JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2023 84

17 01 2024

Final report on

Draft Regulatory Technical Standards

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

Contents

1. Executive Summary

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

In line with Regulation (EU) 2022/2554, the draft RTS sets out requirements for the policy of financial entities on their use of ICT third-party service providers, including ICT intragroup providers and concerns all ICT services provided by them that support critical or important functions.

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

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

2. Background and rationale

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

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

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

4. Furthermore, when developing 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, the draft RTS set out requirements for the policy of financial entities on their use of ICT third party service providers, including ICT intra group service providers and concerns all ICT services provided by them that support critical or important function.

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

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

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

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

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

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

Next Steps

The ESAs will submit the RTS to the European Commission for adoption.

3. Draft regulatory technical standards

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/2554 of the European Parliament and of the Council, of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 and, in particular Article 28(10) thereof,

Whereas:

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

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

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

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

of this Regulation are to be applied in a manner that is proportionate, taking into account, in particular, the financial entities' size and internal organisation and the nature, scope and complexity of their activities. In this regard, this Regulation provides for a non-exhaustive list of criteria to be considered by financial entities for the application of the principle of proportionality.

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

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

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

(8) To ensure appropriate reporting to the management body, the policy should clearly specify and identify the internal responsibilities for the approval, management, control and documentation of contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers, including the ICT services provided under these arrangements in accordance with Article 28(1)(a) of Regulation (EU) 2022/2554.

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

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

expertise and adequate financial, human and technical resources, information-security, appropriate organisational structure, including risk management, and internal controls that the ICT third party service providers should have in place.

(11) To ensure a sound risk management in the provision of ICT services supporting critical or important functions by ICT third-party service providers through contract management, the policy should contain information with regard to the implementation, monitoring and management of contractual arrangements for the use of ICT services supporting critical or important functions including at consolidated and sub-consolidated level, where applicable. This includes requirements on the contractual clauses on mutual obligations of the financial entities and the ICT third-party service providers that should be set out in a written agreement. The policy should ensure the financial entities' or appointed third parties' and competent authorities' rights to inspections and access to information and should also further specify the exit strategies and termination processes.

(12) The European Supervisory Authorities have conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the ESA's Stakeholder Groups established in accordance with Article 37 of Regulation (EU) No 1093/2010, Article 37 of Regulation (EU) No 1094/2010 and Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council.

HAS ADOPTED THIS REGULATION:

Article 1

Overall risk profile and complexity

The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall take into account, for the purpose of Articles 3 to 10, at least the following elements of increased or reduced risk or complexity:

(a) the type of ICT services included in the contractual arrangement between the financial entity and the ICT-third party service provider;
(b) the location of the ICT third-party service provider or its parent company;
(c) whether the provision of ICT services supporting critical or important functions by ICT third-party service provider 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.
(d) the nature of data shared with the ICT third-party service providers;
(e) whether the ICT third-party service providers are part of the same group of the financial entity;
(f) the use of ICT third-party service providers 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;

(g) 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;

(h) the concentration in the provision of ICT services supporting critical or important functions by a single or small number of ICT third-party service providers;

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

(j) the potential impact of disruptions on the continuity and availability of the financial entity's activities.

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 policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as referred to in Article 28 (2) of Regulation (EU) 2022/2554, is implemented consistently in their subsidiaries and is adequate for the effective application of this Regulation at all relevant levels.

Article 3

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

(1) As part of the strategy on ICT third-party risk referred to in Article 28(2) of Regulation (EU) 2022/2554, and taking into account the multi-vendor strategy referred to in Article 6(9) where applicable, the management body of a financial entity shall adopt a written policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers, and ensure its implementation on an individual and, as applicable, on a sub-consolidated and consolidated basis.

(2) The management body shall review the policy referred to in paragraph 1 at least once a year, and update it where necessary. Changes made to the policy shall be implemented in a timely manner and as soon as it is possible within the relevant contractual arrangements. The financial entity shall document the planned timeline for the implementation.

(3) The policy referred to in paragraph 1 shall define or refer to a methodology for determining which ICT services support critical or important functions. The policy shall also specify when this assessment should be conducted and reviewed.

(4) The policy referred to in paragraph 1 shall clearly assign the internal responsibilities for the approval, management, control, and documentation of relevant contractual arrangements and shall ensure that appropriate skills, experience and knowledge are maintained within the financial entity to effectively oversee the relevant contractual arrangements, including the ICT services provided under these arrangements.

(5) Without prejudice to the final responsibility of the financial entity to effectively oversee relevant contractual arrangements, the policy referred to in paragraph 1 shall foresee that the financial entity assesses that the ICT third party service provider has sufficient resources to ensure that the financial entity complies with all its legal and regulatory requirements regarding ICT services supporting critical or important functions that are provided.

(6) The policy referred to in paragraph 1 shall clearly identify, in accordance with Article 5(3) of Regulation (EU) 2022/2554, the role or member of senior management responsible for monitoring the relevant contractual arrangements. This policy shall define how this role or member of senior management shall cooperate with the control functions where it is not part of it and define the reporting lines to the management body, including the nature and frequency of the documents to report.

(7) The policy referred to in paragraph 1 shall ensure that the relevant contractual arrangements are consistent with the financial entity's ICT risk management framework referred to in Article 6(1), the information security policy under Article 9(4), the business continuity policy under Article 11 and the requirements on incident reporting under Article 19 of Regulation (EU) 2022/2554.

(8) The policy referred to in paragraph 1 shall require that ICT services supporting critical or important functions provided by ICT third party service providers are subject to independent review and included in the financial entity's audit plan.

(9) The policy referred to in paragraph 1 shall explicitly specify that the relevant contractual arrangements:

a. do not relieve the financial entity and its management body of its regulatory obligations and its responsibilities to its clients;

b. shall not hinder effective supervision of a financial entity and shall not contravene any supervisory restrictions on services and activities;

c. have provisions in place that ensure that the ICT third party service providers cooperate with the competent authorities; and

d. have provisions in place that ensure that the financial entity, its auditors, and competent authorities have effective access to data and premises relating to the use of ICT services supporting critical or important functions.

Article 4

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

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

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

(b) the planning of contractual arrangements for the use of ICT services supporting critical or important functions provided by ICT third-party service providers including the risk assessment, the due diligence as set out under Articles 5 and 6 of this Regulation and the approval process of new or material changes to relevant third-party contractual arrangements as set out under Article 8 (4) of this Regulation;

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

(d) the implementation, monitoring and management of contractual arrangements as referred to in Articles 7, 8 and 9 of this Regulation for the use of ICT services supporting critical or important functions including at consolidated and sub-consolidated level, where applicable;

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

(f) the exit strategies and termination processes as set out under Article 10 of this Regulation.

Article 5

Ex-ante risk assessment

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

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

Article 6

Due diligence

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

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

(b) uses or intends to use ICT sub-contractors to perform ICT services supporting critical or important functions or material parts thereof;

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

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

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

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

(3) The policy referred to in paragraph 1 shall:

(a) determine the due diligence process for selecting and assessing the prospective ICT third-party service providers, including which of the following elements shall be used for the required level of assurance:

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

(b) Financial entities shall consider the scope and limitations of the elements listed in paragraph 3(a) and where appropriate, more than one element shall be used.

Article 7

Conflict of interests

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

(2) Where ICT services are provided by ICT intra-group service providers, the policy referred to in paragraph 1 shall specify that decisions on conditions, including the financial conditions, for the ICT services supporting critical or important functions are taken objectively.

Article 8

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

(1) The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall specify that the relevant contractual arrangement shall be written and shall include all the elements set out by Article 30(2) and 30(3) of Regulation (EU) 2022/2554. The policy shall also include elements regarding requirements applicable to financial entities as per Article 1 (1)(a) of Regulation (EU) 2022/2554, as well as other relevant Union and national law as appropriate.

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

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

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

(c) where appropriate, third-party certifications

(d) where appropriate third-party or internal audit reports made available by the ICT third-party service provider.

(3) The financial entity shall not rely solely on certifications under paragraph (2)(c) or reports under paragraph (2) (d) over time and these shall be used only if it:

(a) is satisfied with the audit plan of the ICT service third-party provider for the relevant contractual arrangements;

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

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

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

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

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

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

(h) retains the contractual right to perform individual and pooled audits at its discretion with regard to the relevant contractual arrangements and execute them in line with the contracted frequency.

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

Article 9

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

(1) The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall ensure that the relevant contractual arrangements specify the measures and key indicators to monitor, on an ongoing basis,

to assess the performance of ICT third party service providers, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial entity's relevant policies and procedures. The policy should also specify measures that apply when service level agreements are not met including, where appropriate contractual penalties.

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

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

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

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

(d) the financial entity is notified, where appropriate, of ICT- related incidents and operational or security payment related incidents;

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

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

(4) The policy referred to in paragraph 1 shall define the appropriate measures that the financial entity shall adopt if it identifies shortcomings of the ICT third-party service provider, including ICT-related incidents and operational or security payment related incidents, in the provision of the ICT services supporting critical or important functions or the compliance with contractual arrangements or legal requirements and how the implementation of such measures shall be monitored to ensure that they are effectively complied within a defined timeframe, taking into account the materiality of the shortcomings.

Article 10

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

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

Article 11

Entry into force

This Regulation shall enter into force on the twentieth day following 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
[…]

[Choose between the two options, depending on the person who signs.]

On behalf of the President
[…]
[Position]

4. Accompanying documents

4.1 Draft cost-benefit analysis / impact assessment

1. As per Article 15(1) of Regulation (EU) No 1093/2010 (EBA Regulation), of Regulation (EU) No 1094/2010 (EIOPA Regulation) and Regulation (EU) No 1095/2010 (ESMA regulation), any draft regulatory technical standards developed by the ESAs shall be accompanied by an Impact assessment (IA) which analyses 'the potential related costs and benefits'.

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

Problem identification

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

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

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

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

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

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

Policy objectives

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

Baseline scenario

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

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

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

POLICY ISSUE 1: DEFINITION OF CRITICAL AND IMPORTANT FUNCTIONS

Options considered

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

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

Cost-benefit analysis

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

Preferred option

15. Option B has been retained.

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

Options considered

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

- *Clarification of responsibilities of the management body with regard to the adoption and the oversight of the implementation of the policy on ICT services provided by third-party service providers in relation to critical or important functions.*
- *Clarification of the role of internal controls in this context.*
- *Clarification on the frequency of the policy review (at least every year and when necessary).*
- *Necessity to provide for clarity regarding the continuous responsibility for ensuring that the financial entity can be supervised, including that measures can be implemented.*

17. Option B: No additional governance arrangements

Cost-benefit analysis

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

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

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

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

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

Preferred option

23. Option A has been retained.

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

Options considered

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

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

Cost-benefit analysis

26. The specification that the policy should cover the whole lifecycle of contractual arrangement from pre phase to exit will ensure an appropriate and sound risk management framework for this purpose...

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

28. Option A has been retained.

POLICY ISSUE 4: RISK ASSESSMENT OF ICT SERVICE PROVIDERS

Options considered

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

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

Cost-benefit analysis

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

Preferred option

32. Option A has been retained

POLICY ISSUE 5: DUE DILIGENCE OF ICT SERVICE PROVIDERS

Options considered

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

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

Cost-benefit analysis

35. In case of due diligence, a lighter touch approach on the ICT intragroup service providers is justified because group entities are known by the financial entities and covered by the internal control system. This is achieved by a proportionate application of the due diligence requirements as foreseen under Article 6 of the draft RTS with regard to ICT intragroup service providers combined with Article 1 on the criteria listed for the application of the proportionality principle.

Preferred option

36. Option B has been retained.

POLICY ISSUE 5: LEVEL OF ASSURANCE IN DUE DILIGENCE PROCESS

Options considered

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

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

Cost-benefit analysis

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

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

Preferred option

41. Option B has been retained.

POLICY ISSUE 6: SOURCES OF CONFLICT OF INTERESTS

Options considered

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

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

Cost-benefit analysis

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

Preferred option

45. Option B has been retained.

POLICY ISSUE 7: CONTRACTUAL CLAUSES

Options considered

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

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

Cost-benefit analysis

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

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

Preferred option

50. Option A has been retained.

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

Options considered

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

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

Cost-benefit analysis

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

Preferred option

54. Option A has been retained.

Overall Cost-Benefit Analysis

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

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

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

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

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

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

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

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

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

64. POLICY ISSUE 9: PROPORTIONALITY PRINCIPLE

Options considered

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

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

Cost-benefit analysis

Option A and partly B was considered. DORA already sets out a general requirement on the proportionate application of its requirements. The draft RTS further specify some of the criteria for the application of the proportionality principle that can be considered by financial entities and competent authorities when doing the proportionality assessment. In addition, the Level 1 already foresees some exemptions for small entities. Some proportionality was also explicitly introduced regarding the due diligence to be performed when the ICT third party provider is part of a group.

4.2 Summary of responses to the consultation

The consultation ran from 19th June 2023 to 11th September 2023. 104 responses to the consultation were received.

Summary of responses to the consultation and the ESA's analysis

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
General comments			
General application of the RTS	Several respondents requested further clarity regarding the alignment of requirements between existing ESA guidelines and DORA. This includes aspects like proportionality, materiality, and the interpretation of critical functions. Several respondents noted that it would have been easier for credit institutions and investment firms already subject to the EBA guidelines, to provide these firms the option of extending the existing EBA Outsourcing regime to ICT services (non-outsourcing) supporting critical or important functions. One respondent commented that the general application is unclear. Preamble states that	The RTS is aligned with DORA and is consistent with the ESAs guidelines on outsourcing that apply to all areas and not only ICT. 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. The ESAs have a mandate to draft RTS specifying the detailed content of the policy on the contractual arrangements regarding the use of ICT services supporting critical or important functions provided by ICT third-party service in accordance with Article 28 (2) of DORA.	No change No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	RTS applies for all ICT services, not only outsourcing arrangements.	The RTS specifies the detailed content of on the contractual arrangements regarding on the use of ICT services supporting critical or important functions provided by ICT third-party service. The scope of addressees is also broader under DORA and does not include only credit institutions or investment firms.	No change
	Some respondents considered that the lack of convergence in the definition of outsourcing of critical or important function in these two regulations will result in dualism in outsourcing systems in financial entities – the first outsourcing classification system will be for EBA outsourcing guideline's purpose, the latter for DORA purpose.	See comment above. The RTS does not provide for a definition of outsourcing because the scope of DORA is broader than outsourcing. DORA refers to third party arrangements that include also outsourcing arrangements. The definition of critical or important is provided by DORA and the definition under the guidelines is consistent also. There is no contradiction between the two.	No change
	One respondent called for consistency with DORA, including changes in the frequency of policy review and wording related to written agreements in the recitals.	The policy review should be done at least once a year and updated where it is necessary.	No change
	Some respondents considered the RTS to be a shift, from framework requirements in the EBA guidelines, to policy demands, and requested clarification for this "supervisory divergence".	According to DORA 28(2) the strategy on ICT third-party risk shall include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. The ESAs are mandated to develop jointly draft regulatory technical standards to further specify the detailed content of this policy in relation to the contractual	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
		arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.	
Principle based vs rule-based requirements	Several respondents commented that the articles in the RTS translate DORA Level I principle-based requirements into rule-based requirements.	The objective of RTS, as mandated by the EU co-legislators, is to further specify (DORA Article 30(5)) the directly applicable requirements set out under DORA. The RTS is also directly applicable and binding.	No change
Transitional arrangements/Timeline	A few respondents commented that the adoption of the policy for ICT services may require financial entities to review and renegotiate existing contractual arrangements with ICT third-party service providers and called on the ESAs to provide for a grace period (up to 2 years) It was also suggested that contractual requirements should be applied only on a forward-looking basis and financial entities should be permitted to implement any new requirements upon contract renewal, rather than necessitating off-cycle remediation. Financial entities could be left with as little as 6 months to overhaul contracts which in many cases could be global group-wide arrangements with providers who are themselves outside the EU. One respondent suggested a standard for updating agreements	DORA does not foresee transitional arrangements and therefore the requirements under DORA will apply at its date of entry into force. The RTS will enter into force on the twentieth day following of its publication in the Official Journal of the European Union.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	not later than 3 years after DORA's entry into force.		
Subcontracting	Several respondents proposed to specify the rank of subcontractors covered by the requirements and limiting the rank of subcontractors concerned by the requirements.	Financial entities remain fully responsible and accountable 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.	The RTS has been clarified
	One respondent suggested specifying which provisions apply to TPP's subcontractors and clarifying whether it applies only to material subcontractors.	The RTS is addressed to financial entities. Financial entities should have a policy in place regarding contractual arrangement for the use of ICT services supporting critical or important functions provided by ICT TPSP, including their subcontractors (the ones that performs ICT services supporting critical or important function).	The RTS has been clarified
Definition of 'critical or important function'	Several respondents highlighted the need for more precise definitions, especially regarding the term "critical or important function" and suggest aligning it with existing interpretations.	"Critical or important functions" is defined under Article 3(22) of DORA and is consistent with existing definitions under the different sectoral legal framework.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Responses to questions in Consultation Paper JC 2023/35			
Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?			
Proportionality	Many respondents proposed to state more clearly how the proportionality principle may be applied. In particular, some respondents highlighted the absence of a clear definition and dedicated requirements for the principle of proportionality in the draft RTS and emphasised that proportionality should not compromise overall financial system security. One respondent suggested clarifying if the list in Article 1 is exhaustive and recommended adding language to imply that there are risks beyond the listed elements to allow financial entities flexibility in identifying risks. A few respondents suggested a more proportionate approach to consider geopolitical risks. Many respondents commented that the draft RTS suggests non-EU providers are inherently 'riskier' than EU ones and that financial entities should consider this when conducting a risk assessment. Specifically, the proposal under Article 1 of the draft RTS suggests that the location of an ICT third-party service	The principle of proportionality is already set out under Article 4 of DORA. This article explicitly sets out that the application Chapter V Section I of DORA by financial entities shall be proportionate to their size, and overall risk profile, and to the nature, scale and complexity of their services, activities, and operations. 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. Article 1 does not provide for an exhaustive list of criteria or risks to consider. However, it refers to "risks" which include geopolitical risks. The fact that financial entities may use non-EU providers is an element of risk and complexity to consider together with other risks or criteria where appropriate. The RTS has been clarified.	Article 1 has been further clarified. Article 1 has been clarified.

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	provider or its parent company is an '[element] of increased complexity or risk'. As an alternative, it is suggested to draft Article 1 in line with the approach taken under existing guidelines issued by the ESAs on outsourcing and cloud. In addition, another respondent highlighted that the current wording is contrary to the EU's commitments to provide market access without restrictions to foreign suppliers of computer and related services, which includes ICT services. Another respondent urged the inclusion of a reference to decreased complexity/risk to ensure a comprehensive application of the proportionality principle. Several respondents requested a more proportionate approach especially for smaller organisations like credit rating agencies or to introduce a discretionary leeway for entities based on their risk assessment. Several respondents proposed that strengthening the principle of proportionality could involve permitting financial entities to utilise and reference existing third-party risk management policies and procedures for fulfilling the upcoming DORA obligations.	It needs to be considered that there are situations where market access may be restricted from some countries, including that ICT services cannot any longer be received. See comments above. The RTS is addressed to financial entities. Financial entities should have a policy in place regarding contractual arrangement for the use of ICT services supporting critical or important functions provided by ICT TPSP and subcontractors (the ones that performs ICT services supporting critical or important function). The size of the entity is one of the proportionality criteria in the RTS. The RTS does not prohibit to use existing third-party risk management policies (including outsourcing) and	Article 1 has been clarified No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	Instead of setting up a new individual policy, they would welcome having the flexibility to set-up one common policy for Outsourcing and ICT and thus to have a global ICT framework in place.	it is possible to combine them as long as the policy complies with the requirements set out under this RTS and DORA and the management body remains accountable (e.g. appropriately reviews, adapts where necessary and adopts such policy).	
Proportionality and group application	One respondent suggested that contracts linked to intragroup/inter-affiliate services should be subject to a proportionate, outcomes-based application of the RTS requirement. Several respondents sought clarification on whether a group-wide policy is sufficient or if separate policies per entity/location are required.	The use of Intragroup ICT service providers is a criterion to consider for the application of proportionality. A group wide policy, adopted by the financial entities within the group, is possible but needs to take into account also specificities at individual level. The individual financial entities remain responsible to comply with the obligations under DORA and this RTS at individual level.	No change
Group application	Several respondents considered that the level of application as a group is not clearly established in the proposal. They seek further information on how consolidation should be considered by groups, especially when the parent undertaking resides outside the EU or when multiple levels of group aggregation are involved in different jurisdictions.	The requirements set out under the RTS are applicable to EU entities (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 policy should be consistent and well-integrated within the group for financial entities within the EU	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
		and their subsidiaries outside the EU taking into account local legislation.	
	A few respondents suggested using in Article 1 the term 'ICT intra-group service provider' defined in level 1 and not refer to 'ICT third-party service providers part of the same group of the financial entity'.	The suggestion has been taken into account.	The Article has been amended.
	A few respondents emphasized that the parent undertaking should not be responsible for local policy implementation.	The Parent undertaking, where applicable, is responsible at group level to ensure a consistent and well-integrated implementation of group wide arrangements. The local policy implementation responsibility belongs to the local financial entity. The requirements do not prevent FEs and groups to implement the ICT policy as appropriate and in a manner that leverages on the parent level and taking into account local level specificities.	No change
	Several respondents proposed clarifying that the group application should exclude companies within the Group that fall outside the scope of DORA, such as third-country entities or non-financial entities		No change
	A few respondents sought clarification on whether the policy applies to non-EU based	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	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	parent companies with EU-based subsidiaries or only to European entities.	continuity and availability of financial services and activities, at individual and at group level. The requirements apply both at individual level and consolidated level where applicable. For subsidiaries of EU parent undertakings located in third country, they should apply the group policy taking into account local legislation. The requirements set out under the RTS are applicable to EU entities (including parent undertakings in the EU where applicable) and do not apply to non-EU parent entities. However, for the latter, their EU subsidiaries have to comply with RTS. The RTS itself is for contractual arrangements on the use of ICT services supporting critical or important functions wherever those providers are located.	
Article 2	One respondent called for the deletion of Article 2, stating that it goes beyond DORA's mandate. One respondent asked for clarification on whether Article 2 includes subsidiaries only within the EU or also branches in the EU belonging to subsidiaries outside the EU.	This article is relevant for financial entities that are part of a group and is applicable only in this case. It is also consistent with sectoral legislations (CRD, IFD for example). The requirements set out under the RTS are applicable to EU financial entities. The application at group level does not apply to parent undertakings outside of EU that have subsidiaries that have to apply the requirements. The RTS applies also to third country branches. Those branches and subsidiaries should also take into	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
		account their group policy (set by the parent undertaking outside the EU) but have to comply with the RTS. Subsidiaries outside the EU are subject to the RTS only, where applicable, on a consolidated basis, where they are subsidiaries of an EU financial entity that has to apply the requirements on a consolidated basis.	
Question 2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?			
Art 3(1) multi-vendor strategy	Several respondents remarked that a multi-vendor strategy is not mandatory under Article 6(9), therefore it is confusing to consider the multi-vendor strategy.	The RTS has been clarified.	The article has been amended
Art 3(2) yearly review	Several respondents considered that a yearly period is too short to review the ICT policy if that entails reviewing the ICT contracts as well and suggested "regular" rather than yearly review; some requested a two or three-year review period or whenever material changes warrant a review. Several respondents suggested that a 'timely' implementation is unclear and to clarify that updates to contracts may be made in the ordinary contracting lifecycle (expiration/renewal), or that the	The review of the policy on a yearly basis is reasonable and not very burdensome in the case the policy has not changed. "Timely" means that changes made to the policy shall be implemented in a reasonable time period. It is not possible to set a single time period for the multitude of different changes that require implementation. Regarding the contractual arrangements, the comment was addressed, and the point clarified to	No change The article has been amended.

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	implementation requirement be set to three years.	indicate that implementation to the contracts shall be done as soon as possible, which provides some leeway for financial entities and competent authorities to take into account situations where a very large number of contracts would need to be updated following the review of the policy. The financial entity shall document the planned timeline.	
Art 3(2) review by governing body	One respondent suggested that the review should not be done by the governing body but by risk management and IT security units.	The responsibility to carry out this review should be with the management body in accordance with Article 5(2) of DORA. Risk management and IT security functions may be involved in the process but the responsibility to decide on the findings, needed policy or implementation changes lies with the management body.	No change
Art 3(3) methodology for determining which ICT services support critical or important functions	One respondent asked for a reference to be made to the Register of information instead. Additionally, it requested clarification on whether the ownership for such methodology was to be assigned to DORA Level I functions (e.g. risk management) or could be delegated. One respondent suggests clarifying that the 'assessment' in this paragraph also relates to the determination of which ICT services support critical or important functions.	It belongs to the financial entity to determine which function will define the methodology for determining which ICT services support critical or important functions. It could be the risk management function. It is clear from the drafting that the assessment refers to the determination of which ICT services support critical or important functions.	No change No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Art. 3(4) Specific individuals vs functions	Some respondents requested clarification that Article 3(4) refers to functions, not individuals.	This provision of the RTS refers to both. The assignment of responsibilities can be allocated to an individual or a function. Skills, experience and knowledge refer to the individuals in line with Article 5(3) of DORA.	No change
Art. 3(5) Assessment by FEs	Some respondents considered that FEs are not able to assess that TPPs have allocated sufficient resources to ensure that the FE complies with all legal requirements and should only be required to seek assurances of such. Some respondents considered that the resources of the service provider must be adequate with the contractually agreed compliance requirements with regard to the mandated services only, (not with overall compliance of the financial entity). Several respondents considered that ICT TPSPs, cannot be responsible for the FE's compliance with its own legal and regulatory requirements.	The ESAs consider that this is part of the risk assessment/due diligence that should be performed by the FE as they remain responsible to comply with their legal and regulatory requirements. The provision has been clarified and the comment accommodated. The final responsibility to comply with legal and regulatory obligations remains with the financial entities, this ensures that the services received comply with the regulatory requirements.	No change The RTS has been amended No change
Art. 3(6) member of senior management	Some respondents requested clarification of the term senior management.	"Senior management" is usually defined by sectoral directives. For example, under Directive 2013/36/EU it means: those natural persons who exercise executive functions within an institution and who are	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
		responsible, and accountable to the management body, for the day- to-day management of the institution.	
Art. 3(8) Independent review	Some respondents asked for clarification of independence, whether the service or service provider should be subject to an independent review; and whether it includes independence from both parties of the contract.	The ICT services supporting a critical or important function should be the focus of the review. Independent review means from the financial entity's internal audit or an appointed third party.	No change
Art. 3(8) confidentiality	One respondent voiced concerns that audits and reviews should not hinder the TPSP's capacity to protect confidentiality of their services and suggested wording in a recital.	The requirement for independent review is limited to use of ICT services supporting critical or important function provided by the ICT TPSP covered by the contractual arrangements. Service providers need to ensure that they protect the confidentiality of other information in line with the arrangements in place with other clients.	No change
Art. 3(8) Audit plan	Some respondents asked whether the audit requirement is the same as the audit requirement (of critical or important services) under the EBA guidelines on outsourcing; and whether a separate audit plan is expected for Third Party Arrangements. One respondent considered that 3(8) could be interpreted to mean that it imposes a mandatory audit frequency in contradiction with DORA art. 28(6).	Article 3(8) does not impose a mandatory audit frequency and does not impose to have a separate audit plan for outsourcing and third-party risk management.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Art.3(8) independent certification / pooled auditing	Several respondents considered that the requirements are not proportionate and would create duplication of audits towards ICTSPs, and asked for independent certification or pooled auditing to be allowed as recognized by DORA 26(4).	The RTS foresees the possibility for the financial entity to use its own internal audit, independent certification, or pooled audit. However, the RTS also species that financial entities shall not rely solely on certification over time.	No change
Art. 3(9) final responsibility of FE	One respondent suggested that the final liability of the FE is already set out by the level 1 at articles 28(1)(a) and 5(2)(a), therefore this provision is not needed; besides, the word 'relieve' could be interpreted to mean preventing a contractual indemnity in case of breach of contract by the TPSP.	The provisions in 3(9)(a) relate to the FE's responsibilities towards its clients (not providers).	No change
Art. 3(9)	Some respondents considered that requirements in the proposed Article 3(9)(c) and (d) are redundant with key contractual provisions under Article 30(2)(g) 30(3)(e) of DORA or with art.7(1)(d) and art.9(2) of the present RTS.	The level 1 requirements are applicable to the contractual arrangements whereas the RTS requirements specify that such contractual requirements must be stated in the ICT policy. The same holds true regarding articles 7 and 9 of the present RTS. The overall objective is to ensure that those clauses are effective and will be enforced.	No change
Art.3(9) Access	A few respondents requested that the scope of access be restricted to the extent necessary to monitor compliance with contractual arrangements. One respondent considered	The access right should be limited to the contractual arrangement related to the use of ICT services supporting critical or important function provided by the ICT TPSP. Physical access also to data centers	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	that physical access is not applicable to cloud service providers.	belonging to cloud service providers should be foreseen.	
Art.3(9) Cooperation of ICTSP with authorities	Some respondents requested clarification on how to proceed if the ICT TPSP does not agree to include such contractual provisions; or consider that this should be a legal requirement for ICT TPSPs and therefore not included in contractual clauses.	Where an ICT TPSP disagrees to include audit, information and access rights clauses, the financial entities should not enter into contractual arrangements with the ICT TPSP as they would not be able to comply with their regulatory requirements.	No change
Question 3: Is article 4 appropriate and sufficiently clear?			
Art.4(1)	Several comments point to a lack of clarity on the purpose of differentiating between providers as drafted or on the intent of the article; some respondents point to an underlying assumption that some types of providers are preferable to others.	The objective of Article 4(1) is to ensure that financial entities, as part of their risk management and as part of their risk assessment, assess the type of ICT third party service provider. For example, an ICT TPSP authorised or registered by a competent authority in a Member State are subject to a different framework compared to an unregulated ICT TPSP or an ICT intragroup service provider. To facilitate the reading and clarify the RTS, Article 4 has been removed and merged with Article 1.	The RTS has been clarified. Article 4 has been merged with Article 1.
4(1) subcontracting	Most respondents asked for clarification on subcontracting requirements, especially regarding the depth of monitoring along the subcontracting chain, with some favouring removal of the reference to subcontractors from this article to avoid duplication of	All the topics related to subcontracting (risk assessment, conditions for subcontracting, monitoring along the entire subcontracting chain, information processes, etc) raised under this consultation are addressed in detail under the RTS under DORA 30(5). It should also be mentioned that	The article has been amended

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	requirements with the dedicated RTS on subcontracting. Some called for caution as financial entities may struggle to obtain all the relevant information / determining which sub-contractors are regulated or subject to oversight could be unfeasible.	Recital 6 of the RTS stressed that the policy should also apply to subcontractors that provide ICT service supporting critical or important functions or material parts thereof to ICT third-party service providers where this is relevant in case a chain of ICT third-party service providers exists.	
4(1)(c) Third countries	Several respondents considered that a differentiation between EU providers and third country providers is not in line with DORA	See comments above. This is justified for the risk assessment and the due diligence process.	No change
Question 4: Is article 5 appropriate and sufficiently clear?			
Policy	Several respondents suggested deleting the word “procedures” from the article, because it would make the policy too granular.	The comment has been accommodated.	The article has been amended
Monitoring	One respondent pointed out that “monitoring” with regard to contractual arrangements is too broad and does not focus on key indicators.	The link with the Article 10 has been made to clarify further this article.	The article has been amended.
Material change to contractual arrangement	Several respondents requested clarification on what constitutes “new or material change to a contractual arrangement”, as an overbroad application would lead to unnecessary administrative burden for minor or routine changes, without meaningful positive impact on operational resilience. Respondents	This article foresees that the policy should set out an approval process for new third-party contractual arrangement for the use ICT services supporting critical or important functions or material changes to existing one. This provision provides sufficient freedom regarding the process, it is therefore not	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	propose to add that those requirements should only apply to changes leading to a material increase in the risk of disruption of a critical or important function. Some respondents noted that there should be no expectation that management body approval needs to be re-granted when contractual arrangements change, including the use of new subcontractors.	burdensome that a process is implemented to monitor and oversee these arrangements. Regarding the involvement of the management body Article 5(1) (d) sets out that the involvement of the management body is foreseen "as appropriate" regarding the decision-making process on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. It is therefore no required to involve the management body on a systematic basis.	
Clarification of main lifecycle phases	One respondent requested further clarification on the meaning of "main phases of the lifecycle".	The lifecycle refers to different steps that should be undertaken by financial entities regarding ICT third party arrangement for the use of ICT services supporting critical or important functions by ICT TPSP to ensure sound and effective risk management.	No change
Internal control function	Several respondents suggested to clarify "internal controls" in the context of Art. 5(1)(f), as it could refer to a 1st or 2nd line of defence function.	Internal control units are defined in the sectorial directives and usually are independent from the business they control.	No change
Clarification regarding involvement of business units	Some respondents request more clarity on the responsibilities for the involvement of business units.	The involvement of business units refers to the involvement of operational functions.	No change
Comments	**Summary of responses received**	**EBA analysis**	**Amendments to the proposals**

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Question 5: Are articles 6 and 7 appropriate and sufficiently clear?			
Information availability before entering contractual arrangements	Several respondents were concerned regarding the availability of information before entering into a contractual arrangement with an ICTSP. In addition, several respondents suggested that requiring a large amount of information upfront could slow down commercial transactions, restrict competition, as ICTSP might be reluctant to disclose such information or could negatively impact smaller ICTSP without the capacity to provide all required information.	Before entering into an arrangement with an ICT third party service provider for the use of ICT services supporting critical or important functions, a risk assessment and due diligence process has to be performed. This is part of financial entities' mandatory risk management in accordance with DORA. During this phase, ICT TPSP should provide the information necessary for those purposes, otherwise financial entities that would enter into contractual arrangements without making such assessment would breach regulatory requirements.	No change
Groupwide risk assessments	Several respondents suggested that the risk assessment (Art. 6(2)) should allow for reliance on groupwide assessments where the service recipient belongs to a third country group. In addition, several respondents noted that groupwide assessments could save resources and avoid unnecessary duplication of effort, especially when one entity purchases services for a group.	Where applicable, a group risk assessment is possible. It should take into account the specific risks to which each financial entity is exposed or might be exposed to.	No change
Role of audits in due diligence	Several respondents suggested changing the word "audit" to "assessments" in Article 7, as the use of audits in the due diligence stage of the supplier selection process would not be	Financial entities should consider certain elements in the due diligence process and one aspect is how audits are performed by the TPSP. This is important	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	feasible with currently available resources for financial entities.	for ensuring that the financial entities will continue to comply with their regulatory obligations.	
ESG principles in due diligence	Several respondents suggest deleting Art. 7(1)(e) requiring due diligence on acting in an ethical and socially responsible manner, as these requirements will be contained in more detail in the Corporate Sustainability Due Diligence Directive or exceed the legislative mandate for this RTS. Several respondents also noted that this requirement does not address DORA resilience aims.	These aspects are still very relevant in the case of ICT third party risks management. ESG risks need to be managed throughout the supply chain, including social and governance risk, that are linked to labour law, compliance with Directives in this area, e.g. Directive 2054/2006 on equal opportunities and human rights. Moreover, the European Charter of Fundamental Rights already establishes certain values that need to be complied with within the EU, such principles, including the observance of human rights need to be complied with also where FE rely on service providers and subservice providers, including such located in third countries that are not directly subject to the Charter.	No change
Unclear references in Art. 7(3)	Several respondents noted that it is unclear how the references in Art. 7(3) which point to Art. 7(1) are supposed to interact and some assumed a drafting error as consequences would be unnecessarily onerous.	All the cross references have been checked and the RTS has been clarified	The RTS has been clarified
Focus on relevant subcontracting in due diligence	Several respondents request clarification whether due diligence is supposed to focus on the relevant use of subcontractors, specific to	Due diligence to be performed by the FE concerns in particular the third-party service provider, who is responsible to perform due diligence assessments	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	the ICT service provided, rather than the use of subcontractors in general.	regarding the subcontractors, including when new subcontractors are added. The due diligence assessment should consider the risks and possible changes to risks caused by subcontracting. A specific RTS dealing with subcontracting will be developed.	
Further specification of necessary organisational units	Several respondents noted that "risk management" and "internal controls" are not organizational units as implied in Art. 7(1)(a), but rather risk management concepts.	In many FE the corresponding units are established, some may only have specified risk management and control processes and procedures in line with their sectoral legislation.	The RTS has been clarified
Risk of being affected by sanction in due diligence	One respondent believes that including the risk of being affected by sanction in due diligence poses a grave risk to international trade and may negatively impact efforts to de-risk operations as well as competitiveness. The respondent recommends removing references to sanctions.	The risk of restrictive measures (sanctions or embargo) is relevant to operational resilience as such measures may impact the ability of an ICT provider to provide the service or the ability of the financial entity to comply with its legal obligations, and therefore should be part of the due diligence actions required by the ICT policy implemented by financial entities.	The RTS has been clarified
Confidentiality of business continuity plans	One respondent noted that business continuity plans are usually highly confidential and therefore unlikely to be shared for due diligence, even under NDA. Respondent suggested to require the vendor to submit a summary of the plan or applicable certification (such as ISO 22301).	The requirement is on ensuring "the existence of risk mitigation and business continuity measures" and how their functioning within the ICT third-party service provider is ensured, not the actual BC plans themselves.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Intra-group suppliers in the risk assessment	Some respondents have stated that due diligence of intra-group service providers is not necessary, due to oversight by competent authorities and availability of audit reports.	Article 7(1) specifies that the fact that the service provider is an intra-group service provider should be considered, consequently the assessment of the different aspects can rely on already established facts. It is still to be assessed if the intragroup provider is suitable to perform the required service.	No change
Question 6: Is article 8 appropriate and sufficiently clear?			
Article 8 – general remarks	Some respondents raised questions about the relation between Article 8 and comparable provisions in other legislations and Article 28(4)(e) DORA. Another respondent indicated that article 8 should be deleted as conflict of interests management is already regulated independently in the UCITS directive, AIFM directive and MiFID II etc.	The reference to the management of conflict of interests in the policy is line with DORA and in particular with Article 28(4) of DORA that sets out that financial entities shall identify and assess conflicts of interests that the contractual arrangement may cause.	No change
Article 8(2)	Several respondents indicated that the phrase “at arm’s length” should be clarified. Other respondents indicated that it is unclear how the conditions can be specified for the intra-group services to be set at arm's length in the policy and into how much detail this should go and questioned the mandate to set out such requirement. Furthermore, financial conditions of intra group services doesn’t	The wording “at arm’s length” has been replaced and the provision in Article 8(2) clarified.	The RTs has been amended

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	seem to be the right criterion to identify possible conflicts of interests.		
Question 7: Is article 9 appropriate and sufficiently clear?			
Article 9(3) – Third-party certification use	Several respondents would like to see further clarification or even deletion of the wording in Article 9(3) concerning conditions for the use of reports/certifications and not being able to rely on only those over time, arguing that they are the most cost-efficient tool for the industry. One stakeholder proposes an ESA referential for recommended certifications.	Certifications can be used however it should not be the only measure taken to monitor the service related to the critical or important function. The ultimate responsibility lies with the FE, but to ensure the functioning of the financial market a high level of supervisory assurance needs to be ensured.	No change
Article 9(2) – Audit methods	Several respondents would like to receive further guidance whether all mentioned audit methods must be used (see 9(2a-c)), or an audit can be limited to one of the methods.	The use of the FE's internal audit or an appointed third party is mandatory. Pooled audits and certificates may be used where appropriate.	The RTS has been amended
Bargaining power between financial entities and ICT TPPs	Several respondents stress the low bargaining power of FE's regarding many of the more demanding requirements, such as demanding of additional certification or conducting penetration tests on ICT TPP systems. Some respondents refer to Article 9(3d), stressing that "ensuring" key systems and controls are covered in future reports can be difficult for untransparent services like SaaS.	All the financial industry is required to have those clauses in place, so providers must react to the EU regulation as otherwise FE cannot contract with them. Ensuring operational resilience is objective of DORA. There is an oversight mandate by the ESAs for the most critical providers. Transparency of audits or certifications need to be ensured for all services as otherwise FE cannot contract them.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Potentially ambiguous definitions/phrases	Some respondents would like to rephrase or remove terms like “signed by” and rather use neutral versions like “accessible and executed by”, to account better for modern contract practices in the ICT industry. Some also wish to add “agreed by all parties in accordance with the terms of their contractual arrangement” to Art. 9 (4). Some respondents ask for clearer phrasing on potentially ambiguous terms like “reasonable” or “legitimate”, or “material” and “all parties” in Article 9(4), “satisfaction” under Art. 9(3), “other relevant systems and controls” in Article 9(3g), “ICT testing” in Art. 9 (2) or would like to adjust phrases for instance adding “where available” to Art. 9 (2b)**.**	The contract/agreement must be “signed”. Contracts between FEs and ICT TPSPs should be traceable, which may indeed take a physical or digital form. However, “signed by” does not introduce ambiguity in this regard since Regulation (EU) N°910/2014 recognises digital signature processes. ICT testing is defined in DORA Level 1. The meaning conveyed using the words ‘reasonable’ and ‘legitimate’ is that such requests should be grounded in risk-management purposes. ‘Satisfied’ means that the FE should determine that it is able to rely on the results of its audit plan to accurately reflect the risk level of the ICT arrangement.	No change
Consistency with DORA	Several respondents note a redundancy with DORA Level 1 and a too strong focus on audit provisions compared to other aspects listed in DORA Art. 30. Several stakeholders note that penetration tests are not a requirement for all entities as of DORA, while the RTS might give this impression, creating an incoherence between level 1 and 2.	Audit provisions are important to ensure a sufficient level of control by the third line of defence. The comment has been accommodated.	No change The RTS has been amended

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Guidance on sub-contracts	Some respondents would like to receive more guidance on ICT sub-contracts and large multinational ICT TPPs, for instance when it comes to audit/access rights or pen testing and which requirements of the RTS concern also sub-contractors (for instance Article 9(4)).	Article 9(4) applies to the contract between the FE and its ICT third-party service provider. Regarding subcontracting, a separate RTS on sub-contracting will further clarify these questions. Service users should be able to conduct tests and audits on sub-contractors.	No change
Standard clauses	Some respondents would support a public initiative to develop and publish standard contractual clauses as mentioned under Art. 30 (2-4) of DORA level one.	The development of standard clauses has not been mandated to the ESAs.	No change
Specific clauses from level 1	Some respondents highlight that the stipulation in the policy of specific level 1 contractual clauses to be included in contractual arrangements will be difficult to implement for some ICT TPPs for standard IT services.	The level 1 contractual requirements are mandatory under Art. 28 and 30 of DORA.	No change
Third-party led penetration testing	Some respondents suggest adding the possibility for a third-party led penetration test in Art. 9 (2).	The RTS does not preclude or prescribe specific options regarding the way the testing is performed, without prejudice to other provisions on TLPT in the DORA framework. Please refer also to the RTS on TLPT.	No change
Question 8: Is Article 10 appropriate and sufficiently clear?			

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Article 10 – General remarks	Several respondents indicated that it would be difficult to comply with each individual financial entity's own internal security policies. Part of the sentence "*and the compliance of the ICT third-party service providers with the financial entity's relevant policies and procedures*" should therefore be deleted. The services that are provided are often standardised. Some respondents stated that it is not possible to automatically measure the indicators asked or that ICT third-party service providers should have freedom to agree the exact indicators that are assessed. Some respondents felt that the RTS should refer to the use of objectively measurable indicators.	The requirement is addressed to financial entities, not ICT providers. FEs are not forbidden from entering into arrangements with ICT providers which offer standard contracts. Independent of the character of the contract they have to be aware of the risks and assess whether their contractual clauses are in line with their relevant policies and procedures and DORA requirements. The relevant contractual arrangements specifying the measures and key indicators to monitor, are to be agreed by both the FE and ICT provider.	No change
Article 10(1)	A few respondents consider that the phrase "measures to monitor compliance" in Article 10(1) is potentially ambiguous (does it mandate audit powers beyond those already following from DORA and accompanying RTS. Clarification is requested. Respondents suggest replacing the requirement "ongoing basis" with "regular basis", more practicable.	Measures to monitor compliance' entails all measures contractually agreed in addition to the ones required by DORA. It is clear that the requirement is for FEs to define such measures contractually and implement them on an ongoing basis. "Ongoing basis" is the terminology usually used.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Article 10(2)	Respondents pointed to a lack of clarity on the content of "periodic reports" and "reports on ICT security and on business continuity measures and testing". Clarification is requested on "other relevant information" in Article 10(2)(c) and "security payment related incidents". The requirement of Article 10(2)(d) would go in the view of some respondents beyond the scope of DORA as obligations to identify ICT incidents and report major incidents do not apply to ICT third-party service providers. Several respondents requested a clarification about the review (frequency, who should do it). Some respondents have the opinion that the review and audit requirement in Article 10(2)(e) is already included in Article 10(2)(b) and therefore should be combined. The issue of interplay of Article 10(2)(e) with Article 7(3)(b) of the RTS is raised (In Article7, audits are the preferred option).	Periodic reports are reports regularly produced, usually with a monthly, quarterly, biannually or annual period. The content of such reports is expected to cover at least the volume of activity and quality of service for the referred period as well as any contractually agreed piece of information. Other relevant information may be any relevant document in the context of performance and quality standards set out in Article 10. This requirement is for FEs to ensure that they are informed of incidents. The obligation under DORA is with the FE. In line with article 9(2)a, the independent review is to be performed by the ICT TPSP's internal audit function, if established; otherwise by an appointed third party. The scope of the articles is different as 7(3)b deals with the use of audits within the due diligence process while 10(2) deals with the monitoring process.	No change
	Some respondents note that the described approach to vulnerability reporting in Article 10(2)(c) and 10(2)(d) could be problematic	Reporting of zero-day vulnerabilities is not prescribed nor precluded by Article 10 and pertains to the contractual agreement by the parties.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	because it seems to require ICT-service providers to disclose zero-day vulnerabilities.		
Question 9: Is article 11 appropriate and sufficiently clear?			
Clarity and Scope	Several respondents find Article 11 lacking clarity on whether the documented exit plan should be set up for each ICT service or each contractual arrangement, some suggested having one exit plan on each arrangement. Additional clarity is called for on the frequency of periodic review and testing; the definition of plausible scenarios, and depth of testing; timeframe of exit plan; involvement of ICT providers.	FE need to have an exit strategy. An exit plan is required for each ICT contractual arrangement supporting ICT services supporting critical or important functions, which may include several of such functions. This needs to be included in the policy. In some scenarios, towards the same service provider, exit plans related to the change of service providers may be drawn up together. The form of test of such plans is not specified. A wide range of test methods is possible. The periodicity of review of exit plan is to be defined by the ICT policy.	The RTS has been clarified
Feasibility and Testing of Exit Plans:	Numerous respondents express concerns about the feasibility of testing exit plans in real conditions, and suggest alternatives like tabletop exercises, paper-based tests, or desktop exercises. Some respondents noted that testing exit plans in real conditions when cloud services are involved would require an active contractual arrangement with another ICT	Table-top, desk-top or other exercises may be a part of exit plan testing, based on plausible scenarios and realistic conditions.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
	service provider, i.e., every solution needs to have a developed and testable alternative solution. One respondent suggested requiring testing "when appropriate".		
Exclusion of Intra-Group Providers	Several respondents argue that intra-group service providers should be excluded from the requirement for a documented, reviewed, and tested exit plan, citing reasons such as lower and different risks and closer links between the entities.	While the principle of proportionality should apply, there should not be differentiated requirements between intra-group and outside providers – such assessments still follow the principle of proportionality, e.g. a lighter assessment can be performed. Resolution scenarios need to be taken into account as they might change the group structure and ICT service provider might afterwards not be part of the group. The requirements under DORA apply on an individual basis and where applicable on a consolidated and sub-consolidated basis in accordance with Article 28.	No change
Business Continuity Planning vs Exit Planning	Some respondents request a clearer distinction and suggest that exit strategies should be limited to scenarios with longer transfer timeframes. The Proposal to use an exit plan to address operational incidents such as service interruptions or inappropriate or failed service delivery would overlap unnecessarily and inappropriately with purpose of Business BC/DR plans.	Exit may be caused by many aspects, not only operational failure, but this may be one trigger. However, there should be no confusion between business continuity planning and exit planning. Service disruptions need to be taken in to account for exit planning when they are unforeseen and persistent.	No change

Comments	Summary of responses received	ESAs analysis	Amendments to the proposals
Consideration for Cloud Services	Specific attention is drawn to the use of cloud infrastructures, especially those provided by non-EU ICT Service providers, which are not subject to EU regulation.	FE are the addressees of DORA. Non-EU ICT services providing ICT services supporting critical or important functions to financial entities are in the scope of DORA and FE shall ensure that DORA requirements are applied.	No change
Responsibility of implementation schedule	One respondent recommended clarifying that the planned implementation schedule which forms part of the exit plan is the responsibility of the financial entity which should develop it, not the ICT service provider.	The comment has been accommodated.	RTS has been amended
Market considerations and alternatives	Few respondents pointed out that in some areas of the digital services market, there are in practice few or at times no feasible alternatives. The related exit plan could therefore amount to a firm ceasing the service completely, given it is unlikely they will be able to provide such services in-house. Supervisors should take this into account when reviewing the exit plans developed by financial entities.	Financial entities must be compliant with DORA at all times.	No change
Concerns about Sharing Sensitive Information:	According to one respondent, the exit plan should not be shared nor periodically tested with ITC third party providers, especially because commercially sensitive information is included in such exit plans (estimated costs, identified alternative providers etc.)	This provision does not mandate the sharing of sensitive information and it is up to the firm to decide what information should be shared.	No change