JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 53

26 July 2024

Final report

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

1. Table of Contents

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 of ICT services supporting critical or important functions.

Next steps

The ESAs will submit the draft RTS 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 chain of ICT subcontractors[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.

[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.

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 subcontracting for the use of ICT services 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 draft 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 to provide ICT services supporting critical or important functions 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 before entering into an arrangement , 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 chain of ICT subcontractors 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 their risks, including risks linked to gaps in the information provided by ICT third-party service providers and to the financial entities' limited ability to obtain information from ICT subcontractors providing ICT services supporting critical or important functions or material parts thereof, it cannot reduce the responsibilities the financial entities and their management bodies to manage their risks and to comply with their legislative and regulatory requirements.

(4) In this regard, where the provision of ICT services to financial entities depends on potentially long or complex chain of ICT subcontractors whereby several subcontractors may be involved, it is essential that financial entities identify the overall chain of subcontractors providing ICT services supporting critical or important functions.

(5) According to Article 28(1) of Regulation (EU) 2022/2554 financial entities shall, on a continuous basis, identify all sources of ICT risk. In order to do so, when receiving ICT services supporting critical or important functions, financial entities should continue to effectively monitor those ICT services.

(6) Among those subcontractors that provide ICT services supporting critical or important functions, financial entities should put a particular and continuous focus on the subcontractors that effectively underpin the ICT service supporting critical or important functions, including all the subcontractors providing ICT services whose disruption would impair the security or the continuity of the service provision in accordance with Article 3 (1) (b) of the Implementing Technical Standards with regard to standard templates for the register of information.

(7) 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 elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions and to ensure that those requirements are applied in a manner that is proportionate.

(8) When permitted by the financial entities in accordance with Article 30(2) of Regulation (EU) 2022/2554, 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 .

(9) When subcontracting ICT services supporting critical or important functions is permitted, it is of utmost importance that financial entities conduct a risk assessment before entering into an arrangement with ICT third-party service providers 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.

(10) Taking into account the application of the proportionality principle and a risk-based approach, 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. Financial entities should identify the most appropriate way to perform the due diligence on the subcontractors and risk assessment directly by themselves or indirectly through their ICT third-party service providers, considering the specificities of the contractual arrangements and having regard of their final responsibility stemming from Regulation (EU) 2022/2554.

(11) ICT intra-group subcontractors providing ICT services supporting critical or important functions or material parts thereof, including those fully or collectively owned by financial entities within the same institutional protection scheme, where applicable, should be considered as ICT subcontractors. In accordance with Regulation (EU) 2022/2554, the requirements applicable for the use of intra-group subcontracting are the same as those applicable to non-intra-group subcontracting, regardless of the differences that may exist in the risks posed in both cases.

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

(13) 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 of a contractual arrangement 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.

(14) 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 such conditions, including the planning of subcontracting arrangements, the risk assessments, the due diligence, and the approval process for new ICT subcontracting arrangements on ICT services supporting critical or important functions or material parts thereof, or material changes to existing ones made by the ICT third-party service provider.

(15) 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 potential subcontractors in line with the ICT contractual arrangements concluded with the financial entity. The ICT contractual arrangements should therefore foresee that the ICT third-party service provider, or where appropriate, the financial entity directly, assesses 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.

(16) 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.

(17) Financial entities should monitor the performance of the ICT service provision and any relevant changes occurring within their subcontracting chain providing ICT services supporting critical or important function to mitigate any vulnerabilities and threats that may pose risks to their ICT systems and operations.

(18) Financial entities should be informed of new subcontracting arrangements or material changes thereof made by the ICT third-party provider with a notice period that allows them to assess the risks associated with such new arrangements or material changes. Where the outcome of the risk assessment is that the new arrangements or material changes carry a level of risk that exceed their risk tolerance, financial entities should have the right to terminate the contract with the ICT third-party service provider. The financial entity's objections may be addressed by the ICT third-party service provider before the financial entity exercises its termination right.

(19) The European Supervisory Authorities have conducted an open public consultation 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

Overall risk profile and complexity

For the application of this Regulation, financial entities shall take into account the size and the overall risk profile of the financial entity and the nature, scale and elements of increased or reduced complexity of its services, activities and operations, including elements relating to:

a) the type of ICT services supporting critical or important functions covered by the contractual arrangements between the financial entity and the ICT third-party service providers and the type of ICT services covered by the contractual arrangement between the ICT-third party service provider and its subcontractors;

b) the location of the ICT subcontractor providing ICT services supporting critical or important functions or material part thereof or its parent company;

c) the length of the chain of subcontractors providing ICT services supporting critical or important functions or material parts thereof used by the ICT third-party service providers;

d) the nature of data shared with the ICT subcontractors providing ICT services supporting critical or important functions or material parts thereof;

e) whether the provision of ICT services supporting critical or important functions or material parts thereof by the subcontractors is located within a Member State or in a third country, also considering the location where the ICT services are actually provided from and the location where the data is actually processed and stored;

f) whether the ICT subcontractors providing ICT services supporting critical or important functions or material parts thereof are part of the same group as the financial entity to which the services are provided;

g) the use of ICT subcontractors providing ICT services supporting critical or important functions or material parts thereof that are authorised, registered or subject to supervision or oversight 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 and those that are not;

h) the use of ICT third-party service providers that are authorised, registered or subject to supervision or oversight by a supervisory authority from a third country and are subject to supervision or oversight and those that are not;

i) whether the provision of ICT services supporting critical or important functions or material parts thereof is concentrated to a single subonctractor of an ICT third-party service provider or a small number of such subcontractors;

j) the impact of subcontracting of ICT services supporting critical or important functions or material parts on the transferability of the ICT service supporting a critical or important functions to another ICT third-party service provider;

k) 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 when using a subcontractor providing ICT services supporting critical or important functions or material parts thereof.

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

Article 3

Due diligence and risk assessment regarding the use of subcontractors supporting critical or important functions

1) A financial entity shall decide before entering into an arrangement with an ICT third party service provider whether an ICT service supporting critical or important functions or material parts thereof 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 operational and financial abilities of

potential ICT subcontractors to provide the ICT services supporting critical or important functions or material parts thereof, including by participating in digital operational resilience testing as referred to Chapter IV of Regulation (EU) 2022/2554 as required by the financial entity;

b) that the ICT third-party service provider is able to identify, notify and inform the financial entity of any subcontractors in the chain of subcontracting providing ICT services supporting critical or important functions or material parts thereof, and to provide all relevant information that may be necessary for the assessment;

c) that the ICT third-party service provider ensures that the contractual arrangements with the subcontractors providing ICT services supporting critical or important functions or material parts thereof allow the financial entity to comply with its own obligations stemming from Regulation (EU) 2022/2554 and all other applicable legal and regulatory requirements, and grant the financial entity and competent and resolution authorities the same contractual rights of access, inspection and audit along the chain of subcontractors providing ICT services supporting critical or important functions as those granted by the ICT third-party service provider ;

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 supporting critical or important functions or material parts thereof that has been subcontracted or, including where possible and appropriate, the subcontractors effectively underpinning the ICT service supporting critical or important functions or material part thereof directly as set out under Article 5;

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;

g) the risks associated with the 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, inspection 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 or material parts thereof shall periodically carry out the risk 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, ICT concentration risks and geopolitical risks.

3) In accordance with their final responsibility to comply with their legal and regulatory obligations under Regulation (EU) 2022/2554, financial entities making use of the results of the risk assessment carried out by their ICT third-party service providers on their subcontractors, for the purpose of complying with the obligations set out in this article, shall not rely exclusively on them in accordance with Article 5 (4).

Article 4

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

1) 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 supporting critical or important functions are eligible for subcontracting and under which conditions. In particular, and without prejudice to the financial entities' final responsibilities stemming from Regulation 2022/2554, for each ICT service supporting a critical or important function or material parts thereof eligible for subcontracting, the written contractual agreement between the financial entity and the third-party service provider shall specify:

a) that the ICT third-party service provider is responsible for the provision of the services provided by the subcontractors;

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

c) the monitoring and reporting obligations of the ICT third-party service provider towards the financial entity regarding subcontractors of ICT third-party service

providers providing ICT services supporting critical or important functions or material part thereof;

d) that the ICT third-party service provider shall assess all risks associated with the location of the current or potential subcontractors providing ICT service supporting a critical or important function or material part thereof, and its parent company and the location where the ICT service is provided from;

e) the location of data processed or stored by the subcontractor, where relevant;

f) that the ICT third-party service provider is required to specify in its written contractual agreement with the subcontractor providing ICT services supporting critical or important function or material part thereof the monitoring and reporting obligations of the subcontractor towards the ICT third-party service provider, and where agreed, towards the financial entity;

g) that the ICT third-party service provider is required to ensure the continuity of the ICT services supporting critical or important functions throughout the chain of subcontractors in case of failure by an ICT subcontractor to meet its contractual obligations, and that the written contractual agreement with the subcontractor providing the ICT services supporting critical or important functions or material parts thereof includes the requirements on business contingency plans as set out under Article 30(3)(c) of Regulation (EU) 2022/2554 and defines the service levels to be met by the ICT subcontractors in relation to these plans;

h) that the ICT third-party service provider is required to specify in its written contractual agreement with the subcontractor providing ICT services supporting critical or important functions or material parts thereof the ICT security standards and any additional security requirements, where relevant, that shall be met by the subcontractors in line with Article 30(3)(c) of Regulation (EU) 2022/2554;

i) that the subcontractor is required to grant to the financial entity and relevant competent and resolution authorities the same rights of access, inspection and audit as referred to in Article 30(3)(e) of Regulation (EU) 2022/2554 as granted to the financial entity and relevant competent and resolution authorities by the ICT third-party service provider;

j) that the financial entity will be notified of material changes to subcontracting arrangements in accordance with article 6;

k) that the financial entity has termination rights in accordance with article 7 or in accordance with the circumstances set out under Article 28(7) of Regulation (EU) 2022/2554.

2) Changes relative to contractual agreements between the financial entity and ICT third-party service providers that provide an ICT service supporting critical or important functions or material parts thereof, made necessary to comply with this Regulation, shall be implemented in a timely manner and as soon as it is possible. The financial entity shall document the planned timeline for the implementation.

Article 5

Conditions for subcontracting relating to the chain of ICT subcontractors providing a service supporting a critical or important function by the financial entity

1) When permitting sub-contracting ICT services supporting a critical or important functions, the written contractual agreement between the financial entity and the third-party service provider shall provide all the following elements:

   a. that the chain of ICT subcontractors providing ICT services supporting critical or important functions shall be identified in accordance with Article 3(1)(b);

   b. that the identification of the chain remains up-to-date over time in order to allow for the financial entity to discharge its obligation to maintain and update the register of information in accordance with Article 28(3) and (9) of Regulation (EU) 2022/2554.

2) To maintain the financial entity's overall responsibility for the ICT services supporting critical or important functions provided by ICT third-party service providers, including ensuring effective monitoring, the written contractual agreement between the financial entity and the ICT third-party service provider shall enable the financial entity's effective monitoring of the contracted ICT services in accordance with Article 30(3) point (a) of Regulation (EU) 2022/2554.

   The contractual arrangements shall in particular include elements enabling the financial entity to fulfil its obligation to monitor the ICT risk that may arise in relation to its use of ICT services provided by subcontractors providing ICT services supporting critical or important functions, in particular those that effectively underpin the provision of ICT services supporting critical or important functions or material parts thereof.

   The monitoring referred to in the second subparagraph may, where appropriate, rely on information provided by the ICT third-party service provider.

3) The contractual arrangements shall, in compliance with Article 4 of this Regulation, include elements enabling the financial entity to assess whether and how the potentially long or complex chain of subcontractors that provide ICT services supporting critical or important functions or material parts thereof may impact their ability to fully monitor

the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.

4) The contractual arrangements shall include elements allowing the financial entity to obtain information from the ICT third-party service provider on contractual documentation between the ICT third-party service providers and its subcontractors providing ICT services supporting critical or important functions, and on relevant performance indicators, considering the provisions of Article 30 paragraphs 3 letter (e) of Regulation (EU) 2022/2554, and of Article 8 paragraph 2 of 2 of the Commission Delegated Regulation (EU) 2024/1773.

Article 6

Material changes to subcontracting arrangements of ICT service supporting critical or important functions

1) In case of any material changes to the subcontracting arrangements regarding ICT services supporting critical or important functions or material parts thereof, the financial entity shall ensure, through the ICT contractual arrangement with its ICT third-party service provider, that it is informed with a notice period sufficient to assess the impact on the risks it is or might be exposed to, as well as whether such changes might affect the ability of the ICT third-party service provider to meet its obligations under the contractual agreement as referred to under Article 4, and with regard to changes considering the elements of increased or reduced complexity listed in Article 1.

2) 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.

3) If the risk assessment referred to in paragraph 1) finds that the planned subcontracting or changes to subcontracting by the ICT third-party service provider exceeds the financial entity's risk tolerance, the financial entity shall, before the end of the notice period:

   a) inform the ICT third-party service provider of its risk assessment results as referred to in paragraph 1), and,

   b) object to the changes and request modifications to the proposed subcontracting changes before their implementation.

Article 7

Termination of the contractual arrangement

1) Without prejudice to Article 28 paragraph (7) 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 regarding the provision of ICT services supporting critical or imporant functions despite the objection and request for modifications to the changes by the financial entity referred to in Article 6;

    b) when the ICT third-party service provider implements material changes to subcontracting arrangements supporting critical or important functions before the end of the notice period without explicit approval by the financial entity, as referred to in Article 6;

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

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 has become 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 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 an ICT service supporting critical or important function can be subcontracted and what would be the conditions for such 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 proper and sound management of risks by financial entities, and increase the level of digital operational resilience in the financial sector and ensure level playing field across the EU.

Baseline scenario

From the date of application 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 draft 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 and focusing the monitoring on subcontractors that effectively underpin the provision of service 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: Relying wholly on the direct ICT third party providers for the monitoring of the associated ICT risks of the ICT subcontracting chain.

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 this requirement captures subcontractors for the use of ICT services supporting critical or important functions only, in accordance with the level 1 mandate of this Regulation, and that a particular focus is to be put on subcontractors that effectively underpin the provision of the service. (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 it is the financial entities which are ultimately responsible for the compliance with legislative and regulatory obligations and have the main interest in ensuring that the subcontractors are in line with these obligations when providing ICT services supporting critical or important functions, and ultimately bear the risk of non-compliance with the legislation. Finally this option would not be fully in line with the requirements under DORA.

Wholly in relying on the monitoring of associated risks on 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 proportionnality

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 draft regulatory technical standards. 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, too specific definitions would create the risk of leaving 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 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 were mainly already known under the existing framework and had been specified in ESAs' 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 functions or material parts thereof that covers all the steps of the life cycle of such ICT 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.

Standardising requirements and harmonising 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 contractual 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 limited, 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

The consulation ran from 8th December 2023 to 4th March 2024. 116 responses were received.

The comments received focused on the following main areas:

Proportionality

Respondents suggested that a more proportionate approach should be taken regarding the requirements on subcontracting as they would be too burdensome when applied to the full chain of ICT service provision.

Monitoring of the subcontracting chain

Respondents suggested that the responsibility to monitor the ICT subcontractors should be the responsibility of the ICT third-party service provider and so should not be passed to the financial entity, although the financial entity should wish to assure itself that the ICT third party service provider is monitoring and exercising appropriate oversight over the subcontractor.

Imposing requirements on ICT TPSPs

The RTS should impose specific requirements on ICT third-party service providers, including: a responsibility of the third-party service provider for the provision of information to the financial entity, and requirements on audit and access rights. Respondents were concerned that too many rights for the financial directly would make it difficult to enter into subcontracting arrangements.

Termination

The RTS should ensure balance between contractual freedom and FE's statutory right to terminate the contract with the TPSP in specific circumstances under material changes on subcontracting arrangements.

Transtion period

Respondents suggested that ESAs should consider flexibility to enable market participants sufficient time to comply with the final requirements.

Summary of responses to questions in Consultation Paper ESA/CP/2024/xx and joint ESAs analysis

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
General comments and Q6: Do you have any further comment you would like to share?			
Proportionality and complexity	Several respondents noted that the draft RTS lacks a proportionate and risk-based approach. Proposed amendment suggests introducing a materiality threshold for applying the RTS requirements, including for identifying and monitoring subcontractor risks based on potential impact on service provision. In addition, several respondents requested further guidance explaining the expectations for smaller entities and the role of innovative financial services within this regulatory framework would improve the general approach, making it more balanced and pragmatic.	In accordance with DORA, financial entities remain fully responsible for complying with all of their regulatory obligations, including the ability to oversee the use of ICT third party service providers and subcontractors for the use of ICT services supporting critical or important functions. In this respect, the focus should be on the use of subcontractors for ICT service supporting critical or important functions or material part parts thereof. This is independent of the rank of subcontractors. In this respect, financial entities have to monitor all their subcontractors used for the provisions of ICT services supporting critical or important functions or material part thereof. The draft has been clarified. DORA foresees specific exemptions for microenterprises. In addition, the proportionality principle foreseen in Article 4 of DORA applies to this draft RTS together with Article 1 of this draft RTS. In this regard the RTS specify further the criteria that can be taken into consideration by financial entities for the application of the requirements under the RTS in a proportionate way. These criteria are not exhaustive and financial entities can also develop their criteria; however, they should be able to demonstrate to their CAs that they are relevant. It should be stressed that proportionality does mean waiving the requirements. The article has been clarified.	The RTS has been clarified The RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Risk based approach	Several respondents considered that a risk-based should be introduced which will be more practical for both financial entities to implement and supervisors to enforce, based on a less rigid interpretation of the level 1.	In accordance with the mandate under Article 30 (5) of DORA, the draft RTS focuses on subcontracting of ICT services supporting critical or important functions. Article 3 set requirements on ex ante risk assessment and the identification of subcontracting of ICT services supporting critical or important function. Once the identification done, financial entities can focus on the subcontractors providing ICT services supporting critical or important functions or effectively underpinning critical or important functions. This article introduces actually a risk-based approach.	The RTS has been clarified
Consistency of wording	Several respondents suggested to use the level 1 terms to avoid misunderstandings in particular intragroup provider instead of "part of the same group of the financial entity)"	The comment has been accommodated	The RTS has been clarified
Consistency with other regulatory products	Some respondents are concerned on potential overlap with the ESAs Outsourcing Guidelines, which will remain in place in addition to the DORA RTS. They believe that the ESA outsourcing guidelines should be reconsidered in light of what is detailed in the RTS to ensure there will be no duplication of inconsistency of approaches. Misinterpretation on which rules to apply when the service is qualified should be avoided. For instance, if the ICT Supplier provides a critical function on cloud, the financial entity will need to implement the requirements of the ICT Policy according to DORA and the ones related of the cloud outsourcing. We believe an alignment between both would be recommendable where the Cloud outsourcing guidelines could be adapted to reflect the precedence of the DORA requirements.	The RTS is aligned with DORA and is consistent with the ESAs guidelines on outsourcing that apply to all areas and not only ICT. In any case DORA supersedes ESAs guidelines with regard to ICT areas and stakeholders should focus on DORA directly binding requirements. EBA already communicated that the EBA guidelines on outsourcing will be updated to take into account DORA and a more general approach on third party risk.	No change
Scope	A majority of respondents request making explicit in the draft RTS that the requirements apply only to the subcontracting of services 'supporting critical or important functions or material parts thereof'. Extending the application of the	In accordance with the mandate under Article 30 (5) of DORA, the draft RTS focuses on subcontracting of ICT	The RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	full set of requirements to all subcontractors appears both impractical and misaligned with the risk-based approach adopted by DORA and international best practices. Some respondents considered that while significant ICT risks may raise from any of part of the subcontracting chain, the financial entity should be responsible to perform a thorough risk assessment on the entire subcontracting chain. However, extending all the requirements set forth by the RTS to all subcontractors would be inappropriate and misaligned with the FSB's international standards and even with DORA.	services supporting critical or important functions. The draft RTS has been clarified. See comment above.	
Obligations on ICT third-party service providers	According to several respondents, the draft RTS should provide for specific obligation on ICT third-party service providers.	The draft RTS is addressed to financial entities in accordance with the scope of application of DORA and therefore the RTS cannot impose direct obligations on ICT third-party providers.	No change.
Contractual arrangements	Several respondents considered that the requirements which insert FEs directly into the relationship between a TPSP and their subcontractor; involving the FE in the legal agreement between the TPSP and the subcontractor; or requiring direct oversight of a subcontractor by an FE undermine this process and introduce complexity, risk and ambiguity as to how the process should be managed for all parties. It is also likely to undermine the legal protections which FEs benefit from under the existing approach.	The draft is addressed to financial entities in accordance with scope of application of DORA. Being the one finally responsible for complying with their regulatory obligations, DORA set out requirements on how financial entities have to indicate whether subcontracting of an ICT service support a critical or important function or material part thereof is permitted and when it is the case the conditions applying to such subcontracting. The draft RTS has been clarified in this respect.	The RTS has been clarified
Examples	Some respondents suggest that the content of the RTS should be supplemented with an indication of examples of functions considered as critical or important.	RTS cannot contain examples. RTS further specify the requirements of DORA.	No change

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Entry into force	Several respondents recommended to postpone the requirement to amend all agreements within the outsourcing chain for up to two years following the entry into force of DORA. Several respondents stressed their concerns on whether the offered timeline is appropriate for implementation of these requirements for applying them to the already existing, valid arrangements. The list of the risk elements, that should be considered, is quite extensive and it is proposed to define additional time period, preferably one year after DORA entering into the force, for the existing arrangements compliance with the defined risk management requirements.	DORA does not foresee transitional periods and therefore the requirements under DORA will apply at its date of application.	RTS has been adjusted
Question 1 : Are articles 1 and 2 appropriate and sufficiently clear?			
Article 1 proportionality	Several respondents seek clarification that article 1 allows simplified implementation for less risky/complex subcontracted services. It is suggested to add "shall apply the requirements in a proportionate manner" or to change title of article 1 to "principle of proportionality." Respondents stress that Article 1 should be read as a non-exhaustive list, without minimum requirements. If this is not the case, it should be indicated in the article.	The proportionality principle foreseen in Article 4 of DORA applies to this draft RTS together with Article 1 of this draft RTS. In this regard Article 1 of the draft RTS specifies further the criteria that can be taken into consideration by financial entities for the application of the requirements under the RTS in a proportionate way. These criteria are not exhaustive and financial entities can also develop their criteria; however, they should be able to demonstrate to their CAs that they are relevant. It should be stress that proportionality does mean waiving the requirements. The article has been clarified.	The draft RTS has been clarified
Art 1 proportionality	Several respondents advocate for a more proportionate approach focusing the oversight by the FE of material subcontractors for the provision of the ICT services supporting critical or important functions in line with the ITS on Register. The same respondents emphasize that (i) not all ICT services supporting critical or important functions carry the same level of risk to a financial entity; and (ii) not all sub-contractors supporting any aspect of critical or important functions, or a material part thereof, are of equal risk to the financial entity regardless of the sub-	Recital 64 of DORA specifies that in order to ensure a sound monitoring of ICT third-party risk in the financial sector, it is necessary to lay down a set of principle-based rules to guide financial entities' when monitoring risk arising in the context of functions outsourced to ICT third-party service providers, particularly for ICT services supporting critical or important functions, as well as	The draft RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	contractor's role, or potential impact on the financial entity or its delivery of services. Some respondents stress that whilst ideally the FE should not be required to monitor and control ICT subcontractors directly, if the ESAs do not agree, then all the requirements under this RTS should be for critical ICT subcontractors only, but not on minor/immaterial subcontractors or infrastructure providers (in circumstances where large national infrastructure providers will use ICT third party subcontractors to provide local and international communications services).	more generally in the context of all ICT third-party dependencies. In this regard and in accordance with the mandate provided under Article 30 (5) of DORA, the draft RTS focuses on subcontracting of ICT services supporting critical or important functions or material thereof for the monitoring. FE have to monitor the chain of subcontractors of ICT services supporting critical or important functions or material thereof. Once they have identified the ones that provide ICT services supporting critical or important functions or material thereof in particular the ones effectively underpin ICT services supporting critical or important functions, the requirements apply. The draft RTS has been clarified.	
Art 1 proportionality / chain of subcontractors	Several respondents request clarification as to whether financial entities are to assess the whole chain of subcontractors based on the elements listed in Article 1(a-i);	This article is about proportionality and applies to subcontracting of ICT services supporting critical or important functions or material thereof. In this regard Article 1 of the draft RTS specifies further the criteria that can be taken into consideration by financial entities for the application of the requirements under the RTS in a proportionate way. These criteria are not exhaustive and financial entities can also develop their criteria; however, they should be able to demonstrate to their CAs that they are relevant.	The draft RTS has been clarified
Art 1 due diligence / no minimal requirements	Seeks clarification on whether financial entities are required to assess /produce due diligence on the entire chain of subcontractors based on the elements listed in Article 1(a-i) and whether this as applicable on a worldwide basis, and whether a new diligence process must be carried out for each contract.	Once permitted by the FE, the use of subcontractors for the provisions of ICT services supporting critical or important functions or material thereof, the direct TPSP should be able to provide the necessary information to ensure that due diligence have been made towards all the chain of subcontractors potentially providing ICT	No change

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
		services supporting critical or important functions or material thereof	
Art 1. Legal responsibility of TPSP to provide information	Some respondents insist on stressing the responsibility of the ICT Third party to provide the information to the financial entity.	The DORA regulation and its level 2 delegated regulations are addressed to financial entities and therefore it is through the contractual arrangements that the FE should ensure that the direct ICT third party providers will provide the necessary information to ensure the monitoring of subcontractors providing ICT services supporting critical or important functions or effectively underpinning critical or important functions. However this article is about the application of proportionality.	The draft RTS has been clarified.
Art 1 Independent contractors	Several respondents note that many ICT providers use 'independent contractors' and seeks clarification that they are out of scope.	If a service supporting a critical or important function is subcontracted to a firm that falls with the definition of third-party service provider including subcontractors, even if composed of a single independent contractor, the requirements should apply.	No change
Art 1	Some respondents consider that the wording "contractual arrangements between financial entities and ICT third-party service providers on the use of subcontracted ICT services" is misleading and may suggest that FE contracts with ICT TPPs would always specifically and exclusively refer to the provision of subcontracted services.	DORA requires that any subcontracted services supporting critical or important functions should be defined in contractual arrangements of the financial entity with the direct ICT TPSP.	No change
Art1a parent company	A few respondents seek for clarification that the parent company only needs to be considered when the ICT subcontractor is not an EU-based legal entity.	The location of the parent should be considered also among other criteria to assess the complexity and the risks in line with the application of the proportionality principle.	No change
Art. 1b	Some respondents seek for clarity on whether a higher or lower number of subcontractors indicates an increased or reduced level of risk.	Determining whether the number of subcontractors providing ICT services supporting critical or important functions is too high (a high number making it difficult or impossible to appropriately monitor it) or too low is a	No change

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	A few respondents seek removal of this provision on the grounds that this requirement may compel financial entities to use TPPs with shorter supply chains, which is not an indicator of the higher resilience of such services.	part of the criteria to be assessed for the application of the proportionality principle but also for the risk assessment. This requirement is to be considered together with other criteria.	
Art 1e intra group provider	Some respondents request alignment with the level 1 terminology or adding entities within the same institutional protection scheme	The comment has been accommodated	The draft RTS has been clarified.
Art 1) fgh – Disruption, transferability, reintegration.	Some respondents suggest that disruption, transferability and reintegration are already captured by the RTS on ICT policy and should be removed/ or that assessing transferability, disruption risk, and reintegration risk for each subcontractor is unfeasible. Some other respondents suggest clarifying that reintegration or transfer are alternatives. Some respondents ask for clarification or deletion of "'technology specificities'	The comment has been accommodated	The draft RTS has been clarified.
Article 1 1)j) Concentration risk	Several respondents seek alignment to DORA and the definition 'ICT concentration Risk'/ cross-reference to art 29 DORA, or clarification on which concentrations should be assessed.	The comment has been accommodated	The draft RTS has been clarified.
Art 1	Some respondents suggest adding a new criterion regarding subcontractor maturity (eg as illustrated by certifications)	Certification alone is not sufficient. FE should consider a combination of criteria	The draft RTS has been clarified
Art 1 add criteria on oversight	Some respondents suggest adding a new criterion in particular with regard to subcontractors that would be subject to an oversight framework	The comment has been accommodated	The draft RTS has been clarified.
Art 1 suggested criterion on size / risk profile of FE	Some respondents suggest that the size (market capitalisation/financial resources, use by other FEs, international/global presence) and overall risk profile of the FE should be included in the criteria of increased or decreased risk.	The proportionality principle foreseen in Article 4 of DORA applies to this draft RTS together with Article 1 of this draft RTS. Article 4 refers to the size of the FE. In this regard Article 1 of the draft RTS specifies further the criteria that can be taken into consideration by financial entities for the application of the requirements under the	The draft RTS has been clarified.

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
		RTS in a proportionate way. The comment has been partially accommodated	
Art 2 scope	Some respondents ask for clarification on whether this Article applies to the parent company not a FE falling under DORA scope? The same respondents also want to know whether the notion of subsidiaries refers only to the subsidiaries that fall within the scope of DORA. Some other respondents emphasized that the parent undertaking does not have any legal right or means to influence the day-to-day business of its subsidiary.	DORA and accordingly the RTS apply on an individual basis and where relevant, on a sub-consolidated and consolidated basis with the aim to ensure the continuity and availability of financial services and activities, at individual and at group level. The requirements set out under the RTS are applicable to EU entities falling within the scope of application of DORA (including parent undertakings in the EU where applicable). The application at group level does not apply to parent undertakings outside of EU. However, for the EU entities, and where applicable, the RTS foresees that the requirements should be consistent and well-integrated within the group for financial entities within the EU and their subsidiaries outside the EU taking into account local legislation. The Parent undertaking, where applicable (for example under the capital requirement directive for banks), is responsible at group level to ensure a consistent and well-integrated implementation of group wide arrangements.	No change
Art2 intra group providers	Some respondents highlight that intragroup subcontracting should explicitly allow a more proportionate (lighter) approach in applying the RTS requirements	The use of Intragroup ICT service providers is a criterion to consider for the application of proportionality.	No change
Art 2 'where permitted'	Some respondents consider that "where permitted' is superfluous; others require clarification on the intention.	Where permitted is consistent with article 30(2)(a) of DORA. The use of subcontracting of an ICT services supporting critical or important function should be permitted by FE. This approach should be consistent at consolidated or sub consolidated level.	The draft RTS has been clarified.

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Art 2. Parent company “where relevant” / ‘where applicable’	Some respondents suggest adding where relevant/applicable systematically after a mention of the parent company of a subcontractor.	The comment has been accommodated	The draft RTS has been clarified.
Art. 2 Group procedure	One respondent suggests adding a requirement for a group procedure establishing conditions for subcontracting of the use of ICT services supporting critical or important functions by the group entities.	Please refer to the 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	No change
Question 2: Is article 3 appropriate and sufficiently clear?			
Proportionality and complexity	One respondent suggested removing the due diligence requirement completely where the ICT third party service providers prove to have an effective system for vetting and monitoring subcontractors.	FE still need to ensure that the direct TPSP will be able to perform due diligence towards subcontractors	No change
Concentration risk	Some respondents noted that the constraints of this article could "force" the FEs over time to often use the same suppliers, increasing their concentration risk.	Concentration risk isa key risk to be assessed by financial entities as identified in DORA article 29, article 28(4) and is a risk to be monitored on an ongoing basis.	No change
Further clarifications	A few respondents noted that it is unclear if financial entities are to undertake this risk assessment as part of a due diligence process or when contracting with ICT TPP.	Due diligence is part of the risk assessment, and both should be performed before entering into an arrangement.	No change
Open-source and blockchain solutions	A few respondents noted that the draft does not address how open-source solutions, which are often developed and maintained by a community rather than a single third-party service provider, would fit into the subcontracting framework. In cases involving blockchain transactions, where subcontractors are unknown due to reliance on technology, flexibility is sought. Public blockchain setups may not involve traditional subcontracting agreements, highlighting the need for adaptability in DLT technologies.	The draft RTS cannot address specific situations and applies to the use of subcontracting for the provisions of ICT services supporting critical or important functions	No change

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Move requirements under Article 4	A few respondents proposed that requirements under letters b), c), and i) of Article 3(1) RTS may be best included under Article 4 as they describe provisions to be addressed within the context of contractual determinations. The Article seems to be redundant with Article 4	These requirements pertain to the risk assessment that should be performed before entering into arrangements and are aspects that enable the FE to decide on whether an ICT service supporting critical or important functions may be subcontracted by an ICT third-party service provider.	No change
Article 3(1)	Several respondents noted that directly monitoring subcontractors can drain resources from strategic risk mitigation. Instead, focusing on robust risk management frameworks, including due diligence and contractual agreements, tailored to third-party engagements, is more effective. Financial entities must ensure subcontractors adhere to regulatory standards without exhaustive oversight, as they remain ultimately accountable for risks and compliance. A few respondents requested clarifications on what would happen if any individual requirements of this article cannot be met.	Article 3 sets out requirements on the risk assessment that should be performed by FEs before entering into arrangements to ensure that risks will be effectively identified and managed. The monitoring of the subcontractors providing ICT services supporting critical or important function is ensured through the direct third-party service provider under the RTS. This article provides for a list of items that should be assessed by FE against their risk strategy and risk appetite. It is up to FEs, following the assessment, to decide whether an ICT service supporting critical or important functions may be subcontracted by an ICT third-party service provider or not.	No change
Article 3(1)(a)	According to some respondents it is not clear what "**participate in operational reporting"** means and who is the subject of this sentence. The ICT TPSP can receive operational reporting from the subcontractor, but not participate in it. Some respondents noted that point (a) implies that ICT third-party service providers and subcontractors must engage in operational reporting and testing as required by the financial entity. This suggests a level of involvement for subcontractors that may not align with modern one-to-many service models like cloud services. It's recommended to qualify this obligation with **"as appropriate**" to better suit diverse service arrangements.	The comment has been accommodated	The RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Article 3(1)(b)	The vast majority of respondents noted that involving financial entities in **decision-making** is challenging and not clear and could cause operational issues for third parties. Therefore, it's suggested that the requirement should be limited to simply informing the FEs, rather than involving them in the decision-making process. According to some respondents the phrase "**when relevant and appropriate**" should be clarified to define the involvement of the FE in the decision-making process, which should be strictly restricted.	The comment has been accommodated	The RTs has been clarified
Article 3(1)(c)	The majority of respondents noted that the requirement could **undermine contractual legal principles** related to confidentiality between contracting parties. Making a FE's compliance dependent on their insight and influence in contracts where they are not a party is inherently problematic since it may also breach professional secrecy between the ICT TPP and the subcontractor. The term "**replicated**" suggests mirroring the FE contracts, financial entities should only assess if subcontracting agreements include provisions substantially equivalent to or in line with the relevant clauses in their contracts with ICT service providers. A few respondents proposed to **delete this point** since the scope (and type) of services that the ICT third-party service provider receives from any subcontractor may well be very different than the services it delivers to the financial entity. Also, **Article 3 already include appropriate conditions** to provide confidence to the financial entity on the effectiveness of the subcontractors' controls used by a third-party ICT service provider. A few respondents proposed to have this requirement only when standard contractual clauses are made available.	The comment has been accommodated. FE should ensure that the direct TPSP will itself ensure that the subcontractors providing ICT services supporting critical or important functions undertakes to comply with all applicable laws, regulatory requirements and contractual obligations; and grant the FE and competent authority the same contractual rights of access and audit as those granted by the direct TPSP.	The RTS has been clarified
Article 3(1)(d)	A few respondents seek clarification that while financial entities should analyse risks in the context of this provision, they should not be legally obligated to enforce compliance from entities with whom they do not have a contractual	In accordance with DORA, a FE, when they permit the use of subcontracting for the provision of ICT services supporting critical or important functions, should be able	No change

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	relationship. Financial entities are unable to look beyond the assurances of an ICT third-party service provider without regulatory powers. Some respondents suggested that point (d) should end with "as appropriate" to avoid a one-size-fits-all approach in subcontractor monitoring, acknowledging the diversity in subcontracted services and corresponding contracts. A few respondents suggested to specify the information security standards considered to be appropriate for Supervision purposes and in general the meaning of appropriate. A few respondents noted that this provision is duplicating Article 28(4-5) DORA and Article 6(1)(a) of the finalized RTS on the Policy on the use of ICT services, therefore it should be removed.	to monitor the risks linked to the subcontracting chain. In this context, they are able to act towards the direct TPSP. Audit, information and access rights may also be exercised directly towards the subcontractors. It is clear that the assessment referred to in point d) is related to the adequacy and capacity of the ICT TPSP to monitor its subcontractor. It belongs to the FE to determine the appropriateness of standards used by the TPSP. The ESAs believe that this provision is not replicating the articles mentioned since this provision is specific for subcontracted ICT services supporting critical or important functions.	No change
Article 3(1)(e)	The majority of respondents recommendation to **entirely remove** this section **as FE is limited in its possibilities to perform oversight** by the fact that sub-delegation is the ultimate competence and responsibility of the TPSP and there is no contractual relationship between the financial entity and the subcontractor. Alternatively, **external audit certificates** from auditors or the results of pool audits or due diligence results of the TPSP should be accepted as sufficient evidence.	In accordance with DORA, a FE, when they permit the use of subcontracting for the provision of ICT services supporting critical or important functions, should be able to monitor the risks linked to the subcontracting chain. The draft RTS and its scope have been clarified in this regard.	The draft RTS has been clarified
Article 3(1)(f)	The majority of respondents noted that the article is **ambiguous** regarding whether "**step-in rights**" pertain to the financial entity or the ICT third-party service provider. If they refer to the financial entity, it's unclear if these rights relate directly to the ICT third-party service provider, the subcontractor, or both. Many respondents proposed to propose to change the wording “including step-in rights” to “including, **where relevant and possible**, an ICT third-party service provider’s step-in rights”. Some respondents noted that **the step-in rights** requirements **should be deleted** since they are impractical for ICT service providers with many financial entity	The comment has been accommodated	The draft RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	clients and subcontractors, potentially favouring only the largest providers, reducing competition while increasing concentration risk.		
Article 3(1)(g)	A few respondents are requesting alignment with Article 1(1)(a) of the RTS. One term should be used consistently, either 'location' or 'geographical location.' Several respondents requested clarification about the meaning on geographical risks.	The comment has been accommodated. The political stability and security situation of the jurisdictions in question should be considered, including: i. the laws in force, including laws on data protection; ii. the law enforcement provisions in place; and iii. the insolvency law provisions that would apply in the event of a service provider's failure and any constraints that would arise in respect of the urgent recovery of the FE's data in particular; the risks associated with the geographical location of the potential subcontractors.	The draft RTs has been clarified
Article 3(1)(h)	One respondent requested clarification regarding the word "concentration" and whether it should be intended as subcontractor concentration towards the ICT third-party service providers, financial entity concentration directly towards subcontractors, or else.	Concentration risk is defined in Article 29 DORA.	No change
Article 3(1)(i)	A few respondents requested more clarity regarding whether this section pertains solely to the audit rights of the financial entity (FE) over the third-party provider (TPP), or if it extends to the entire subcontracting chain. Some respondents argued that the annotation "any" is too broad.	The exercise of audit, inspection and access rights extend to the subcontractors providing ITC services supporting critical or important functions or material part thereof. The right of access, inspection and audit must be ensured and therefore any obstacle should be properly assessed.	No change
Article 3(2)	Several respondents proposed to specify the frequency of the periodical assessment following the principle of proportionality. Some respondents proposed that instead of periodically reviewing these risk assessments it should be proposed that FEs shall require from their main providers to inform them about material changes that may occur at the level of their subcontractors.	The draft RTS follows a risk-based approach. Each financial entity must determine the frequency of review.	The RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	Some respondents noted that the wording "possible changes in business environment, including but not limited to changes in the supported business function" appears unclear. Also, the use of the word "their" in the draft is ambiguous. It is unclear if the re-assessment should concern the business environment of the financial entity or that of the service provider or a subcontractor	The comment has been accommodated	The RTS has been clarified
Question 3: Is article 4 appropriate and sufficiently clear?			
Article 4 existing subcontracting agreements	One respondent commented that the RTS should cover contracts that are not considered as critical or important.	Non-critical or important ICT TPP contracts are out of scope, based on Article 30 (5) of Regulation (EU) 2022/2554.	No change
Article 4 should only apply to a subset of subcontracting or use a more generalised language	Some respondents raised the issue that intragroup agreements should fall under a simplified regime. Some respondents recommended adding key contractual clauses. One respondent recommended more detailed requirements regarding data storage or processing locations. Two commenters recommended to that the Article's current Points are removed, and the following text is added: "• the ICT third-party service provider shall ensure, by way of written contract, that the subcontractors undertake to comply with all applicable contractual obligations set out in the agreement, including, but not limited to, by way of undertaking to grant the same audit and access rights as set out in the	Intragroup agreements should comply with the same requirements and DORA does not distinguish intragroup agreement vs. agreements outside of the group. The conditions under which subcontracting is allowed is a mandatory part of the contractual agreement based on Article 30 (2) a) of Regulation (EU) 2022/2554. Key mandatory contractual clauses are directly set under DORA. The comment has been partly accommodated.	No change No change The RTs has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	agreement and to comply with the security requirements set out in the agreement.) • the duties and responsibilities of the ICT third-party service provider under the agreement shall remain unaffected by any subcontracting, and the ICT third-party service provider shall retain full accountability for the subcontracted services and its subcontractors' performance as for its own.." [European Association of Cooperative Banks, European Cloud User Coalition ECUC]		
Article 4	Some respondents argue that integrating the needs of multiple financial entities into the service offerings is cumbersome and may result in market repercussions. Managing later changes results in a frequent modification of the contract between the financial entity and the third-party ICT service provider.	The requirements are addressed to financial entities. DORA and the level 2 regulatory products specify the mandatory elements that should be inserted in the written contractual agreement between the FE and the TPSP. FE should also ensure that these aspects will be covered when the use of subcontracting for the provisions of ICT services supporting, or critical function is permitted. This is in line with the mandate under Article 30(5). It then belongs to FE and TPSP and subcontractors to organise themselves.	No change
Some Points regarding material change should be cross-referenced in Article 6	One respondent commented that provisions in Article 4 of the Draft RTS do not deal with material changes to the subcontract	A specific article has been inserted in the draft RTS	No change
Article 4 should be explicitly limited to critical or important functions and should use the formula of DORA	Several respondents recommended adding the reference to critical or important functions, some adding a reference to the formula used in Article 30 (1) of Regulation (EU) 2022/2554. A respondent remarked that the point needs clarification on whether the term "contractual agreement" refers to the agreement between the financial entity and the ICT third-party service provider, or the ICT third-party service provider	The draft refers to the contractual arrangement between the FE and the direct TPSP. In accordance with DORA, this contractual arrangement should set out the conditions for the use of subcontracting to provide ICT services supporting critical or important functions or material part thereof. It belongs then to the FE to ensure that the ICT third-party service provider shall ensure, by way of written contract, that the subcontractors undertake to comply with all applicable contractual obligations set out	The draft RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	and its subcontractor. It is unclear for them who is ultimately responsible if the subcontractor is unable to meet its obligations or fails under the arrangement. 'When describing in the written contractual arrangements the ICT services to be provided by an ICT third-party service provider (…), 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: (…). The written contractual arrangement should be documented on paper or in another downloadable document with durable and accessible format," using the formula in Art 30 (1). 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 and document in the contract between the financial entity and the ICT third-party provider, which ICT services support critical or important functions, describe which critical or important functions those ICT services support in sufficient detail to enable the ICT third-party service provider to identify which elements of its ICT services support critical or important functions of the financial entity, 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 in respect of ICT services supporting an identified critical or important function:"	in the agreement, including, but not limited to, by way of undertaking to grant the same audit and access rights	
Article 4 overreaches its mandate	Some respondent argued that the RTS contains more than the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions. One of them proposes the following change: "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~~ the written	The comment has been accommodated.	The draft RTs has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	contractual arrangements shall identify which ICT services are eligible for subcontracting and under which conditions.		
Article 4 does not contain reference to material changes	One respondent raised the issue that Article 4 of the Draft RTS, should include rules for the ICT TPP dealing with material changes in the subcontracting arrangements	The RTS is addressed to financial entities. In any case Articles 6 and 7 of the RTS capture this point.	The draft RTs has been clarified
Art 4	Some respondents state that it is necessary to clarify whether the entity should be informed in advance about the start of the subcontracting or whether it should be informed at a later date.	The FE should be informed of the start of the subcontracting before it starts.	The draft RTs has been clarified
Article 4 a) scope of monitoring	Some respondents sought clarification on whether the monitoring in 4a) refers to Article 5 of the RTS or other texts (eg. quantitative criteria based on Article 10 or monitoring as defined in Article 30 (3) e)	The scope of monitoring under article 4 a) relates to the written agreement and the contractual obligations between the FE and the direct TPSP regarding subcontracting on the provision of ICT services supporting critical or important functions or effectively underpinning critical or important function. Article 5 is about the ongoing monitoring (risk-based) of the chain of subcontractors **providing critical or important function or material thereof.**	The RTS has been clarified
Article 4 b) scope of reporting	Two respondents remarked that this Point needs clarification whether the reporting and monitoring requirements relate to point 4 a) or to general reporting/monitoring obligations for the ICT TPP. Two respondents recommended removing this clause since it regulates the relationship between the third-party ICT service provider and the financial entity instead the third-party ICT service provider and its subcontractor. A respondent recommended that this clause should refer to access to the third-party ICT service provider providing access to its subcontracting agreements.	The monitoring and reporting obligations of the ICT third-party service provider towards the financial entity regarding the subcontracting relates to point a). The article has been clarified. The RTS is addressed to FE and this article is in line with the mandate under Article 30(5) of DORA.	The RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Art 4c) parent company	Some respondents commented that the wording of Article 1 a) and this Point should be aligned. One respondent recommended removing the reference from the parent company.	The comment has been accommodated	The RTS has been clarified
Article 4 c) location risks	Several respondents raised that "all risks" should be modified to "relevant" risks or a more precise qualifier be used. Two commenters proposed "all risks to the ICT service supporting a critical or important function that are relevant to whether there might be a material impairment of the kind described in Article 3(22) of Regulation (EU) 2022/2554"	The comment has been parly accommodated	The RTS has been clarified
Article 4 c) current subcontractors	A respondent recommended limiting the requirement to current subcontractors only. One respondent recommended expanding the requirement to existing subcontractors.	The comment has been accommodated	The RTS has been clarified
Article 4c) communication of assessment	One respondent mentioned that without the requirement to communicate the results, the risk assessment done by the ICT third party provider does not provide benefit to the financial entity in addition to the requirements set out in Articles 1 and 3.	The draft RTS foresees that the ICT third-party service provider is required under Article 4b) to monitor and report towards the financial entity; it belongs to the both parties to the contract to define the modalities of such obligation in the contractual obligation	No change
Article 4 d) ownership of data	Several respondents commented that data cannot be owned according to national law. Some respondents recommend = deleting Article 4 (d) or refer to, instead of "ownership," "data processed or hosted on behalf of the financial entity" is offered.	The comment has been partially accommodated	The RTS has been clarified
Art 4e) alternative assurance levels	One respondent remarked that Article 30 (3) e) (ii) allows the financial entity and the ICT service third-party provider to agree on alternative assurance levels if other clients' rights are affected, whereas the RTS does not reflect this.	As this is foreseen directly under Article 30(3) of DORA, it is not necessary to repeat the requirement.	No change
Article 4 e) direct monitoring of FEs on subcontractors	Numerous respondents found that financial entities' monitoring should be limited to the ICT Third Party and not to subcontractors as the financial entity is not party to the contract. According to the recommendations, the ICT services providers	This point may be necessary for example when the FE uses it access, inspection and audits rights towards the subcontractor. In this context the subcontractor may	The RTS has been clarified

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	should ensure that their contracts with subcontractors are in compliance with their monitoring and reporting obligations. One respondent recommended the following: Add under 4 e) "in its written contractual agreement with the ICT subcontractor" after "is required to specify."	provide information directly to the FE. This is fully in line with DORA. The comment has been accommodated	
Art.4e) reporting - where relevant	One respondent asked clarification for the term "where relevant." One commenter supported the qualifier as direct monitoring of the subcontractor is not the default practice.	See answer above	No change
Article 4 f) continuous provision of service	The majority of the respondents questioned whether the term "ensure the continuous provision of the ICT services" is proportionate. Some feel that this could lead to the subcontractors rejecting to sign. They recommend limiting this to critical TPPs, limiting to the TPP to periodically assess the resilience and recovery of these functions, qualifying the expected availability requirement, or removing the requirement.	The provision has been clarified.	RTS has been clarified
Article 4 g) incident response and BCP	Respondents remarked that the incident response and business continuity plans (of the subcontractor) should not be part of the agreement between the FE and TPSP due to security reasons and because they are generally separate (living) documents. One commenter recommended limiting this requirement to subcontractors whose failure may have a material impact to the critical or important function. Some respondents recommended concentrating on the TPP complying with this requirement. One respondent remarked that it is unclear whether the subcontractor is required to have their own business contingency plans or they have to comply with the plans of the financial entity.	That incident response and BCP is contained in a separate document is not an impediment to fulfilment of the requirement. The point is that BCP should be agreed and binding between the TPSP and the subcontractor in accordance with the requirement applicable to FE. The provision has been adjusted.	RTS has been clarified
Art 4g) contingency	Two respondents recommended changing the reference to 'the business contingency' plans (Article 30 (3) c) of DORA).	The comment has been accommodated	RTS adjusted

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Art 4g,h) testing	One respondent remarked that more information should be provided regarding the type and periodicity of the tests required. One respondent recommended that greater emphasis be placed on the obligation to necessarily involve subcontractors in testing.	The type and periodicity of such testing are the responsibility of the contracting parties. Subcontractor involvement is covered in the risk analysis under article 3 ("as required by the financial entity"). It may be an agreed contractual obligation	No change
Art 4g,h) customization	Some commenters raised the issue that TPPs need to provide unique, individual responses (per financial entity) which leads to customization in the contractual agreements between ICT third-party service provider and subcontractor.	The subcontractor is required to demonstrate, through the contractual arrangement with the direct TPSP that it meets the requirements set by the direct TPSP (and thus the financial entity)	No change
Art. 4 h) confidentiality	Two respondents remarked that subcontractors will be unwilling to share their security controls framework with entities who are not their direct clients.	The point is that security standards should be agreed and binding between the TPSP and the subcontractor, and that this should be a requirement of the contract between the FE and the TPSP. The provision has been adjusted.	RTS has been clarified
Art. 4i) no direct relationship	Some respondents raised the issue that a subcontractor is not in direct contractual relationship with the financial entity, therefore it may not accept the financial entity's audit rights.	The extension of access, audit and inspection rights along the subcontracting chain is not a new requirement (see outsourcing framework under the respective sectoral legal framework).	No change
Art. 4i) FE expected effort	One respondent commented that the current wording that financial entities would mean that financial entities are expected to exercise those audit rights to the same level as with third-party service providers. One respondent recommended adding that the TPP should spend "commercially reasonable effort" to achieve this objective.	Access, audits and inspect rights are exercised by the FE and CAs on a risk based approach	No change

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Art. 4i) narrow down to services to the FE	One respondent recommended to limit audit rights at the subcontractor to assets or resources which are involved in the provision of services to the financial entity.	Access, inspection and audit, rights are limited to the provisions of ICT services supporting critical or important function or material part thereof.	No change
	Several respondents recommended removing "at least" since subcontractors are unlikely to be subject to more stringent audits than the ICT third party provider, or suggested "materially equivalent" rights.	The comment has been accommodated	RTS has been clarified
	Some respondents indicated that pooled audits should be specifically allowed. One respondent suggests that the contract with ICT third-party service providers require them to share audits conducted on the subcontractors by an independent party.	Pooled audits are allowed by L1.	
Art. 4j) duplicative	Some respondents stressed that this requirement appears partly duplicative with regards to Article 7.	Agreed that the FE's right to terminate the agreement under article 7 does not need to be replicated in the contract.	RTS adjusted
Article 4 j) should be removed or amended.	A significant number of respondents recommended that termination rights should only apply in case of a material breach of the agreement, or that the provision be to reflect the content of the contract. Respondents argued that the contract should only be terminated where the ICT third-party service provider fails to meet its service levels.	Suggestion accepted to provide that termination rights should be included in the contract in the cases referred to in Article 28 (7) of DORA.)	RTS adjusted
Art 4j) corrective actions, exit plans	One respondent remarked that a reference to exit plans should be added. Some respondents stress that a failure to meet service levels may lead to corrective actions, as referred to in Article 30 (3) a) of Regulation 2554/2022, rather than termination.	The scope of this provision is termination rights.	No change
Question 4: Is article 5 appropriate and sufficiently clear?			

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Art 5 proportionality / scope	A majority of respondents consider that monitoring the entire ICT subcontracting chain by FE imposes an unreasonable a disproportionate burden on financial entities and ICT providers. Several respondents consider that it is impractical to expect a FE to directly assess and manage every risk across each element of the supply chain without application of the principle of proportionality, and stress that dispositions should reflect the intention in the DORA legislative text for a proportionate approach to ICT third-party risk management. Several respondents stress that review of contractual documentation would consume lot of time and resources of the outsourcer/financial entity. Several suggest that the application of a risk-based approach (sometimes citing the FSB toolkit on 3rd party-risk) could be considered for the monitoring of the subcontractors to ensure a better focus of resources. A few respondents suggest that a materiality threshold should be included. Several respondents considered align Article 5 with the approach in the ITS on the Register of information so that the **requirement** to **monitor** the ICT **subcontracting chain** should **be limited** to **subcontractors** that **effectively underpin** the provision of these ICT services i.e. all the subcontractors providing ICT services whose disruption would impair the security or the continuity of the service provision. One notice that a small financial entity might not have negotiation leverage and sufficient resources to perform monitoring at level at each subcontractor as request in Article 5.	In order to allow financial entities to reap the benefits of innovative solutions, a policy choice was made by DORA and these RTS not to impose a hard limit on the number of levels in the subcontracting chain when ICT services supporting critical or important services are subcontracted by TPSPs. However, the financial entity should be able to monitor the subcontracting chain in its entirety. With regards to the proportionate application of this requirement, it has been clarified that financial entities are to particularly focus such monitoring on subcontractors that effectively underpin the provision of the service.] The choice to use subcontracted services supporting its critical or important functions is a choice of the financial entity for which it should bear responsibility.	RTS adjusted
Art 5 complexity and cost	Several respondents consider the **complex** nature of such operational task, for instance in relation to **software products**. One considers there could be **one-to-many** relationships beyond **one-to-one** traditional service model. For example in the public cloud infrastructure : a single subcontractor engaged by a cloud service provider (CSP) is relevant to potentially all the CSP's customers. Although the CSP will have separate contract with each financial entity (this could be hundreds of financial entities), it will have one contract with each financial entity. One respondent consider that having **both** ICT third-party service **providers** and **financial entities contacting** the **same subcontractors** in the ordinary course for	FEs need to be in a position to asses whether the TPSP can continue to provide the ICT service supporting a critical or important function including subcontractors providing ICT services supporting critical or important functions. In this respect they should be able to monitor them and comply with their own regulatory obligations.	RTS adjusted

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	the same information creates confusion and unnecessary cost and effort for all parties involved. A few respondents considered that the scope of services received by the ICT provider from any subcontractor may be much wider than the services it delivers to the FE. Besides subcontractors could contribute in different ways and with different relevance to the provision of the overall ICT service. Some respondents considered that the article 5's operational application would be **extremely onerous** on financial entities.		
Article 5.1 – Responsibility	A majority of respondents consider that monitoring the underlying ICT subcontractors should be the responsibility of the ICT third party service provider as part of ensuring their ability to continue delivering services to the FE. They claim that giving the responsibility for monitoring of subcontractors to the financial entity might have the effect of diluting the overall responsibility of the ICT third-party provider to provide the ICT services end-to-end. Some respondents consider that (external) audit reports/certificates from the ICT provider could be sufficient and be leveraged to get assurance on the management of the overall service, including subcontracted components. Other respondents consider that if the financial entity does not receive the required information from the ICT third-party service provider within a reasonable amount of time, then the financial entity should be authorized to contact a subcontractor directy. Some respondents indicated that is not clear where this responsibility ends and where that of the main supplier begins.	The requirements of this RTS, and indeed the ultimate responsibility for the decision to use subcontracted services supporting critical or important functions, lie with the financial entities. Conversely an ICT provider's responsibility to monitor its subcontractors is contractual. An ICT third party service provider and its subcontractors must provide the information necessary to ensure that the risk assessment and the monitoring can be carried out by the financial entities.	No change
Article 5.1 – frequency	Some respondents ask for clarifications on the frequency of review.	Financial entity must ensure at any time that ICT risks are well assessed to achieve resilience. This should not be confused with a periodic review.	No change

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Art 5.1 Redundancy with ITS on register	Several respondents consider that the documentation requirements **redundant with** the maintenance of the **information register** 28.9 DORA and suggest to delete or clearly refer to it.	The requirement has been clarified to define the concrete steps involved in the monitoring, including he documentation in accordance with the ITS on the Register of Information.	RTS adjusted
Art 5.2 – confidentiality, 'as appropriate'	The majority of respondents consider that since financial entities do not have a **direct commercial relationship** with such sub-contractors, it is not clear why ICT third-party service providers would allow FEs to review **commercially sensitive agreements** established with subcontractors. Then, it raises a legal issue and creates both confidentiality, competition and antitrust concerns. One respondent seeks clarification on the term '**as appropriate**' in the sentence *'including through the review of contractual documentation, as appropriate'.*	The requirement is limited to monitor ICT services supporting critical or important functions provided by the ICT provider covered by the contractual arrangements. The contractual agreements need to ensure that confidentiality is protected.	No change
Article 5.2 - Review of KPIs	Some respondents consider that the disposition should be more **prescriptive**. They welcome **additional guidelines** on how requirements could be applied.	The RTS has been adjusted.	RTS has been adjusted
Question 5: Are articles 6 and 7 appropriate and sufficiently clear?			
Art 6,7 statutory termination rights	Several respondents raised that the termination right in Art. 7 (1) and the right to request modifications in Art. 6(4) create direct obligations on the service providers and do not describe the contractual conditions as set out in Art. 30(5) DORA. A few noted that establishing a statutory termination right would interfere with contractual freedom and voiced constitutional concerns.	DORA 28(7) and 28(8) establish statutory termination rights. The requirements of these RTS are written in accordance.	No change
Art 6,7 **Right to object is not feasible / termination fees**	Many respondents have noted that a veto to changes in subcontracting arrangements is not realistic, noting that many financial entities lack the necessary bargaining power. A few has responded that a veto is only realistic for those ICT-TPSP that are designated as critical and are under oversight.	Articles 6 and 7 establish firstly a right of the financial entity to be informed by the TPSP under a notice period in case of material changes to subcontracting arrangements, and secondly a right to terminate the contract in precise cases linked to them. The TPSP should	RTS has been clarified.

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	Some have noted that such a veto would impact many ICT third-party service providers' business model, especially for one-to-many nature of many cloud service providers. Also, respondents noted that a veto requirement could potentially lead to ICT third-party service providers no longer offering their services to financial entities, limiting their capacity for digitalization and innovation. Some respondents noted that a veto could prevent the rollout, change or expansion of services with benefits for thousands of customers, also affecting those not subject to DORA. Additionally, while some financial entities approve, a few other might not, creating a situation of uncertainty. Several respondents point out that these concerns might lead to further concentration of service providers. One respondent suggested that objections should only be allowed for material operational risks and not be tied to more subjective criteria such as the financial entities risk appetite. A few respondents suggest that changes aimed at improving the overall solidity of the ICT-TPSP should be exempt from the right to object and that objections should only be made in exceptional circumstances. A few respondents suggest that the right to object assumes a disproportionate level of influence and should be limited to a right to terminate the contractual agreement or request modifications to the subcontracting arrangements. Several respondents suggest to add that a termination according to Art. 7 should not come with (financial) penalties that discourage the financial entity from exercising this right.	be allowed for a period of time to respond to the financial entity's concerns and objections, before it can exercise the termination right. The definition of this response period falls under the contractual freedom between the financial entity and the TPSP.	
Art 6.1 Clarification on material changes	Many respondents request clarification on what constitutes a material change in subcontracting arrangements and give examples, one suggested limiting to those that are reasonably expected to have material adverse impacts.	Material changes are changes that have an effect on the risk level of the categories described in article 3.	RTS adjusted

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
	Some respondents point out that requiring the financial entity to assess all changes with regard to materiality imposes a heavy burden.		
Art 6.1 Clarification on notice period	Many respondents request clarification on the length of a sufficient advance notice period and some request a set time frame, e.g. of 60 or 90 days. One respondent suggested substituting "sufficient" with "reasonable" for more certainty. Several respondents noted that there should be room for exceptions in case of emergency situations (e.g. financial stability of the subcontractor, non-compliant services, etc.). One respondent noted that a regulated financial entity acting as an ICT-TPSP might come into a conflict between fulfilling its regulatory and contractual obligations by not changing subcontracting arrangements in due time.	This should be left to the contractual arrangements.	RTS adjusted
Art 6.1 Criteria for risk assessment	Several respondents point out that there is no guidance or criteria communicated for the risk assessment mentioned in Art. 6(1).	The risk assessment under article 6 refers to the risk assessment categories under article 3.	No change
Art. 6.2 Information on assessment results	Several respondents noted that risk assessment results could contain internal or confidential information and there could be other, including commercial, reasons not to inform the ICT-TPSP of the content of the analysis. Some added that divulging information could pose a security or operational risk to the financial entity, while others have requested clarification on what a ICT-TPSP should do with the information provided. Some suggested that information should only happen in case the financial entity rejects the change in subcontracting conditions, others warned that such information might lead to challenges to the assessment by ICT-TPSPs.	RTS clarified to indicate that the ICT-TPSP is informed of high-level details leading to the objection against proposed changes in the subcontracting arrangements.	RTS clarified
Art 6.3 Clarification on passive consent	Several respondents propose to clarify that the ICT-TPSP can assume passive consent is given when no objection is raised in the agreed period. The wording of Art. 7 creates a right to terminate unless approval is given.	The current wording already covers the requested changes sufficiently.	No change

Comments on provision	Summary of responses received	Joint ESAs analysis	Amendments to the proposals
Art 7 Reference of termination clauses	Several respondents pointed out that the reference of Art. 28(10) DORA in Art. 7 of the draft RTS is probably a clerical error and should reference Art. 28(7) instead.	Suggestion accepted	RTS adjusted
Art 7a : good cause and notice period from FE to TPSP before termination	A few respondents point out that the termination right should only be available for good cause and after giving proper notice to the ICT-TPSP with the possibility to remedy the situation.	The current requirement already provides flexibility to assess and remedy the situation before termination.	No cahnge
Art 7a: Limitations on termination rights	Some respondents suggested that the right to terminate should also be satisfied by discontinuing to use the affected service, while continuing to use other services not encumbered by the proposed subcontracting change.	This level of detail is too contract-specific and amounts to the definition of an ICT service. The current requirement offers appropriate flexibility.	No change.