ESMA
Securities and Markets Stakeholder Group

EIOPA - IRSG

eba European Banking Authority
BANKING STAKEHOLDER GROUP

JC 2024 18

12 03 2024

Joint European Supervisory Authority Consultation paper on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554

Background

The Digital Operational Resilience Act (DORA) mandated the European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) to jointly develop policy instruments, including technical standards, to ensure a consistent and harmonized legal framework in the areas of ICT risk management, major ICT-related incident reporting and ICT third-party risk management for all EU financial entities.

The second batch, that is open for consultation until 4 March 2024, comprises the following:

- RTS and ITS on content, timelines and templates on incident reporting
- GL on aggregated costs and losses from major incidents
- RTS on subcontracting of critical or important functions
- RTS on oversight harmonisation
- GL on oversight cooperation between ESAs and competent authorities
- RTS on threat-led penetration testing (TLPT)

General comments

The Stakeholder Groups (SGs) welcome the opportunity to comment on the *"Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554".*

The consultation paper (CP) outlines specific policy issues in regard to the monitoring of subcontracting chains, the proportionality principle and the definition of ICT services and critical and important functions. While the CP refers to the Level 1 text regarding the latter, specific provisions are proposed in relation to monitoring of chains of subcontracting and the principle of proportionality that may both need further amendments in the final RTS.

The draft RTS applies risk management and contracting requirements to the entire ICT subcontracting chain of an ICT TPP in respect of services supporting critical or important functions, or material parts thereof. The SGs agree that this approach is appropriate, in principle, to achieve the desired high level of supply-chain transparency and accountability but note that it does not always reflect current industry practice and may be challenging to implement. In particular, it adds complexity to the risk management practices of financial entities (FEs), and may divert resources from managing material supply chain risks. For any individual FE, these drawbacks may outweigh potential benefits to risk management, at least in the near term. The SGs appreciate, however, that efforts to improve transparency and accountability throughout the ICT supply chain are likely to yield material collective benefits in the medium/long term. To the extent that this process may require, in some instances, a restructuring and streamlining of supply chains appropriate transitional provisions should be considered.

It appears unclear to what extent the application of proportionality is applied as the ESAs continue to broadly consider that: (i) all ICT services supporting critical or important functions carry the same level of risk (or importance) to an FE; and (ii) any subcontractor linked to an ICT service supporting material parts of, a critical or important function is equal regardless of their role and potential impact to the delivery of services. Some members of the SGs therefore suggest that the application of a materiality threshold in accordance with a proportionate and risk-based approach would be advisable to ensure that FEs are able to identify and monitor the material risks along the subcontracting chain, and those subcontractors whose disruption or failure could lead to a material impact to service provision. They believe that this approach would also reflect the intention in the DORA legislative text for a proportionate approach to ICT third-party risk management.

Other members of the SGs emphasise, by contrast, that any subcontractor along the supply chain could *a priori* become a 'single point of failure' and cause disruption to a critical or important function, with potentially systemic consequences. They note that it appears challenging to reliably assess in advance whether any individual part of the supply chain can be singled out as posing a 'material risk'. They believe that a holistic approach is needed and responsibility for the integrity and robustness of the supply chain should reside in one place. FEs are entrusted with the delivery of critical or important functions and should therefore assume responsibility for monitoring the integrity of the supply chain they employ. They feel that this responsibility should not be dissipated among multiple actors.

Questions for consultation

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

The SGs consider the Articles appropriate but recommend further clarification regarding the scope of application. The current text of Article 1 implies that the risks in scope apply to the entire ICT service instead of the "subcontracted ICT services supporting critical or important functions or material parts thereof", as outlined in the recitals.

Some members of the SGs are of the view that paragraph (b) of Article 1 is not proportionate. They note that Article 1(b) paragraph requires FEs to monitor their entire subcontracting chain of ICT providers. They believe that this approach is unrealistic and imposes a disproportionate burden on financial entities, and suggest that a materiality threshold should be included. Similarly, based on the definition of "subcontractor", which they consider broad, they believe that the criterion 'concentration risk ' in paragraph 1 (i) of Article 1 may be difficult to assess for FEs and suggest that a materiality threshold, or a narrower definition, should be applied.

Other members of the SGs note, by contrast, that FEs are generally free to choose their suppliers, and to agree relevant operational and contractual arrangements. It is therefore incumbent upon them to conduct appropriate due diligence to obtain adequate visibility on the structure of their supply chains, including potential dependencies and vulnerabilities. Given the complexity of systems and supplier dependencies it may be difficult to carry out a reliable assessment of materiality ex-ante.

Question 2: Is article 3 appropriate and sufficiently clear?

Article 3 requires financial entities to undertake a comprehensive risk assessment regarding the use of subcontractors by ICT TPP. While the SG agree that it is the responsibility of any FE to assess potential risks from making use of services outsourced to third parties, it is questionable to what extent FE can realistically be involved in the decision-making process of the ICT TPP. At present, especially smaller FEs are frequently faced with a limited number of large ICT TPPs who are able to negotiate on the basis of largely standardised service-level agreements that confer a significant degree of discretionary latitude to the supplier. While this situation may evolve over time, FEs may find it difficult, in the near term at least, to pass on their risk assessment and monitoring obligations down the ICT supply chain.

Paragraph (b) of Article 3(1) requires that the assessment by FEs as to whether an ICT service supporting critical or important functions may be subcontracted by a TPP to include that the TPP will be able to inform and involve the FE in the decision-making related to subcontracting. The SGs believe that notifying and/or involving FEs in the decision making related to subcontracting could be a significant challenge and may require TPPs to make substantial changes to current operational practice. It would also require FEs to demand a level of commercial detail, control and access from their TPPs that is not in line with current commercial practice. This is likely to be challenging, particularly for smaller firms, as some TPPs may simply refuse to provide the requested information. Some members of the SGs believe, therefore, that TPPs' obligations should, at a minimum, be limited it to 'informing the FEs.'

Some members of the SGs are of the view that the explicit requirement in item (c) of Article 3(1) to ensure that certain clauses of the contract between the FE and TPP are replicated in the contract between the TPP and its subcontractor could undermine the fundamental legal safeguards aimed at preserving confidentiality between, contracting parties. They are concerned that making an FE's compliance with its own obligations contingent upon having visibility, and a say, in contracts between third parties is inherently problematic. In the same vein, they argue that item (e) of Article 3(1) introduces an expectation on the part of supervisors that FEs should monitor and oversee subcontractors directly. In the absence of a direct contractual relationship between FEs and subcontractors they believe that it would be practically challenging to influence the supply chain beyond the TPP. They are of the view that this should also not be necessary and argue that FEs already implement comprehensive, risk-based due diligence processes and supplier controls to ensure that

supply chain risks are managed and mitigated, and contractual frameworks that ensure regulatory obligations cascade down the supply chain. They believe that FEs should be able to rely on TPPs governance and management of subcontractors and FEs' main concern should thus be with the TPP.

Item (i) of Article 3(1) requires an assessment from FEs on any obstacles to the exercise of audit, information and access rights by the competent authorities, resolution authorities, the financial entity, including persons appointed by them. Some members of the SGs believe that FEs` oversight should be limited to TPPs, and not include subcontractors, as the FE is not a party to the contract. They believe that it is the TPPs' responsibility to ensure that their contract with subcontractors includes adequate access rights for competent authorities.

The RTS requires FEs to monitor and oversee subcontractors directly, where possible and appropriate, which does not reflect existing practices and may have legal and practical limitations, especially for smaller FEs. Larger FEs implement comprehensive due diligence processes and contractual provisions already today to ensure the risks associated with the use of subcontractors are managed and mitigated. Requiring direct oversight over the full chain of subcontractors, however, in particular where no direct contractual relationships exist, appears taxing even for large FEs and may not be proportionate for smaller ones.

The SGs are of the opinion that further consideration of the proportionality principle should be considered regarding the criteria for risk assessments based on the materiality of the service provided by subcontractors. The SGs would welcome further clarification on potential transitional arrangements for the review and remediation for existing contracts after the date of application. Expecting the full remediation by the date of application of the RTS for all existing contracts would likely have unintended consequences. The focus should be on the most material contracts in the beginning with a certain timeframe for completion of the review and remediation after the date of application.

Question 3: Is article 4 appropriate and sufficiently clear?

The SGs are of the view that Article 4 is sufficiently clear, subject to the following comments:

- Some members of the SGs believe that further amendments may be needed in terms of appropriateness. For example, the contractual requirement to ensure the continuous provision of ICT services, even in case of failure by a subcontractor, implies that disruption of services cannot occur. The SG understand that this is not the intention of the RTS but it rather seeks to ensure that TPPs put in place measures to be able to withstand or recover from a disruptive event. Another aspect is the assessment on all risks associated with the location of a potential subcontractor. Some members of the SGs propose to emphasise that this assessment should focus on material risks instead of all risks and ask, furthermore, that the focus of the provisions is on the primary TPP to ensure it has robust governance procedures in place to monitor and oversee potential subcontractors.

- Article 4 applies contracting requirements to the entire ICT subcontracting chain of a TPP in respect of services supporting critical or important functions, or material parts thereof. Some members of the SGs believe that the RTS should only capture ICT services supporting a material part of critical functions to prevent the application of onerous requirements to some minor services supporting a critical function. Other members note, by contrast, that a holistic approach is needed to prevent

potential disruptions of critical or important function and note that even services perceived as minor could leave the relevant system vulnerable.

- Some members of the SGs are concerned that the draft RTS captures an unworkably broad scope of subcontractors and would therefore the ESAs to consider limiting the requirements of Article 4 to sub-contracting that could have a material impact on critical or important With regard to article 4 paragraph e), FEs oversight should be limited to the TPP and not to subcontractors as the FEs are not party to the contract. TPPs shall ensure that their contract with subcontractors are in compliance with monitoring and reporting obligations. Other members of the SGs believe that the RTS accurately implements the mandate set out by the co-legislators, which aims specifically at focusing FEs' attention on the transparency, integrity, and robustness of their supply chain, including subcontractors. FEs are entrusted with the delivery of certain critical or important functions.

Question 4: Is article 5 appropriate and sufficiently clear?

The SGs are broadly satisfied that Article 5 is appropriate and sufficiently clear. Some members of the SGs observe, as mentioned previously (see Q2.), that the expectation that FEs could review contractual arrangements between a TPP and its subcontractor may not be realistic. These members also argue that subcontracting arrangements are often not established at the inception of the original contract between an FE and the TPP, which poses practical challenges for FEs and in meeting the prescribed requirements when subcontracting arrangements are finalised following the execution of the original contract.

Some members of the SGs suggest, in addition, that the monitoring of obligations should focus on essential key performance indicators (KPI) that are needed for the functioning of critical and important functions. This would also mirror existing guidelines on outsourcing. They are of the view that current wording is not sufficiently clear and talks about KP more generally.

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

The SGs consider these Articles to be generally appropriate. Nevertheless, Articles 6 (3) and 6(4) appear difficult to implement. They present a significant challenge and seem to overestimate the ability of many FEs, at least at present, to effectively object or request modifications from a large (C)TPP. Furthermore, some members of the SGs suggest that it would be important to harmonise provisions with EIOPA's guidelines on cloud outsourcing and Guideline 13 on sub-outsourcing of critical or important operational functions or activities.

This advice will be published on the websites of the European Supervisory Authorities.
Adopted on 10 March 2024

[signed]	[signed]	[signed]	[signed]
Rim Ayadi Chair Banking Stakeholder Group	Michaela Koller Chair Insurance and Reinsurance Stakeholder Group	Veerle Colaert Chair Securities and Markets Stakeholder Group	Christian Stiefmueller Rapporteur