EIOPA - IRSG

ESMA
European Securities and Markets Authority
Securities and Markets Stakeholder Group

EBA EUROPEAN BANKING AUTHORITY
BANKING STAKEHOLDER GROUP

JC 2023 35

Deadline: 11 September, 2023

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

Introduction

The Joint Committee (JC) is seeking feedback on draft Regulatory Technical Standards (RTS) which the ESAs are mandated to develop under Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, commonly referred to as 'DORA'. These draft RTS are related to the policy that shall be adopted by financial entities, as part of their risk management framework, on the use of ICT services supporting critical or important functions provided by ICT third-party service providers under empowerments in DORA Article 28(2).

The ESAs are mandated to further specify the detailed content of this policy. Article 28(2) establishes the following: "As part of their ICT risk management framework, financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, shall adopt, and regularly review, a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in Article 6(9), where applicable. 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. The management body shall, on the basis of an assessment of the overall risk profile of the financial entity and the scale and complexity of the business services, regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical

or important functions." Furthermore, Article 28(10) states that: "The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to further specify the detailed content of the policy referred to in paragraph 2 in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024."

The draft standards set out the requirements for all phases that should be undertaken by financial entities regarding the life cycle of ICT third-party arrangements management and have been developed considering 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".

Given that the DORA legislation and the RTS is cross-sectoral, the stakeholder groups of the three ESAs have accordingly sought to collaborate to prepare a joint response. Where necessary, we have identified any comments which we consider to be specifically relevant for one or more sector or type of financial entity.

General comments

We welcome the overall approach the JC has taken of setting overall principles, with further specification for specific sectors or types of entity only where necessary in the light of their activities and the associated risk profile. We consider this is likely to be both simpler to implement and more effective than trying to anticipate and prescribe in advance every detail.

We are also pleased to see that the three ESAs are working together as a single, integrated team which is necessary to deliver the regime efficiently and in a timely way, to make the best use of the available resources, and to ensure appropriate coherence in the resultant regime.

On the background and rationale point 3 states that the RTS is considering already existing specification provided in Guidelines published by the ESAs, but no specific consideration is given in the RTS to the EBA Guidelines on improving resolvability, nor to the SRB expectation for banks in what respect to operational continuity in Resolution. Critical ICT third party providers are normally also considered critical for operational continuity in resolution. A comprehensive review of the draft RTS should be made considering Resolution aspects, as such specific mention should be made on different articles of the draft RTS, in particular, art. 9 should specially mention the resolution clauses required by the resolution framework.

The RTS refer several times the "data" and "data processing" and it would be beneficial to clarify if these references should be interpreted in the context of GDPR. Furthermore, there are several regulations (DORA, EBA Guidelines on outsourcing arrangements, normative acts related to the transposition of Directive 2014/59) that cover requirements for different types of Third-Party

Arrangements (mandatory clauses in the agreement, registry requirements, due diligence, etc.). We suggest that the ESAs aim to, as far as possible, standardise and align the regulatory requirements, including further regular reporting to supervisors at both national and EU level. We are of the view that current international initiatives should be taken into consideration when developing RTS to ensure consistency with international best practices and benchmarks. For instance, the Financial Stability Board published in June 2023 a public consultation on a toolkit for financial institutions and financial authorities for "Enhancing Third-Party Risk Management and Oversight".

Answers to specific questions

Question 1: Are the articles 1 (Complexity and risk considerations) and 2 (Group application) regarding the application of proportionality and the level of application appropriate and sufficiently clear?

The articles are clear, but there is some room for further clarification. E.g. the scope of 3rd parties should be reduced in accordance with their risk level and the requirements for exit plans should be more precise. Moreover, exit plans tests cannot be conducted in real conditions and thus regular tabletop tests should be conducted instead. In addition, if the EBA guidelines on outsourcing are still valid, its interplay with these guidelines and with DORA regulation must be clarified.

Article 1 (Complexity and Risk Consideration) provides a set of elements of increased complexity and risk that should be taken into account when drafting the policy on the use of ICT services supporting critical or important functions. Proportionality is being provided to financial entities, which is useful, and complies with the mandate received. However, some of the elements might be better explained as the outcome that is sought in relation to some of the elements is not totally clear. For instance, the element that refers to the location of the ICT third-party service provider or its parent company.

Article 2 (Group application) refers that the policy on the use of ICT services supporting critical or important functions shall be implemented consistently in the subsidiaries. Although it is probably implicit that the policy should also be implemented consistently at branch level too, for the avoidance of doubt we consider that it should be mentioned explicitly in the article.

Question 2: Is article 3 (Governance Arrangements regarding the policy on the use of ICT services supporting critical or important functions) regarding the governance arrangements appropriate and sufficiently clear?

Article 3(4) refers to the fact that the policy shall ensure that appropriate skills, experience and knowledge are maintained to effectively oversee relevant contractual arrangements, but it does not specify what type of skills, experience and knowledge is actually expecting. It would be important to have more clarity as to whether these skills, experience and knowledge should have a more technical, Risk or IT nature or should be related to specialized legal knowledge in the field. Emphasis should be placed on ensuring that each line of defence has the appropriate independence and expertise to perform its intended function. It is also important to ensure that an emphasis on ICT risk management as a distinct consideration does not lead to an unhelpful disjunction between governance of ICT risk and broader operational risk given likely interdependences between them. We believe that there needs to be more investment in technical skills and training in ICT related issues and in the intersections between technical skills in ICT and policy making and supervision.

Article 3(5) provides that the policy shall foresee that financial entities assess that the ICT third party provider has sufficient resources. We consider that rather than “sufficient” it might be better to refer to “adequate” resources, considering that financial entities might have done their due diligence before entering into legal agreements with Third Party Providers.

Article 3(6) states that a particular role or member of senior management should be responsible for monitoring the contractual arrangements for the use of ICT services supporting critical or important functions. In order to guarantee minimum levels of consistency and harmonization across different jurisdictions and financial entities, we consider that it is relevant to clarify whether this role should be part of the senior management of the firm, whether it should be part of the second line of defense (and, as such, part of an independent function), the level of accountability and the set of skills that would be needed for the role.

The article goes on to say that the policy must define the reporting lines to the management body, including the nature and frequency of the documents to report. We consider that rather than the “documents to report” it should say “the information to report”. A typical problem with reporting is that information is conveyed in a way which might be meaningful for IT professionals but does not convey the impact on the business, its customers, clients or counterparties. We think it is important that this problem is recognized and addressed.

There are several regulations (DORA, EBA Guidelines on outsourcing arrangements, normative acts related to the transposition of Directive 2014/59) that cover requirements for different types of Third-Party Arrangements (mandatory clauses in the agreement, registry requirements, due diligence, etc.). We suggest that the ESAs aim to, as far as possible, standardise and align the regulatory requirements.

Question 3: Is article 4 appropriate and sufficiently clear?

Some big providers that subcontract services do not provide this information to the financial institutions, which could in practice make it difficult for them to comply with the requirement. The ESAs should duly consider whether the policy should include services subcontracted by suppliers. If in the final RTS, the obligation to include subcontractors remains mandatory, it should be specified up to what level of contracting should be included, e.g. focusing on subcontractors providing a material part of the ICT services supporting a critical or important function, whose disruption or failure could lead to material impact to the service provision.

Furthermore, subcontracting is already addressed under Article 30 of DORA, with a separate draft RTS (Regulatory Technical Standard) due later in 2023 to provide further information on the conditions which should be attached to subcontracting of services relating to critical and important services.

Question 4: Is article 5 appropriate and sufficiently clear?

The practical meaning of the term 'the involvement of business units' needs to be elaborated, so that it becomes clear what the responsibilities that the RTS is placing on the financial entities business units are.

In this context, what is meant by 'internal controls' could also be further clarified. Is the intention of the ESAs to refer to a specific function in the 2nd line of defense or 1st line of defense, or is it rather internal controls in a more general meaning?

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

The RTS may clarify that there is no expectation on firms to operationally establish a separate risk assessment as indicated by Article 6(2), or to put in place a sub-set of metrics specifically aimed at ICT

services where existing 'sectoral legislations and regulations', such as the EBA guideline on outsourcing arrangements, already require such assessments.

The inclusion of subcontractors in article 7 1 (b) adds complexity in terms of compliance with the provision, because sub-contractors may vary throughout the lifetime of the service. It may be difficult for providers to determine ex ante which subcontractors will be used throughout the lifetime of a contract.

In para 7 1 d) in the due diligence article, the term "audits" is used. To perform audits may be difficult at the point of supplier selection, so the ESAs could consider using the term "assessment" rather than "audit". Similar wording is used in Article 7(3) where the word "audits" should be replaced with "assessments".

Article 7(3)(c) reads as if each and all of the elements listed must be used as part of the process for selecting and assessing the prospective ICT TPP. It is presumed this was an inadvertent drafting error, as it would be unnecessarily onerous to require FE's to consider all of these elements. Our proposal would be to add "at least **one of** the following elements…".

Question 6: Is article 8 appropriate and sufficiently clear?

Article 8 aligns with existing guidance in the EBA guidelines on outsourcing arrangements regarding the approach to and governance of intragroup arrangements, consistently with a harmonised and outcomes-based regulatory approach.

The term "conflict of interest" and the objective of identifying conflicts of interest require clarification, in a similar vein to what would be considered appropriate measures to identify, prevent and manage conflict of interests in the policy.

Question 7: Is article 9 appropriate and sufficiently clear?

We welcome and support the approach taken in Article 9 in providing clear contractual requirements, in particular including requirements to assure access and audit rights, as these should lead to reducing the costs of lengthy negotiating arrangements with ICT third-party service providers. However, more clarity would be beneficial around whether the new requirements would only apply to new agreements entered with third-party service providers after the entry into force of the RTS or whether there is an expectation that financial entities renegotiate current contractual agreements to meet the new requirements. If the latter is expected, our experience tells that it can be a long and complex process to include clauses in existing contracts.

Article 9(3) provides that the policy shall specify whether third-party certifications and reports are adequate and sufficient to comply with regulatory requirements. We are of the view that, whenever possible, certifications should be provided by accredited bodies only and that supervisory authorities should have a role in accrediting those certification bodies to level the playing field.

Question 8: Is article 10 appropriate and sufficiently clear?

The use of the word penalty is not seen as appropriate in this context and are in the remit of competent authorities and should therefore be removed.

Article 10(1) also requires FEs to monitor ICT TPP's compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information. We recommend to

replace the term “authenticity” with “accuracy” of data and information to align with existing concepts and terminology in EU data protection law and current guidelines on outsourcing arrangements.

Question 9: Is article 11 appropriate and sufficiently clear?

There is a need for clarification on what is meant by “exit plan testing”. It would be more appropriate to perform tabletop exercises to validate the exit plan. The requirement for exit plans for each ICT service to be periodically tested may be challenging for those services where there are no feasible alternatives.

There is also a need to clarify whether or not the exit plan is to be established for each ICT service or for each contractual arrangement evaluating each ICT service separately.

Finally, exit plans should be distinguished from business continuity planning (BCP).