

8 October 2025

Sped n. 62/25

**Re: AMF Italia response to the “EBA Draft Guidelines on the sound management of third-party risk”**

**Question n. 1: Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?**

As a general remark we would like to underline that the boundary between ICT and non-ICT arrangements remains ambiguous, which may result in inconsistent interpretations and applications by financial entities. It is therefore essential that the EBA provides a clearer delineation of which agreements fall within the scope of these Guidelines and which are instead subject to the provisions of DORA.

In particular, the criterion used to determine whether an agreement is ICT-related or non-ICT, as described in the ESAs Q&A “DORA030 – 2999” and referred to in footnote 42 of the Guidelines, does not fully address the issues arising from the decision made by the financial entity regarding more complex existing agreements that encompass a variety of services and activities.

For such agreements, once the financial entity has determined whether to classify them as ICT or non-ICT (and therefore whether to subject them to the DORA framework or to the Guidelines), various risk management scenarios may arise (pre-contractual, monitoring, strategies, etc.). For instance, in the event of an ICT-related incident, the competent authority could observe that a “complex” agreement—mainly involving non-ICT services but also including ICT services supporting a CIF—has not been managed under DORA requirements, leading to findings of omissions in the register.

Therefore, in the case of complex agreements, it would be helpful for financial entities if the EBA were to provide a clearer position, explicitly stating that when the non-ICT service is relevant (and thus essential), DORA should not apply; or, alternatively, clarifying that the mere inclusion in the agreement of an ICT service supporting a CIF, even if not material, brings the entire agreement within the scope of DORA.

Furthermore, with respect to the scope of the draft Guidelines, we kindly request the following clarifications:

- In the case of a banking group where the parent company qualifies as a significant credit institution, should subsidiaries that are prudentially consolidated — but not explicitly listed among the addressees of the Guidelines — also fall within the scope of application? For instance, intermediaries under Article 106 of the Italian Consolidated Banking Act (TUB) or asset management companies, given that, unless we are mistaken, only branches are expressly mentioned in the draft Guidelines.

- In light of the definitions of “Third-party arrangement”, “Third-party service provider” and “Intra-group third-party service provider”, is it correct to consider agreements between branches of an EU credit institution and/or between the parent company and an EU branch of a European credit institution as out of scope of the draft Guidelines?
- In the event that the Guidelines also apply to the agreements referred to in the previous point, and without prejudice to the principle of proportionality, is it correct to assume that such agreements would be subject to the full application of the Guidelines, or would certain derogations apply.
- Is it confirmed that the distinction between outsourcing and purchasing is not relevant for the draft Guidelines and that, therefore, both types of agreements fall within their scope of application under the same terms?

Finally, we would like to highlight the need for closer alignment with the BRRD framework regarding the concept of a “critical or important function.” While the Guidelines indicate that the definition also includes “critical functions” as defined in Article 2(1), point (35) of the BRRD, we note that certain differences exist between the respective taxonomies (see SRB Guidance on the Critical Functions Report: “*the reporting requirements for CIR 2018/1624 template Z 07.01 “Critical Functions” rows 0160-0240 (Payment, Cash, Settlement, Clearing, Custody)*”).

**Question n. 2: Is Title II appropriate and sufficiently clear?**

In the current Italian regulatory framework, above all, the principle of proportionality is anchored to the size of financial institutions, whereby larger and more complex entities are required to establish more robust governance and control arrangements compared to smaller and less complex institutions.

At the same time, proportionality is calibrated to the risk profile associated with the outsourced activity: within the scope of outsourcing, only functions classified as Critical or Important Functions (CIFs) are subject to enhanced safeguards (e.g., monitoring of subcontracting chains, notification of material changes).

In light of the above, we note that the draft Guidelines under consultation extend the scope of application to **all** ongoing arrangements with third parties supporting critical functions. Moreover, section 11.2 provides that the risk analysis of such arrangements (including the scenarios of possible risk events) must be carried out in the same manner, regardless of whether the service provided qualifies as a CIF or not (with the exception of subcontracting referred to in paragraph 77).

The most critical aspect, however, concerns the contractual phase, where the strengthened safeguards that, in the previous Guidelines, were limited to the outsourcing of CIFs, are now extended indiscriminately to all contracts (see paragraph 85).

In our view, these extensions undermine the fundamental principle of proportionality, whereby only CIFs were previously identified as activities requiring the most stringent safeguards. In practice, institutions would be required to treat all third-party agreements with the highest level of scrutiny and conduct equally thorough risk analyses for all contracts. This would equate agreements worth tens of millions of euros with those worth only a few thousand euros.

We therefore consider it appropriate that EBA:

- define objective parameters for risk assessment;
  - require institutions to classify in-scope agreements on the basis of such parameters, allocating them to 2–3 categories of increasing risk;
  - set differentiated requirements regarding safeguards and reporting of contractual changes, in line with the assigned risk category.
- With reference to paragraph 32, since the work performed by the Financial Stability Board (FSB) and the Basel Committee on Banking Supervision (BCBS) have been considered in defining the Guidelines, in our opinion it should be amended to match what it stated in the FSB toolkit on third-party risk management published in December 2023: *“In line with the approach set out in Chapter 1, for the purposes of the toolkit, regulated financial institutions, to the extent they are engaging in financial services transactions, such as, correspondent banking, lending, deposit-taking, provision of insurance, clearing and settlement, and custody services, are generally not considered third-party service providers, and the financial services they provide are not in the scope of third-party service relationships. While these financial services might be objectively critical for any financial institutions that rely on them, the risks they raise are addressed through other, often more specific financial regulatory and supervisory frameworks.”*.
- We request confirmation that the exclusion of market information data services (Bloomberg, Moody’s, S&P, Fitch) from the list of functions outside the scope of application in paragraph 32 of the draft Guidelines is due to the fact that such information providers have been migrated into the ICT framework and are therefore included in Annex 3 of Regulation (EU) 2024/2957.
- Paragraph 33 states that each entity defines which services/processes/functions should be considered as CIFs, and subsequently applies stricter requirements also to any relevant third-party providers. However, paragraphs 34 and 37 appear to reverse this order: if a financial entity outsources operational tasks related to internal control functions to a TPSP, it should always consider such tasks as CIFs—effectively allowing the third-party provider to determine whether the internal function is CIF or not. We therefore request that paragraphs 34 and 37 be amended to align with paragraph 33, leaving the responsibility to define the CIF or non-CIF nature of services/processes/functions with each financial entity.

**Question n. 5: Is Annex I, provided as a list of non-exhaustive examples, appropriate and sufficiently clear?**

- As stated in the Guidelines, Annex I contains a table of certain functions “*covered by the third party agreement*” or “*categories*” under which the “*third party arrangements*” could fall, which can be used by financial entities as an example when compiling the register. Consequently, Annex I should not be a “*Non exhaustive list of functions that could be provided by a third-party service provider*” but a “*Non exhaustive list of categories under which third party arrangements could fall*”; we suggest therefore to change the title of Annex I accordingly, in order to avoid any conflict with paragraph 32 of the Guideline and European laws/regulations/Guidelines already addressing what is permitted/not permitted with reference to the delegation of a certain function.
- In Annex 1, among the functions falling under the “Lending” category and which may be covered by agreements with third parties, there appears “Client acquisition, sales and origination.” Since this service has never been considered outsourcing, we request clarification on how this aligns with credit brokerage agreements and distribution agreements.
- We request clarification on the distinction between the category “administrative services” in Annex I and the activities excluded under point 32 of the Guidelines.
- We kindly ask EBA to confirm that, even if “depository tasks” are included in Annex I, their delegation will still be regulated by their applicable specific regulatory provisions.