.

2. The policy shall also prescribe how the financial entity shall assess that the ICT third party service providers used for the ICT services supporting critical or important functions meets appropriate performance and quality standards in line with the contractual arrangement and the financial entity's own policies by ensuring that:

    (a) the ICT third-party service providers address appropriate reports on their activities and services provided to the financial entity, including periodic reports, incidents reports, service delivery reports, reports on ICT security and on business continuity measures and testing;

    (b) the performance of ICT third-party service providers is assessed with key performance indicators, key control indicators, audits, self-certifications and independent reviews in line with the financial entity's ICT risk management framework;

    (c) other relevant information is received from the ICT third-party service provider;

    (d) the financial entity is notified and responds to ICT related incident and operational or security payment related incidents;

    (e) an independent review and compliance audits with legal and regulatory requirements and policies are performed;

3. The policy shall prescribe that the assessment referred to in paragraph 2 should be documented and its results should be used to update the financial entity's risk assessment set out in Article 6.

4. The policy referred to in paragraph 1 shall define the appropriate measures that the financial entity shall adopt if it identifies shortcomings of the ICT third-party service provider in the provision of the ICT services supporting critical or important functions or the compliance with contractual arrangements or legal requirements and how the implementation of such measures shall be monitored to ensure that they are effectively

complied within a defined timeframe, taking into account the materiality of the shortcomings.

Question 8: Is article 10 appropriate and sufficiently clear?

Article 11

Exit and termination of contractual arrangements for the use of ICT services supporting critical or important functions

Without prejudice to Article 28 (7) and (8) of Regulation (EU) 2022/2554, the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall include requirements for a documented exit plan for each ICT service supporting critical or important functions provided by an ICT third-party service provider and their periodic review and testing, taking into account possible service interruptions, inappropriate or failed service delivery or the unexpected termination of a relevant contractual arrangement. The exit plan shall be realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the relevant contractual arrangements.

Question 9: Is article 11 appropriate and sufficiently clear?

Article 12

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,

For the Commission

The President

5. Accompanying documents

Draft cost-benefit analysis / impact assessment

1. As per Article 15(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) which analyses 'the potential related costs and benefits'.

2. This analysis presents the IA of the main policy options included in this Consultation Paper (CP) on regulatory technical standards (RTS) to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554.

Problem identification

3. Financial entities' reliance on the use of ICT is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in recent years, helping cost reduction in financial intermediation, enabling business expansion and business models changes, and enabling the scalability of financial activities while offering a wide range of ICT tools to manage complex internal processes.

4. With the growing digitalisation the scope, nature and scale of third-party arrangements has changed and increased over time. In particular, the use of ICT services provided by third parties that support critical or important functions became more common, leading to more dependencies and more concentrated ICT risks. In addition to the concentration of IT infrastructures in single financial entities, high concentrations of ICT services within a limited number of third-party service providers, including intragroup ICT service providers, have the potential to lead to risks for the stability of the financial market, particularly if no additional safeguards would be implemented.

5. The extensive use of ICT services and their technical and global nature, have also led to increasingly complex contractual arrangements, where contractual terms are not always tailored to the prudential standards or other regulatory requirements to which financial entities are subject. For example, the contractual arrangements may not provide for sufficient safeguards that allow for the fully-fledged monitoring of subcontracted services, thus rendering financial entities unable to assess the associated risks and competent authorities to supervise if critical and important functions are provided in a way that complies with the regulatory requirements. Moreover, as ICT

third-party service providers often provide standardised services to different types of clients, such contractual arrangements do not always cater adequately for the individual or specific needs of financial industry actors.

6. In the absence of clear and bespoke standards at EU level applying to the contractual arrangements concluded with ICT third-party service providers, the external factors of ICT risks have not been comprehensively addressed. Consequently, it is necessary to set out certain key principles to guide financial entities' management of ICT third-party risk, which are of particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions. Those key principles are set without prejudice that some financial entities are subject to even wider risk management requirements that require them to manage all risks, including ICT risks that exist in the supply chain.

7. In this context, as part of the ICT risk management framework referred to in Article 6(1), and the strategy on ICT third party risk the ESAs have been mandated under Article 28(10) Regulation (EU) 2022/2554 to develop draft regulatory technical standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.

Policy objectives

8. The draft regulatory technical standards specifying the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers aims to establish a common framework for such policies across Member States of the EU. The objective of this framework is to enable financial entities to manage their third-party risk with regard to ICT services supporting critical or important functions provided by ICT third-party service providers in line with the prudential requirements, and, in this regard, to ensure a level playing field when using such services.

Baseline scenario

9. With the entry into force of DORA, financial entities must comply with Chapter V "Managing of ICT third-party risk", Section I "Key principles for a sound management of ICT third party risk" of DORA.

10. The above legal requirements form the baseline scenario of the impact assessment, i.e. the impact caused by DORA is not assessed within this impact assessment, which focuses only on areas where further specifications have been provided in the regulatory technical standards.

11. The following aspects have been considered when developing the RTS.

POLICY ISSUE 1: DEFINITION OF CRITICAL AND IMPORTANT FUNCTIONS

Options considered

12. Option A: relying on the definition provided under DORA but providing more detailed criteria regarding the notion of "critical and important functions".

13. Option B: Referring to definition of DORA only as the draft RTS is about the content of the policy.

Cost-benefit analysis

14. Specifications to the definition would lead to a higher level of harmonization. However, a too specific definition would create the risk that it leaves out some aspects that might become more relevant over time. In addition, considering the different types of financial entities that are subject to DORA, relying on the definition within DORA, without the provision of detailed specifications seems to be more appropriate.

Preferred option

15. Option B has been retained.

POLICY ISSUE 2: GOVERNANCE ARRANGEMENTS REGARDING THE POLICY ON THE USE OF ICT SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTION

Options considered

16. Option A: Inclusion of additional specifications regarding governance arrangements:

- *Clarification of responsibilities of the management body with regard to the adoption and the oversight of the implementation of the policy on ICT services provided by third-party service provides in relation to critical or important functions.*
- *Clarification of the role of internal controls in this context*
- *Clarification on the frequency of the policy review (at least every year and when necessary).*
- *Clarification that the contractual arrangements should be consistent with the ICT business continuity policy requirement as referred to in Article 11(1) of DORA*

- *Necessary to provide for clarity regarding the continuous responsibility for ensuring that the financial entity can be supervised, including that measures can be implemented*

17. Option B: No additional governance arrangements

Cost-benefit analysis

18. The RTS includes governance requirements that aim to ensure that contractual arrangements with third-party providers of ICT services supporting critical and important functions do not impede financial entities from fulfilling the prudential requirements under DORA.

19. The RTS requires that the internal responsibilities and all the associated skills, experience and knowledge are maintained within the financial entity to ensure an effective monitoring and oversight of the contractual arrangements. This requirement is necessary to provide for clarity regarding continuous responsibility for ensuring that the third-party provider and the financial entity can be supervised.

20. Regarding the frequency of the policy review, DORA set out that tit should be done regularly. The requirement to review it at least once a year was seen as necessary considering the rapid expansion of the provision of ICT services by third part providers to financial entities, new technology and business opportunities. In this case, it is not disproportionate that the review of the policy should be performed annually. In case, there are no changes, then the process will still not be burdensome for financial entities.

21. The contractual arrangements should be consistent with the ICT business continuity policy requirement as referred to in Article 11(1) of DORA, to ensure consistency throughout the framework.

22. These governance requirements are not expected to have material additional costs but should provide benefits in terms of clearer regulatory and supervisory expectations to financial entities. Therefore, their inclusion in the RTS was seen as necessary.

Preferred option

23. Option A has been retained.

POLICY ISSUE 3: MAIN PHASES OF THE LIFE CYCLE FOR THE USE OF ICT SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS PROVIDED BY ICT THIRD PARTY SERVICE PROVIDERS

Options considered

24. Option A: Specification that the policy should cover the whole lifecycle of contractual arrangements

25. Option B: Focus on only the implementation of contractual arrangements themselves

Cost-benefit analysis

26. The specification that the policy should cover the whole lifecycle of contractual arrangement from pre phase to exit will ensure an appropriate risk management and move to another service provider (in-house or third party) in the case of insufficient or failed service provision.

27. Ex-ante risk assessment, due diligence and conflicts of interest should be included to manage and plan the provision of services and to ensure that it will be in line with financial entities' own regulatory requirements. Termination and exit strategies should be included to limit and manage dependencies. Exit plans must already exist when entering into such arrangements that are critical and important to ensure that the financial entity can react in good time if services are provided insufficiently or if the service provider fails.

28. Option A has been retained.

POLICY ISSUE 4: RISK ASSESSMENT OF ICT SERVICE PROVIDERS

Options considered

29. Option A: Same risk assessment for ICT intragroup and ICT third-party service providers

30. Option B: Different risk assessment for ICT intragroup and ICT third-party service providers

Cost-benefit analysis

31. The ex-ante risk assessment is required to be the same for both third party and ICT intragroup service providers since these risks need to be considered at individual basis due to potential future events like resolution or sale. Lak of such requirements at intragroup level may lead to a situation where the same standards are not applied for internal service providers that leads to an underestimation of risks related to ICT services.

Preferred option

32. Option A has been retained

POLICY ISSUE 5: DUE DILIGENCE OF ICT SERVICE PROVIDERS

Options considered

33. Option A: Same due diligence for ICT intragroup and ICT third party service providers

34. Option B: Different due diligence for ICT intragroup and ICT third party service providers

Cost-benefit analysis

35. In case of due diligence, a lighter touch approach on the ICT intragroup service providers is justified because group entities are known by the financial entities and covered by the internal control system. This is achieved by a proportionate application of the due diligence requirements as foreseen under Article 7 of the draft RTS with regard to ICT intragroup service providers combined with Article 1 on the criteria listed for the application of the proportionality principle.

Preferred option

36. Option B has been retained.

POLICY ISSUE 5: LEVEL OF ASSURANCE IN DUE DILIGENCE PROCESS

Options considered

37. Option A: Use all sources available to assess the ICT third-party service provider

38. Option B: Use only sources that are independent from the ICT third-party service provider

Cost-benefit analysis

39. The policy on due diligence should specify a certain level of assurance concerning the ICT third-party service providers' business reputation, reliability and risk management framework. To ensure that the required level of assurance is reached, the financial entity should use at least one source of information that is independent from the service provider to ensure objectivity and reliability. If the assurance provided is not sufficient or not sufficiently independent, the financial entity should conduct audits itself or entrust external auditors with those tasks on its behalf.

40. Reliance on sources provided by the ICT third-party service provider only would not allow the establishing of a sufficient level of assurance, due to potential lack of independence of the assessments.

Preferred option

41. Option B has been retained.

POLICY ISSUE 6: SOURCES OF CONFLICT OF INTEREST

Options considered

42. Option A: Identify specific sources of conflict of interest (CoI) and management requirements.

43. Option B: Do not identify specific sources of conflict of interest as these are sufficiently covered under Regulation (EU) 2022/2554 itself.

Cost-benefit analysis

44. Given that providing requirements on conflict of interest is not explicitly part of the mandate (policy on contractual arrangements) the policy only refers to management and mitigation of COI. However, it is important that financial entities identify all COIs (Article 28 (4) (e) of Regulation (EU) 2022/2554).

Preferred option

45. Option B has been retained.

POLICY ISSUE 7: CONTRACTUAL CLAUSES

Options considered

46. Option A: Include in the policy the stipulation of specific contractual clauses specified in Regulation (EU) 2022/2554 to be included in contractual arrangements.

47. Option B: Do not include in the policy the stipulation of specific contractual clauses specified in Regulation (EU) 2022/2554 to be included in contractual arrangements.

Cost-benefit analysis

48. The clarification of supervisory expectations regarding the content of the policy on ICT third party arrangements benefits the financial entities during the negotiations of contractual conditions and practical deliveries and creates a level playing field.

49. Clear contractual requirements, including requirements to assure access and audit rights, lead to minor one-off costs and reduce the ongoing costs for negotiating arrangements with ICT third-party service providers, as they establish a non-debatable set of contractual conditions to be agreed on. The policy shall specify that those contractual clauses shall always be in the contract and effective otherwise financial entities cannot use ICT third-party service providers.

Preferred option

50. Option A has been retained.

POLICY ISSUE 8: MONITORING OF THE CONTRACTUAL ARRANGEMENTS FOR THE USE OF ICT SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS

Options considered

51. Option A: Require the monitoring of the application of the contractual arrangements

52. Options B: Do not require the monitoring of the application of the contractual arrangements

Cost-benefit analysis

53. Continuous monitoring of service delivery is necessary, as provision of the services in the agreed way in accordance with contractual arrangements ensures compliance of the financial entity with applicable supervisory and regulatory requirements, including with requirements on incident reporting.

Preferred option

54. Option A has been retained.

Overall Cost-Benefit Analysis

55. This section assesses the overall costs and benefits of the RTS.

56. The draft RTS impose a limited set of specific requirements on financial entities which mainly were already known under the existing framework and had been specified in Guidelines (e.g. on outsourcing) and to some of the financial entities covered by DORA and specifies the requirements on the content of the policy regarding the use of ICT services supporting critical or important functions required under DORA.

57. The provided specifications will lead to more harmonised practices regarding the use of ICT third party services providers when providing ICT services supporting critical or important functions. The RTS will benefits financial entities by creating a higher level of transparency regarding regulatory requirements and supervisory expectations.

58. Standardised requirements and harmonisation for the setting of policies lead to a reduction of costs for implementing processes. Harmonisation should also increase the efficiency of supervision and comparability across financial entities and across Member States.

59. The draft RTS aim to ensure financial entities have an exhaustive policy on the use of ICT service providers supporting critical and important function that covers all the steps of the life cycle of such ITC third party arrangements. This will facilitate the management of related risks, by ensuring that

appropriate risk management measures and ICT management measures are applied throughout the lifecycle of such arrangements.

60. The content of the policy regarding the risk assessment and due diligence of ICT third party arrangements needs to include a more thorough assessment of the ICT risks. However, costs should be limited as the content of the policy focuses only on ICT services provided by third parties that are supporting critical or important functions. The costs of implementing such assessments are expected to be limited, because these policies should in principle be already in place at least partly and part of the financial entities should already be familiar with them.

61. The RTS will trigger some costs for financial entities for updating and implementing updated policies, which will differ depending on their nature considering that some sectoral legislation already establishes a set of requirements for outsourcing that is quite detailed, the additional costs should be very low for part of them. For some others that were not familiar with those requirements the entry cost will be slightly more costly to comply with DORA requirements, On the other hand, standardised requirements towards third party service providers will strengthen the negotiation position of financial entities when negotiating contracts with ICT service providers.

62. The overall impact is considered low, as financial entities must already have documentation in place regarding their organisational structure, which includes outsourcing or other third-party arrangements.

63. Given the existing procedures and the consistency with the other legislation that is already in place applicable to some financial entities, the cost for applying new, binding and more harmonised procedures in the area of financial activities should be low in general and are mainly caused by the underlying Regulation rather than the technical specifications provided in the RTS.

64. POLICY ISSUE 9: PROPORTIONALITY PRINCIPLE

Options considered

65. Option A: Introduce a principle-based proportionality article applicable horizontally to all financial entities under the scope of DORA

66. Options B: Identify specific requirements, e.g. frequency of the review or the details of the content of the different parts of the policy that could be applied in a proportionate manner, due diligence requirements when the ICT third party provider is part of a group.

Cost-benefit analysis

Option A and partly B was considered. DORA already sets out a general requirement on the proportionate application of its requirements, The draft RTS further specify some of the criteria for the application of the proportionality principle that can be considered by financial entities and competent

authorities when doing the proportionality assessment. In addition, the Level 1 already foresees some exemptions for small entities. Some proportionality was also explicitly introduced regarding the due diligence to be performed when the ICT third party provider is part of a group.

6. Overview of the questions for consultation

Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?

Question 2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?

Question 3: Is article 4 appropriate and sufficiently clear?

Question 4: Is article 5 appropriate and sufficiently clear?

Question 5: Are articles 6 and 7 appropriate and sufficiently clear?

Question 6: Is article 8 appropriate and sufficiently clear?

Question 7: Is article 9 appropriate and sufficiently clear?

Question 8: Is article 10 appropriate and sufficiently clear?

Question 9: Is article 11 appropriate and sufficiently clear?