ABI Associazione Bancaria Italiana

ABI response to EBA consultation on Draft Guidelines on the sound management of third-party risks (EBA/CP/2025/12)

October 2025

POSITION PAPER

2025

The Italian Banking Association (ABI) would like to thank the European Banking Authority (EBA) for the opportunity to comment **the Draft Guidelines on the sound management of third-party risks**.

ABI's views on specific aspects of the EBA proposal are set out in the responses to the following questions.

***

Question no. 1: are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?

The scope of application of the Guidelines is deemed as not sufficiently clear considering that:

- the boundary between ICT services, subject to DORA, and NON-ICT services continues to be decidedly uncertain and blurred;
- it is necessary to define more precisely the criteria for identifying supplies which, in view of their low level of risk and the consequent application of the principle of proportionality, may be excluded from the scope of application of the Guidelines.

Regarding the first point, it is essential to clarify the boundary between ICT services – which are therefore subject solely to the DORA Regulation regardless of whether they are outsourced or not, and whether they are services supporting a critical or important function – and NON-ICT services, which would therefore be subject to the new EBA Guidelines. This need stems from the fact that the proposed Guidelines further exacerbate the interpretative and application uncertainties arising from an already overly vague and uncertain definition of "ICT service" introduced by the DORA Regulation and the resulting Implementing Regulations (EU No. 2024/2956), which has been repeatedly highlighted by various financial institutions to the competent authority.

This is also in light of the fact that these Guidelines expressly state that "where for the provision of a non-ICT service, the arrangement with a third-party service provider also implies the use of ICT services as defined under Article 3(21) of DORA, it belongs to the financial entity to determine whether the use of ICT service is material for the provision of the services under the third-party arrangement and therefore triggers the application of DORA framework in lieu of the present Guidelines. See also ESAs Q&A DORA030.". ABI also underlines that DORA does not provide requirements for the management of risks other than ICT risk and these GLs do not regulate the ICT risk. Consequently, the alternative application of one of the two frameworks does not cover all possible relevant risks. Now, if the boundaries between the two categories of services (ICT on the one hand and NON-ICT on the other) are not clarified sufficiently precisely, there is a risk that each financial institution will qualify them at the limit of its discretion.

Therefore, given the above uncertainties, in the absence of intervention (regulatory or interpretative) on the definition of ICT services provided by the DORA Regulation, it is at least necessary that the boundaries between ICT and non-ICT services be clarified in detail in the Guidelines under analysis; limiting oneself to the assumption that anything not subject to the DORA Regulation is NON-ICT, in a context of uncertainty as to what is

subject to the DORA Regulation, represents an obstacle to correct classification by financial entities and the Authorities themselves.

With regard to the second aspect highlighted in the introduction, the decision to extend the Guidelines to all NON-ICT supplies (with specific exceptions): the risk is that supplies which - by their nature, value or impact – do not pose a risk to the operational resilience or financial stability of the entity will also be subject to regulatory requirements; the Authority itself acknowledges in the document (page 66) that the assessment of the "criticality or importance" of the function entrusted to third parties involves elements of subjective judgment.

For this reason, ABI particularly welcomes the option granted by the proposed Guidelines to apply the principle of proportionality already when identifying the supplies subject to the Guidelines (paragraph 32(f) of Title II, Chapter 3), allowing for their non-application to relationships whose risk is irrelevant in relation to the resilience of the financial entity. ABI sees opportunities to strengthen proportionality further in areas such as contractual requirements and the register. Requirements should also be risk-based. For example, the full set of requirements for a third-party provider supporting a critical or important function should not apply where the provider's failure would have no or only minimal impact on the function (e.g. administrative support to the process). More broadly, a common understanding is needed of which types/products/categories/groups of services should fall within the scope of the GLs, and which, due to the nature of the service and the risk involved, should in principle be excluded. Additional exclusions, or "whitelisting" are necessary.

Otherwise, the concrete application of this principle of proportionality remains somewhat vague and left to the self-assessment of individual entities, with the risk of inconsistent application and regulatory uncertainty. Given that the principle of proportionality determines the same scope of application as the Guidelines, it would be appropriate to provide more specific and operational criteria for its application, also to avoid approaches that are too formal or, conversely, excessively discretionary and that could lead to contradictions in the application of this principle across the financial sector. It is therefore suggested that specific drivers (as not exhaustive examples: short term arrangements, contract value not exceeding a specific threshold) be identified to guide financial entities in qualifying agreements that have a real impact on their operational resilience and business continuity.

The Guidelines also modify the concept of essential or important function, which becomes 'critical or important function', borrowed from the DORA Regulation. With a view to guiding financial entities, ABI suggests that such definition be better qualified since it still contains some uncertainties.

Still with regard to the definition of "critical or important function", ABI notes that the definition and its related footnote are not fully aligned with the definition of critical or important functions under recital 17 of the document (included in the "Rationale and objective of the Guidelines" section), which adds the following wording: "However, the definition of 'critical or important function' in these Guidelines encompasses the 'critical functions' as defined in Article 2(1) point (35) of BRRD".

With regard to entities subject to these Guidelines, issuers of ARTs (Asset Referenced Tokens), as referred to in the MiCA Regulation (EU No. 1114/2023), have also been correctly included. On the contrary, the exclusion of crypto-asset service providers (CASP) (pursuant to Article 3(15) of MiCAR) represents an unjustified difference in treatment compared to entities included in the scope of application of the Guidelines that provide services for crypto-assets.

For example, where a bank provides crypto-asset services, contracts with third-party suppliers entered into by the bank in relation to services governed by the MiCA Regulation would be subject to DORA (if ICT) and the Guidelines (if NOT ICT); otherwise, other entities authorised to provide crypto-asset services would be subject to DORA regulations in the case of signing an ICT service provision contract, while they would not be subject to the Guidelines in the case of providing a NON-ICT service, resulting in inconsistent treatment and application of the two regulations, contrary to the purposes of the Guidelines in question. In addition, with regard to the subjective scope of application, without prejudice to the principle of application on a consolidated and sub-consolidated basis for financial groups under these Guidelines, it is hoped that the Authority will provide more detailed guidance on the management and obligations relating to intra-group service providers, including in terms of registration, due diligence and exit strategies (see Title I, Chapter 2).

Furthermore, specific guidelines are needed to ensure uniform management of third-party suppliers on a consolidated basis, so as to facilitate intermediaries in implementing internal organisational solutions and management strategies that enable them to monitor third-party risk more effectively.

With regard to the transitional period (two years from the publication of the final version of the Guidelines) for the adaptation of contracts, ABI is in favour of its application for the overall adaptation to the provisions, given the need to reassess the scope of the contracts to be subject to the new Guidelines. Nevertheless, considering the potential volumes expected for non-ICT contracts to be adjusted, we believe it would be essential to differentiate the transitional period based on the type of contracts within scope. Specifically, we propose a two-year period solely for contracts that have already been recorded as outsourcing arrangements, and a longer period for the remaining types of contracts.

Concerning the review period for third-party arrangements involving critical or important functions - particularly paragraph 19 - ABI stresses that a 2-year period to review and remediate all existing third-party arrangements in scope of these Guidelines would pose significant challenges, particularly in light of the DORA experience. Particularly for new entities in scope, such review process requires substantial changes in succession of process steps and the related internal policy framework, as well as considerable resources and staffing; the short timeline proposed in the draft Guidelines risks causing operational disruption and increased compliance costs. ABI therefore recommends an extended deadline for implementation of all third-party arrangements.

Finally, some specific remarks are as follows:

- The draft Guidelines apply to third-party arrangements, defined as arrangements "between a financial entity and a third-party service provider […] for the provision

of one or more functions to the financial entity". However, throughout the Guidelines occasional references are made to third parties that support critical or important functions, namely in par. 24 of the background and rationale section and in section 12.1 of the draft Guidelines. The concept of "support", which in ABI's understanding comes from the DORA framework, is not defined in the document and is not included in the definition of third-party arrangements itself; using it therefore entails the risk of broadening excessively the scope of application of the Guidelines and/or the scope of the requirements on critical and important functions;

- In accordance with the sections 'Addressees' and 'Management of third-party risks by financial entities within groups and institutions that are members of an institutional protection scheme' (par. 25), the question arises whether a parent company of a banking group must also include its prudentially consolidated subsidiaries within the scope of these Guidelines, despite the subsidiaries not being explicitly mentioned among the addressees of the Guidelines (these are, in fact, asset management companies, investment firms, financial intermediaries, and insurance intermediaries).

Question no.2: is Title II appropriate and sufficiently clear?

Paragraph 32 identifies which functions, at a general level, are excluded from the application of the Guidelines, including 'the acquisition of services that do not have a material impact on the financial entity's risk exposure or operational resilience.'

First of all, 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 ABI's opinion such paragraph should be amended to match what it stated in the FSB toolkit on third-party risk management published in December 2023 [1].

Furthermore, ABI deems important to further elaborate the wording of the exclusion contained in paragraph 32(f), i.e. 'the acquisition of services that do not have a material impact on the financial entity's risk exposure or operational resilience.'

The above exclusion essentially consists of introducing a concept of proportionality when qualifying the contractual relationship with the third-party supplier (extra-group or intra-group) and the possibility of excluding from the application of the obligations set out in the Guidelines under consultation all relationships that, in fact, have no impact on the financial entity's risk exposure and operational resilience.

[1] "*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.*".

ABI supports introducing a principle of proportionality when qualifying the contractual relationship that considers the riskiness and value of the supply.

In this regard, in order to clarify the scope of application in relation to the principle of proportionality, it is suggested that the list of exclusions given as examples in paragraph 32(f) be supplemented with the following closing provision: "and, in general, all supplies, attributable to any service, which, based on the operational resilience risk assessment methodologies adopted by the intermediary, do not have a material impact on the institution's risk exposure or operational resilience".

In case such aforesaid suggestion would not been accepted, still with reference to par. 32, ABI would ask clarification about why

- the "market information services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch)" have been eliminated from arrangements that should not be considered as outsourcing (see par. 28, lett.b) of current Guidelines on outsourcing arrangements EBA/GL/2019/02), and
- the "goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line)" have been eliminated from arrangements that should not consider as outsourcing (see par. 28 lett.g) of EBA/GL/2019/02)?
-

These eliminations impact the scope of the agreements to be evaluated: ABI propose to reintroduce such references.

Question no. 3: are sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?

With regard to Section 6 (Third Party Risk Management Policy – Policy Content Requirements – Planning Paragraph), the first step should be the identification of the activities that fall within the scope of the agreement. In order to avoid carrying out a new and recurrent full third parties assessment, the Guidelines should introduce the concept of continuous monitoring, indicating the time limits and criteria for the necessary TPSP -Third Party Service Provider - assessment (e.g. the financial entity must carry out an initial risk assessment and a new risk assessment in the event of material regulatory changes or changes introduced to the service – see the section "Change management and supervision").

With regard to Section 7 paragraph 53 (Conflicts of interest), ABI deems that the Guidelines should clarify what exactly is meant by "material" conflicts of interest.

Furthermore, in section 10 regulating the financial entity's obligation to maintain and implement a register of information for its contractual agreements, both individually and at a consolidated level, the Guidelines encourage financial entities to merge both ICT and non-ICT supplies into a single register, aligning the contents with the DORA Register.

In this regard, it should be noted that paragraph 61 requires financial entities to keep information relating to contractual agreements with third-party suppliers in the register, together with the relevant supporting documentation, for an appropriate period of at least five years. Regarding the retention of information on agreements concluded, within the

scope of DORA, EU Implementing Regulation No. 2024/2956 has eliminated the above obligation compared to the previous draft. This would create unequal treatment between ICT and non-ICT supplies, resulting in a misalignment between the two registers, which would appear to be contrary to the intention of uniformity of the Guidelines under consultation. In conclusion, ABI would ask to remove the abovementioned provision.

Considering the provisions of point 63 of the Guidelines, the third-party register should be compiled for all providers. However, in order to avoid overburdening the information collection process and in line with the proportionality approach outlined in point 23, ABI would request that consideration be given to limiting the inclusion in the register to only those third parties that support critical or important functions, as identified through a risk-based analysis.

This approach would allow the application of the same evaluation and analysis criteria (risk assessment, due diligence, pre-contractual analysis) to the register as those required for critical or important functions, while ensuring a proportionate and coherent management aligned with the relevance of the provider to the financial entity.

Question n. 4: Is Title IV of the Guidelines appropriate and sufficiently clear?

With regard to Section 12.2 (Access, Information and Audit Rights – Key Requirements – Risk-Based Audits), ABI suggest better specifying that risks that can trigger audits should be identified before the contract is signed.

That said, the process outlined appears overall detailed but excessively rigid. In particular, the requirement to include standardised contractual clauses (e.g. access rights, audit, exit strategy) may prove non-negotiable with global providers, thereby partly hindering banks' access to strategic technological solutions.

With regard to relationships with third-party providers and sub-contractors, ABI proposes that the Guidelines include a safeguard clause for cases in which, despite the presence of contractual obligations and adequate monitoring arrangements, the bank does not receive timely communication of material changes to the conditions and requirements of the service as defined by the Guidelines. In such cases, the intermediary should be able to document the event, implement risk mitigation measures, and notify the Competent Authority, without incurring automatic or strict liability.

With reference to point 115 of the Guidelines, which states that financial entities should ensure, on an ongoing basis, that third-party arrangements meet adequate performance and quality standards, ABI proposes to clarify that such monitoring obligations should apply exclusively to third parties supporting critical or important functions, as identified through a risk-based analysis. This approach would be consistent with the principle of proportionality expressed in point 23 and would allow monitoring activities (such as reporting, performance evaluation through KPIs/KCIs, self-certifications, independent reviews, etc.) to be focused on providers that play a significant role in the financial entity's operational continuity, thereby avoiding excessive burdens for non-critical third-party arrangements.

With regard to the Exit Strategy, the requirements outlined in points 118 and 119 appear to be overly specific and, in certain cases, not practically implementable particularly when referring to third parties with which the bank has full outsourcing arrangements. For smaller institutions, developing exit plans with the level of detail required would necessitate direct engagement with alternative providers, including requesting formal quotations that would need to be periodically reviewed. This process could entail significant operational and financial burdens, making it difficult to implement in a sustainable manner.

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

Annex I contains a table of certain functions, which can be used by financial entities as an example when compiling the register.

The list provided in Annex I includes two types of services that could be provided by third parties, namely "Secretarial services" and "Travel and entertainment services" that fall under the functions that are explicitly excluded from the scope of the draft Guidelines as per Paragraph 32(f):

"the acquisition of services that do not have material impact on the financial entities' risks exposures or on their operational resilience (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators)".

The list needs therefore to be amended accordingly to ensure consistency with Paragraph 32(f).

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 appears not to be a "Non exhaustive list of functions that could be provided by a third-party service provider" but rather a "Non exhaustive list of categories under which third party arrangements could fall"; ABI suggests therefore changing the title of Annex I accordingly, in order to avoid any conflict with paragraph 32 of the Guidelines and European laws/regulations/guidelines already addressing what is permitted/not permitted with reference to the delegation of a certain function.

In addition, introducing a whitelisting of riskless or specific services would be beneficial, which could encompass, among other services, the engagement of law firms, regulatory related services, office premises, memberships, office supplies and administration, energy and infrastructure, HR-related services, etc.

Under the premise that the Guidelines explicitly state that "This list is to be used for classification by financial entities and should only be considered as a list of non-exhaustive examples. Financial entities are encouraged to maintain their own classification rather than using those examples set out in the Annex, if more relevant or appropriate", and that

therefore this list should not be considered exhaustive or binding, as entities themselves may use any type of classification they deem most appropriate for their business, ABI would nonetheless seek clarification as to the two following aspects:

- the payment services and the investment service are always functions not ICT DORA
- how the service "Client acquisition, sales & origination" differ from product distribution agreements.