EIOPA - IRSG

ESMA
Securities and Markets Stakeholder Group

EBA EUROPEAN BANKING AUTHORITY
BANKING STAKEHOLDER GROUP

JC 2023 36

Deadline: 11 September, 2023

Joint European Supervisory Authority Consultation paper on

Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers as mandated by 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 first batch of technical standards, to be submitted by 17 January 2024, include:

- RTS on ICT risk management framework and RTS on simplified ICT risk management framework;
- RTS on criteria for the classification of ICT-related incidents;
- RTS to specify the policy on ICT services performed by ICT third-party providers;
- ITS to establish the templates for the register of information.

General comments

The Stakeholder Groups (SGs) welcome the opportunity to comment on the *"draft Implementing Technical Standard (ITS) to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under DORA (Digital Operational Resilience Act)"*.

We are of the opinion that the proposed standard templates can be used for the establishment of harmonized registers for information on the use of ICT services provided by ICT Third Party Service Providers (ICT TPPs) in order to support the sound monitoring of ICT third-party risk in the financial sector.

It is important that all legal frameworks that contain requirements on financial entities to keep registers of information about relationships with ICT-suppliers are coherent, and that they do not lead to double reporting and overlaps. Currently, both the EBA guidelines on outsourcing arrangements[1], the guidelines on improving resolvability[2] and the DORA contain such requirements. We would encourage the EBA to take a consistent approach and to assess whether some of the requirements could be altered, removed or merged to avoid that these multiple regulatory frameworks which partly target the same supplier relationships, become overly complex to apply both for supervisors and for financial entities.

The consultation paper (CP) claims to acknowledge the principle of proportionality. This, however, appears not obvious when looking at the number of data points totaling to more than 100 required attributes, far more than required for the register outlined by the EBA GL on outsourcing arrangements for instance, and where the immediate need for the requirement is not always obvious. Proportionality appears to be based solely on the number of ICT TPPs that the financial entity relies on but does not take into account other essential risk-based factors such as the size and complexity of the legal entity or the criticality of the ICT third-party service provided that are relevant to the application of proportionality based on the risk level of the ICT third-party provider portfolio. In this context, the SGs also reminds that ICT intra-group service providers are established and operate within the risk management framework of supervised groups.

Questions for consultation

1. Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?

The concept of Legal Entity Identifier (LEI) was introduced for entities to uniquely identify legally distinct entities that engage in financial transactions. The requirement to generally provide LEI for all relevant legal entities goes beyond current industry practices and fails to consider the practical challenges of procuring LEIs across extensive supply chains which often comprise multiple material subcontractors. Requiring financial entities (FE) to ensure that material subcontractors procure LEI

[1] EBA/GL/2019/02 -Final Report on EBA Guidelines on outsourcing arrangements

[2] EBA/GL/2022/01 – Guidelines on improving resolvability for institutions and resolution authorities under articles 15 and 16 BRRD (Resolvability Guidelines)

for themselves as indicated by Art. 4 (8) appears challenging given the indirect nature of the relationship with the subcontractor and contractual arrangements with the direct ICT TPP.

The ITS may clarify that for legal entities, where LEI are not available, like for individuals, the ESAs may be able to accept other means of identification, such as legal names or NACE codes at least for a transitional period.

LEI is used to uniquely identify a legally distinct entity that engages in a financial transaction (LEI identifying the parent entity plus a LEI for each of its subsidiaries). This should be aligned with the definition of services in scope, which in our view should be linked not to any ICT service - as inferred from art. 7 of the Background and Rationale section-, but only to those directly linked to financial services (i.e., in scope of EBA Outsourcing). Also, given that the LEI is voluntary, it might be difficult for financial entities to ensure that ICT service providers and material subcontractors "shall procure and maintain a valid LEI" as per Art. 4(8).

2. **Do you agree with Article 4(1)b that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?**

We agree with Article 4(1)b.

However, internationally active ICT TPP might be so large or complex that it would be unduly burdensome to identify all subcontractors alongside the ICT supply chain used for an individual critical or important service consumed by a financial entity (FE). A requirement for those ICT TPP under supervision by the ESAs to report on their subcontractors and make available that information on the ESAs webpage could be an alternative.

The proposed definition of 'material subcontractors' leads to a broad scope which may stand in contrast to a risk-based approach. The ITS scope broadly considers any subcontractor linked to an ICT service supporting, or supporting material parts of, a critical or important function as a 'material subcontractor'. In order to better capture 'material' subcontractors, we propose that the scope should instead be limited to subcontractors providing a material part of the ICT service supporting a critical/important function, whose disruption or failure could lead to material impact to service provision.

3. **When implementing the Register of Information for the first time:**

   - **What would be the concrete necessary tasks and processes for the financial entities?**
   - **Are there any significant operational issues to consider?**

   Please elaborate.

Pursuing a harmonized reporting model across member states through development of the DORA register will improve the quality, reliability and comparability of FE information on their third-party relationships.

The establishment of a register of information should ideally leverage on existing information kept in similar registers to reduce unnecessary burden for the reporting entity.

The identification and sourcing of the information required in accordance with Art. 4(4) ITS may take substantial time and efforts, particularly at consolidated level or more complex institutions. A 1-year implementation window may be challenging for entities that use the services of a large amount of ICT TPP, incl. the collection of information on material subcontractors. Consequently, a longer transition period for implementation, similar to the two-year transition period which was allowed under the EBA GL on outsourcing arrangements is recommended.

In light of the above, the ITS should clarify to what extent this register of information may replace or complement information requirements of the EBA GL on outsourcing arrangements and existing requirements from competent authorities (CA), such as the SSM. We are of the opinion, that the envisaged register of information should serve both requirements, since ICT and outsourcing services are very similar in many aspects. Following the principle of proportionality, any register for non-critical services should be limited to essential details of the contract like the parties concluding the contract and the subject matter of the contract.

The challenge would also be how to align with EBA Outsourcing Register, when the scope is different. Also, firms have already invested in developing the EBA Outsourcing Register and cannot leverage this effort if now firms need to follow specific templates. The proposed solution might be to leave existing financial entities subject to the EBA GL to add to their existing Registers a second layer identifying ICT service providers included in the supply chain of functions falling in scope of outsourcing.

4. Have you identified any significant operational obstacles for keeping information regarding contractual arrangements that have been terminated for five years in the Register of Information?

No comment.

5. Is Article 6 sufficiently clear regarding the assignment of responsibilities for maintaining and updating the register of information at sub-consolidated and consolidated level?

The Article lacks sufficiently clarity as regards the assignment of responsibilities for maintaining and updating the register of information at sub-consolidated levels.

Furthermore, it vaguely refers to "all financial entities part of the group", and if we think about certain companies and their US based central Headquarters, it seems difficult that the "ultimate parent company undertaking" takes the lead on defining the scope of consolidation and sub-consolidation for the purposes of this EU Regulation.

6. Do you see significant operational issues to consider when each financial entity shall maintain and update the registers of information at sub-consolidated and consolidated level in addition to the register of information at entity level?

If centrally operated and consolidated, there should not be operational issues at different entity or consolidation levels. The SGs acknowledges that not all groups may operate central systems though. In such cases, timely alignment and updating of registers kept at different entity levels may lead to operational issues.

Article 4 (3) requires financial entities to update the information contained in the register of information on an “on-going” basis. We point to the important role of an ICT Third Party Risk

Strategy. Financial entities shall, based on the risk profile of their ICT third party providers, define in which intervals the documentation shall be updated. When setting the intervals, FEs shall take into account the reporting intervals to competent authorities as set forth under Article 9.

Furthermore, we highlight that the ITS establishes uniform templates for the register of information. Thus, it opposes the provision in Article 9 that competent authorities shall – in addition to these uniform templates - set out appropriate formats for reporting purposes. We advocate that the format as set forth in the ITS shall be used to forward information to the competent authorities.

Finally, it is complex to apply in multinational groups with entities based outside of the European Union and with multiple legal entities operating different business lines. In addition, based on our experience with the EBA Register, it is operationally complex to identify a "contractual reference number" that allows to establish the linkages with other entities within the same group and external service providers.

7. Do you agree with the inclusion of columns RT.02.01.0041 (Annual expense or estimated cost of the contractual arrangement for the past year) and RT.02.01.0042 (Budget of the contractual arrangement for the upcoming year) in the template RT.02.01 on general information on the contractual arrangements? If not, could you please provide a clear rationale and suggest any alternatives if available?

It appears not immediately obvious why this information is needed for the purposes of monitoring and supervising activities as regards digital operational resilience. There is no direct link between expenses and budget for the assessment of criticality of the services provided by ICT TPPs. In case of intragroup outsourcing services, budgeting of such expenses is typically fully embedded in the annual process at the legal entity level and cannot necessarily be compared to the costs of using an external ICT TPP. We, therefore, consider that it should be one or the other, but asking for both seems to duplicate the work and it is quite cumbersome.

8. Do you agree that template RT.05.02 on ICT service supply chain enables financial entities and supervisors to properly capture the full (material) ICT value chain? If not, which aspects are missing?

The objective of the template is to identify existing dependencies on ICT service supply chains. Nevertheless, it is unclear to what extent the ranking of subcontractors provides meaningful information for any of the stated register objectives. Identifying if a subcontractor is a 4th or 6th party shall not change oversight or supervision of supply chains. In our view, it is important that the register differentiates between (i) direct third parties and (ii) material subcontractors for the purposes of supporting effective risk management and oversight. Please also see our answer to Q2 regarding material subcontractors.

9. Do you support the proposed taxonomy for ICT services in Annex IV? If not, please explain and provide alternative suggestions, if available?

Annex IV captures several ICT services that are unlikely to present material or systemic risks to some financial entities, however the vast majority of data points still apply which may result in overly broad reporting requirements and scope. It is therefore appropriate that financial entities take a proportionate and risk-based approach to the reporting requirements based on the level of risk associated with a given service, without introducing a standardized classification of risk that would impact a financial entity's risk assessment.

In addition, the proposed taxonomy includes a number of categories which should not be classified as ICT services and are, therefore, inconsistent with the definition of ICT services in the Level 1 text.

Therefore, we believe that it should be left open following the approach of art. 3.21 of DORA, specifying the scoping criteria rather than including a closed list. This way there could be more flexibility to align with the scope of EBA outsourcing.

10. Do you agree with the instructions provided in Annex V on how to report the total value of assets and the value of other financial indicator for each type of financial entity? If not, please explain and provide alternative suggestions?

It appears not immediately obvious what the relevance of this information for the purposes of the register or broader digital operational resilience is (see Q7).

11. Is the structure of the Register of Information clear? If not, please explain what aspects are unclear and suggest any alternatives, if available?

Article 3(1)(b) provides that: "*when filling-in the register of information financial entities shall complete each data point with a single value. If more than one value is valid for a specific data point, the financial entity shall add an additional row in the corresponding template for each valid value"*. This approach may increase the number of rows exponentially and make it difficult for FEs to generate the report, and for those reviewing the report. We recommend the structure of the templates is amended to allow FEs to separate multiple values with a semi-colon in order to minimise the number of rows.

12. Do you agree with the level of information requested in the Register of Information templates? Do you think that the minimum level of information requested is sufficient to fulfill the three purposes of the Register of Information, while also considering the varying levels of granularity and maturity among different financial entities?

As indicated in the reply to question 7, it appears not immediately obvious why certain information is needed for the purposes of monitoring and supervising activities as regards digital operational resilience. To the contrary, it seems that important information for the risk assessment of ICT third-party risk by the financial entities, is not requested, such as the number of incidents that happened at the ICT TTP, whether they conform to all regulatory provisions governing ICT risk or whether the (external) auditor had any findings on ICT risk management.

Furthermore, the we are of the opinion, that some references require a more thorough definition, such as:

- RT.02.02.0130: identification of level of sensitiveness of the data stored or processed by ICT third-party providers. Rather than classifying sensitiveness as "high, medium, low", it should be tied to existing concepts of sensitive data, such as the GDPR
- RT.08.01.: "easy, difficult, highly complex" reintegration of contracted ICT services

13. Do you agree with the principle of used to draft the ITS? If not, please explain why you disagree and which alternative approach you would suggest.

Unclear what the question refers to.

14. Do you agree with the impact assessment and the main conclusions stemming from it? In addition to the consultation questions above, for each column of each template of the register of information, the following is asked:

a) Do you think the column should be kept? Y/N

b) Do you see a need to amend the column? Y/N

c) Comments in case the answer to question (a) and/or question (b) ”No”