JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2023 67

27 November 2023

Consultation Paper

on Draft Regulatory Technical Standards

to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of 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 Annex 2. Comments are most helpful if they:

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

Submission of responses

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

All contributions should be submitted online at www.esma.europa.eu under the heading 'Your input - Consultations'. 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

Information on data protection can be found at www.esma.europa.eu under the heading 'Data protection'.

2. Executive Summary

Article 30(2)(a) of Regulation (EU) 2022/2554 requires financial entities to include in contractual arrangements on the use of ICT services a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting critical or important functions, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting. The ESAs are mandated to develop jointly draft regulatory technical standards to further specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.

In accordance with Regulation (EU) 2022/2554, this draft RTS sets out requirements when the use of subcontracted ICT services supporting critical or important functions or material parts thereof by ICT third-party service providers is permitted by financial entities and set out the conditions applying to such subcontracting. In particular, the draft RTS requires financial entities to assess the risks associated with subcontracting during the precontractual phase; this includes the due diligence process. The draft RTS sets out also requirements regarding the implementation, monitoring and management of contractual arrangement regarding the subcontracting conditions for the use of ICT services supporting critical or important functions or material parts thereof ensuring that financial entities are able to monitor the entire ICT subcontracting chain.

Next steps

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

3. Background and rationale

1. Article 30(2) a) of DORA requires from financial entities that: " the contractual arrangements on the use of ICT services shall include at least the following elements […] a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting".

2. In accordance with Article 30(5) of DORA, "the ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions".

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. When developing these 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, this draft RTS sets out requirements for financial entities when the use of subcontracted ICT services supporting critical or important functions by ICT third-party service providers is permitted, and the applicable conditions to such subcontracting ensuring that financial entities are able to assess the associated risks along the entire ICT subcontracting chain[1] and the compliance with their own legislative and regulatory obligations.

6. ICT intragroup subcontractors, including the ones fully or collectively owned by financial entities within the same institutional protection scheme, providing ICT services supporting critical or important functions should be considered as ICT third-party services providers. Intragroup ICT subcontracting should not be treated differently from subcontracting outside of the group. The risks posed by those ICT intragroup subcontractors may be different but the requirements applicable to them are the same in accordance with Regulation (EU) 2022/2054. When the use of ICT subcontractors is permitted, then those also include ICT intragroup subcontractors.

7. The draft RTS further specifies 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, when permitted, subcontracting for the use of ICT services

[1] Comparable terms include 'ICT supply chain' as found in the G7 Fundamental Elements for third party cyber risk in the financial sector (October 2022) and in the FSB consultation document on "A toolkit for financial authorities and financial institutions as well as service providers for their third-party risk management and oversight" (June 2023). As the level 1 mandate specifically refers to subcontracting, the term 'ICT subcontracting chain' is used throughout this document.

supporting critical or important functions or material parts thereof as referred to in Article 30(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, in order to ensure a group-wide management of ICT third-party risks where applicable.

8. The use of ICT subcontractors by ICT third-party service providers for the use of ICT services supporting critical or important functions or material parts thereof cannot reduce the responsibility for the financial entities and their management bodies to manage their risks and to comply with legislative requirements.

9. To ensure financial entities' sound governance arrangements including risk management and internal controls with regard to the use of ICT subcontractors by ICT third-party service providers, the draft RTS covers the whole life cycle of contractual arrangements with the ICT third-party service providers. It starts with the planning phase of the use of subcontracted ICT services, including risk assessments and due diligence processes, then covers the ongoing service delivery, monitoring and auditing, and ends with the exit from such arrangements.

10. To ensure that the subcontracted ICT services supporting critical or important functions or material parts thereof are provided with the necessary level of quality, financial entities shall assess that the ICT third-party service provider and where appropriate the ICT subcontractors have sufficient resources, including expertise and adequate financial, human and technical resources, ICT security arrangements, an appropriate organisational structure, including risk management and internal controls to effectively monitor the subcontracted ICT services supporting critical or important functions and that the ICT third-party service provider is able to comply with the contractual requirements.

11. The draft RTS shall be read together with Regulation (EU) 2022/2554 which defines ICT services and a critical or important function and includes provisions on mandatory contractual arrangements with ICT third-party service providers including for the use of subcontracting. While these RTS set out requirements regarding subcontracting by ICT third-party service providers for the use of ICT services supporting critical or important functions or material parts thereof, Regulation (EU) 2022/2554 also sets out risk management requirements for the use of ICT third-party services providers including subcontractors providing ICT services supporting functions that are not considered critical or important. The draft RTS shall also be read in conjunction with other draft RTS mandated by DORA, particularly on the 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, on the register of ICT services provided and on ICT risk management.

4. Draft regulatory technical standards

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

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 to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554

(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 30(5) thereof,

Whereas:

(1) Article 30(2) of Regulation (EU) 2022/2554 requires from financial entities to set out contractual arrangements on the use of ICT services that should include at least a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of ICT service supporting critical or important functions, or material parts thereof (hereafter "ICT services supporting critical or important functions) is permitted and, when that is the case, the conditions applying to such subcontracting.

(2) To ensure a consistent and uniform application by financial entities and supervisory convergence across the European Union, it is necessary to further specify the elements set out under Article 30(2) of Regulation (EU) 2022/2554.

(3) The provision of ICT services to financial entities often depends on a complex ICT subcontracting chain whereby ICT third-party service providers may enter into one or more subcontracting arrangements with other ICT third-party service providers. While this indirect reliance on ICT subcontractors may have an impact on financial entities' ability to identify, assess and manage its risks including risks linked to gaps in the information provided by ICT third-party service providers and limited ability to obtain information from these ICT subcontractors, it cannot reduce the responsibilities the financial entities and their management bodies to manage their risks and to comply with the legislative and regulatory requirements.

(4) In this regard, where the provision of ICT services to financial entities depends on a potentially long or complex ICT subcontracting chains whereby several subcontractors may be involved, each providing a part of the ICT service that supports a critical or important function, it is therefore essential that financial entities monitor the entire subcontracting chain of ICT providers to identify and monitor all the subcontractors that effectively provide the ICT service supporting critical or important functions.

(5) When subcontracting ICT services supporting critical or important functions is permitted, it is of utmost importance that financial entities conduct a risk assessment to have a clear and holistic view of the risks associated with subcontracting, and be in a position to properly monitor, manage and mitigate the risks that may affect the provision of the subcontracted ICT services supporting critical or important functions. Financial entities should have appropriate processes in place, directly or indirectly through their ICT third-party service providers, to address the relevant risks that may impact the provision of ICT services supporting critical or important functions, in accordance with their contractual arrangements with ICT third-party service providers.

(6) 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 these regulatory technical standards.

(7) When permitted by the financial entities, the use of subcontracted ICT services supporting critical or important functions by ICT third-party services providers cannot reduce the ultimate responsibility for the financial entities and their management bodies to manage their risks and to comply with their legislative and regulatory obligations.

(8) In order to have a comprehensive management of the risks that could arise when subcontracting ICT services supporting critical or important functions, it is necessary to take into account 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, including for subcontracting arrangements. In this regard, it is necessary to set out requirements for financial entities that should be reflected in their contractual arrangements with ICT third-party service providers when the use of subcontracted ICT services supporting critical or important functions is permitted.

(9) To mitigate the subcontracting risks, it is necessary to specify all the conditions under which ICT third-party service providers can use subcontractors for the provision of ICT services supporting critical or important functions. For this purpose, ICT contractual arrangements between financial entities and ICT third-party service providers should set out the planning of subcontracting arrangements, their risk assessments, their due diligences, and the approval process for new ICT subcontracting arrangements regarding ICT services supporting critical or important functions or material changes to existing ones by the ICT third-party service provider.

(10) In order to identify the risks that could arise before entering into an arrangement with an ICT subcontractor, the ICT third-party service providers should follow an appropriate and proportionate process to select and assess the suitability of prospective subcontractors in line with the ICT contractual arrangements between the financial entity and itself. ICT contractual arrangements between the financial entities and the ICT third-party service

providers should therefore foresee that the latter, or where appropriate or possible, the financial entity directly, assesses at least the subcontractors' business reputation, its resources including expertise and adequate financial, human and technical resources, information security, its organisational structure, including the risk management and internal controls that the subcontractor should have in place.

(11) In order to mitigate the subcontracting risks along the life cycle of contractual arrangements, it is necessary to set out the minimum content of the contractual arrangements between the financial entities and the ICT third-party service providers when using ICT subcontracting for the use of ICT services, in particular with regard to the monitoring of the subcontracting chain and the notification of new subcontracting arrangements or material changes thereof made by the ICT third-party provider and the objection, modification and termination rights of the financial entity.

(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

For the purpose of applying Articles 2 to 7 regarding the contractual arrangements between financial entities and ICT third-party service providers on the use of subcontracted ICT services and the conditions applying to it, the following elements of increased or reduced risk shall be taken into account by financial entities:

a) the location of the ICT subcontractor or its parent company;

b) the number of ICT subcontractors;

c) the nature of data shared with the ICT subcontractors;

d) the location of data processing and storage;

e) whether the ICT subcontractors are part of the same group of the financial entity;

f) the transferability of the ICT service supporting a critical or important functions to another ICT third-party service provider, including as a result of technology specificities;

g) the potential impact of disruptions on the continuity and availability of the ICT services supporting critical or important functions provided by the ICT third-party service provider;

h) the difficulty of reintegrating the ICT service supporting critical or important functions by the ICT third-party service provider;

i) the concentration risks.

Article 2

Group application

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, where permitted, that the conditions for subcontracting the use of ICT services supporting critical or important functions as referred to in Article 30(2) of Regulation (EU) 2022/2554 are implemented consistently in their subsidiaries and are adequate for the effective application of this Regulation at all relevant levels.

Question 1 : Are articles 1 and 2 appropriate and sufficiently clear?

Article 3

Risk assessment regarding the use of subcontractors

1) A financial entity shall decide whether an ICT service supporting critical or important functions may be subcontracted by an ICT third-party service provider only after having assessed at least:

a) that the due diligence processes implemented by the ICT third-party service provider ensure that it is able to select and assess the abilities, both operational and financial, of prospective ICT subcontractors to provide the ICT services supporting critical or important functions, including by participating in operational reporting and operational testing as required by the financial entity;

b) that the ICT third-party service provider will be able to inform and involve the financial entity in the decision-making related to subcontracting when relevant and appropriate;

c) that the relevant clauses of the contractual arrangements between the financial entity and the ICT third-party service provider are replicated as appropriate in the subcontracting arrangements between the ICT third-party service provider and its subcontractor to ensure that the financial entity is able to comply with its own obligations under Regulation (EU) 2022/2554;

d) that, without prejudice to the financial entity's final responsibility to comply with its legal and regulatory obligations, the ICT third-party service provider itself has adequate abilities, expertise, financial, human and technical resources, applies appropriate information security standards, and has an appropriate organisational structure, including risk management and internal controls, incidents reporting and responses, to monitor its subcontractors;

e) that the financial entity has adequate abilities, expertise, financial, human and technical resources, applies appropriate information security standards, and has an appropriate organisational structure, including risk management, incident response and business continuity management and internal controls, to monitor and oversee the ICT service that has been subcontracted or, where possible and appropriate, the subcontractors directly;

f) the impact of a possible failure of a subcontractor on the provision of ICT services supporting critical or important functions on the financial entity's digital operational resilience and financial soundness, including step-in rights;

g) the risks associated with the geographical location of the potential subcontractors in relation to the ICT services supporting critical or important functions provided by the ICT third-party service provider;

h) the ICT concentration risks at entity level in accordance with Article 29 of Regulation (EU) 2022/2554;

i) any obstacles to the exercise of audit, information and access rights by the competent authorities, resolution authorities, the financial entity, including persons appointed by them.

2) Financial entities that use ICT third-party service providers that subcontract ICT services supporting critical or important functions shall periodically carry out the assessment referred to in paragraph 1) against possible changes in their business environment, including but not limited to changes in the supported business functions, in risk assessments including ICT threats, concentration risks and geopolitical risks.

Question 2 : Is article 3 appropriate and sufficiently clear?

Article 4

Description and conditions under which ICT services supporting a critical or important function may be subcontracted

When describing in the written contractual arrangements the ICT services to be provided by an ICT third-party service provider in accordance with Article 30(2)(a) of Regulation (EU) 2022/2554, financial entities shall identify which ICT services support critical or important functions and which of those are eligible for subcontracting and under which conditions. In particular, and without prejudice to the final responsibility of the financial entity, for each ICT service eligible for subcontracting the written contractual agreement shall specify:

a) that the ICT third-party service provider is required to monitor all subcontracted ICT services supporting a critical or important function to ensure that its contractual obligations with the financial entity are continuously met;

b) the monitoring and reporting obligations of the ICT third-party service provider towards the financial entity;

c) that the ICT third-party service provider shall assess all risks, including ICT risks, associated with the location of the potential subcontractor and its parent company and the location where the ICT service is provided from;

d) the location and ownership of data processed or stored by the subcontractor, where relevant;

e) that the ICT third-party service provider is required to specify the monitoring and reporting obligations of the subcontractor towards the ICT third-party service provider, and where relevant, towards the financial entity;

f) that the ICT third-party service provider is required to ensure the continuous provision of the ICT services supporting critical or important functions, even in case of failure by a subcontractor to meet its service levels or any other contractual obligations;

g) the incident response and business continuity plans in accordance with Article 11 of Regulation (EU) 2022/2554 and service levels to be met by the ICT subcontractors;

h) the ICT security standards and any additional security features, where relevant, to be met by the subcontractors in line with the RTS mandated by Article 28(10) of Regulation (EU) 2022/2554;

i) that the subcontractor shall grant to the financial entity and relevant competent and resolution authorities at least the same audit, information and access rights as

granted to the financial entity and relevant competent authorities by the ICT third-party service provider;

j) that the financial entity has termination rights in accordance with article 7, or in case the provision of services fails to meet service levels agreed by the financial entity.;

Question 3 : Is article 4 appropriate and sufficiently clear?

Article 5

Monitoring of the entire ICT subcontracting chain by the financial entity

1) When an ICT service supporting critical or important functions is subcontracted the financial entity shall fully monitor the ICT subcontracting chain and shall document it, including on the basis of the information provided by the ICT third-party service provider, in accordance with Article 28 paragraphs (3) and (9) of Regulation (EU) 2022/2554.

2) The financial entity shall monitor subcontracting conditions, including through the review of contractual documentation between ICT third-party service providers and subcontractors, as appropriate, and key performance indicators to ensure that all the conditions referred to in Article 4 are complied with along the entire ICT subcontracting chain.

Question 4 : Is article 5 appropriate and sufficiently clear?

Article 6

Material changes to subcontracting arrangements

1) In case of any material changes to the subcontracting arrangements, the financial entity shall ensure, through the ICT contractual arrangement with its ICT third-party service provider, that it is informed with a sufficient advance notice period to assess the impact on the risks it is or might be exposed to, in particular where such changes might affect the ability of the ICT third-party service provider to meet its obligations under the contractual agreement, and with regard to changes considering the elements listed in Article 1.

2) The financial entity shall inform the ICT third-party service provider of its risk assessment results as referred to in paragraph 1) by the end of the notice period.

3) The financial entity shall require that the ICT third-party service provider implements the material changes only after the financial entity has either approved or not objected to the changes by the end of the notice period.

4) The financial entity shall have a right to request modifications to the proposed subcontracting changes before their implementation if the risk assessment referred to referred to in paragraph 1) concludes that the planned subcontracting or changes to

subcontracting by the ICT third-party service provider exposes the financial entity to risks as specified in Article 3(1) that exceed its risk appetite.

Article 7

Termination of the contractual arrangement

1) Without prejudice to the termination clauses set out in accordance with Article 28 paragraph (10) of Regulation (EU) 2022/2554, the financial entity has a right to terminate the agreement with the ICT third-party service provider in each of the following cases:

    a. when the ICT third-party service provider implements material changes to subcontracting arrangements despite the objection of the financial entity, or without approval within the notice period as referred to in Article 6,

    b. when the ICT third-party service provider subcontracts an ICT service supporting a critical or important function explicitly not permitted to be subcontracted by the contractual agreement.

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

Article 8

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. Draft cost-benefit analysis / impact assessment

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'.'

This analysis presents the IA of the main policy options included in this Consultation Paper (CP) on regulatory technical standards (RTS) to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Regulation (EU) 2022/2554.

Problem identification

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.

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.

The extensive use of ICT services and their technical and global nature also led to subcontracting of ICT services and an increasingly complex subcontracting chain, which leads to dilution of responsibilities and uncertainty on where the risks lie.

In the absence of clear and bespoke standards at EU level applying to subcontracting of ICT services supporting critical or important functions by third-party service providers, the external factors of ICT risks have not been comprehensively addressed. Consequently, it is necessary to set out certain

elements to be determined and assessed to guide financial entities' management of ICT third-party risk including subcontracting, which are of particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions and which may subcontract some of these ICT services supporting critical or important functions to other third parties.

In this context, as part of the the contractual arrangements on the use of ICT services supporting critical or important functions between financial entities and ICT third-party service providers, the ESAs have been mandated under Article 30 (5) of the Regulation (EU) 2022/2554 to develop draft regulatory standards to specify elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.

Policy objectives

The draft regulatory technical standards specifying the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions aims to establish a common framework across the Member States of the EU for assessing whether a ICT service supporting critical or important function can be subcontracted and what would be the conditions for subcontracting. The objective of this framework is to enable financial entities in accordance with their final responsibilities to comply with the regulatory obligations, to manage and monitor their third-party risk with regard to ICT services supporting critical or important functions provided by ICT third-party service providers including the entire subcontracting chain of ICT services supporting critical or important functions in line with DORA and, in this regard, to ensure a level playing field.

Baseline scenario

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.

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.

The following aspects have been considered when developing the RTS.

Policy issue 1: Monitoring the chain of subcontracting

Options considered.

Option A: monitoring the associated ICT risks along the entire ICT subcontracting chain for the use of ICT services supporting critical or important functions.

Option B: monitoring the associated ICT risks over a limited number of ICT subcontractors along chain for the use of ICT services supporting critical or important functions

Option C: delegating the monitoring of the associated ICT risks of the ICT subcontracting chain to the ICT third party providers.

The use of ICT subcontractors by ICT third-party service providers for the use of ICT services supporting critical or important functions or material parts should not reduce the responsibility for the financial entities and their management bodies to manage their risks and to comply with legislative requirements. As a result, the only way to ensure this is by ensuring that the financial entities are ultimately responsible to assess the risks associated with the entire ICT subcontracting chain, and the compliance with their own legislative and regulatory obligations. In addition it is worth mentioning that it is envisaged to capture subcontractors for the use of ICT services supporting critical or important functions only. (Option A).

The monitoring of only a few subcontractors for the use of ICT services supporting critical or important functions (Option B) may lead to increased risks along the chain because the DORA framework focuses on the use of ICT services supporting critical or important functions. It may also lead to dilution of responsibilities as the financial entities who are ultimately srepsonsible fo the compliance with legislative obligations and have they main interest in ensuring that the subcontractors are in lign with these oblgations. and ultimately the risk of non-compliance with the legislation.

Delegation of the monitoring ot the ICT service third party providers (Option C)is not in line with the DORA framework.

Preferred Option. Option A has been retained.

POLICY ISSUE 2: Application of proprtionnality

Options considered.

Option A: No need to have an article on the application of the proportionality principle

Option B: Specifying further the elements of reduced or increased of risk to be considered for the application of the proportionality principle

The application of proportionality is explicitly mentioned under Article 4 of DORA and as a consequence there is no need to further specify the criteria to consider for the application of propritionality (Option A).

Although the principle is mentioned under Article 4 of DORA, the criteria mentioned under this Article are quite broad. 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 these regulatory technical standard. For the purpose of the application of this RTS , it is therefore important to further specify a non exhaustive list of criteria or elements of risks that can be considered by financial entities and help them in the implementation of the requirements envisaged by the RTS.

Preferred Option. Option B has been retained.

POLICY ISSUE 3: Definition of of ICT services and critical and important functions

Options considered

Option A: relying on the definitions provided under DORA but providing more detailed criteria regarding the notion of “critical and important functions” and “ICT services”

Option B: Referring to definitions of DORA only as the draft RTS is about the use of subcontracting for the use of ICT services supporting critical or important functions and the conditions for the use of subcontracting.

Specifications to the definitions would lead to a higher level of harmonization. However, a too specific definitions 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 definitions within DORA, without the provision of detailed specifications seems to be more appropriate. The analysis should be made by financial entities in line with their risk assessment and on a case by case basis taking into account of the DORA definitions.

Preferred option.Option B has been retained

Overall Cost-Benefit Analysis

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

The draft RTS imposes 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 specifies the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.

The draft RTS aim to ensure financial entities have an exhaustive approach to the use of subcontracting of ICT service providers supporting critical and important function or material parts thereof that covers all the steps of the life cycle of such ITC third party contractual arrangements. It also ensures that financial entities are able to assess the associated risks along the entire ICT subcontracting chain and the compliance with their own legislative and regulatory obligations.

In addition, the provided specifications will lead to more harmonised practices regarding the use of subcontracting when providing ICT services supporting critical or important functions. The RTS will benefit financial entities by creating a higher level of transparency regarding regulatory requirements and supervisory expectations, and facilitate the compliance with the legislative requirements throughout the chain of subcontracting.

Standardised requirements and harmonisation of the elements to determine and assess when subcontracting ICT services supporting critical or important functions leads 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.

The RTS will trigger some costs for financial entities related to the monitoring of the chain of subcontracting, which will differ depending on their business model and the complexity of the subcontracting chain. For certain financial entities (e.g. credit institutions), sectoral legislation already establishes a set of requirements for outsourcing that is quite detailed, so the additional costs should be very low. On the other hand, standardised requirements towards ICT third party service providers will strengthen the negotiation position of financial entities when negotiating contracts with ICT third party service providers.

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

Given the existing procedures and the consistency with the other legislation that is already in place, 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.

6. Overview of the questions for consultation

Question 1 : Are articles 1 and 2 appropriate and sufficiently clear?

Question 2 : Is article 3 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?