Sella
Piazza Gaudenzio Sella, 1 - 13900 BIELLA (BI)

Biella, 7 ottobre 2025

Feedback on the proposal of EBA *Guidelines on the sound management of third-party risk*.

Introduction

The Sella Group supports the proposed regulatory intervention, insofar as it standardises the management of risk arising from the use of third-party suppliers, simplifies the frameworks based on the distinction between ICT and non-ICT services, and removes the regulatory relevance of the concept of outsourcing. However, extending the Guidelines to almost all non-ICT supplies excessively broadens the scope of application. For this reason, we request that the boundary between ICT and non-ICT supplies be clearly defined (as there are still uncertainties in interpretation) and that the criteria for applying the principle of proportionality be specified from the supply identification stage (which we hope will also be recognised in relation to ICT supplies). Finally, given the impact of the new legislation, it is expected that the two-year deadline for compliance will apply to the entire content of the Guidelines, with the sole exception of the current obligation to enter ICT supplies that are also outsourced into the outsourcing register.

Answers to the specific questions are detailed below.

Question n. 1

Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?

The text under consultation aims to extend obligations/safeguards/precautions previously required only for contractual relationships classified as 'outsourcing' to all contractual agreements with third-party suppliers, subject to certain exclusions that are set out in other parts of the document. The definition of 'outsourcing' is reintroduced, but not as a category to which the regulatory requirements apply, but rather as a subset of contractual agreements with third-party suppliers. Considering that the concept of outsourcing is, on the one hand, devoid of any practical relevance and, on the other, only leads to interpretative uncertainties – and therefore potential discrepancies – the Sella Group is favourable to depriving it of any relevance at the regulatory and sanctioning level.

That said, with regard to the concept of outsourcing, it is considered that the scope of application of the Guidelines in question is not sufficiently clear insofar as:

- 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.

With regard to 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.[1]

This is also in light of the fact that these Guidelines expressly state that *"Where, for the provision of a non-ICT service, the agreement with a third-party service provider also involves the use of ICT services as defined in Article 3(21) of DORA, it is up to the financial institution to determine whether the use of the ICT service is relevant to the provision of services under the agreement with the third party and, therefore, determines the application of the DORA framework in place of these Guidelines. See also ESA Q&A DORA030*". 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 profound confusion as to what is subject to the DORA Regulation, acts as 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) and to eliminate the "outsourcing" subset entails a very significant expansion of the scope of application: 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, we particularly welcome 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.

However, 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 at the system level. It is therefore suggested that specific drivers be identified to guide financial entities in qualifying agreements that have a real impact on their operational resilience and business continuity.

[1] For example, Implementing Regulation (EU) No 2956/2024 has included among ICT services certain activities or services that do not appear to fall within the definition of ICT services under the DORA Regulation (provision of digital or data services), such as the category "Cyber risk management": Verification of compliance with cyber risk management requirements in accordance with Article 6(10) of Regulation (EU) 2022/2554.

With regard to the other definitions, the Sella Group agrees that it would be appropriate to include among the definitions that of 'operational resilience', which goes hand in hand with that of 'digital operational resilience' introduced by the DORA Regulation and referring specifically to the robustness of ICT services, systems and infrastructure supporting banking activities.

According to DORA, "digital operational resilience" refers to the ability of a financial institution to build, ensure and verify its operational integrity and reliability by ensuring, directly or indirectly, through the use of services provided by third-party ICT service providers, the full range of ICT capabilities necessary to ensure the security of the network and information systems used by the financial institution and which support the continuous provision of financial services and their quality, even in the event of disruptions. Conversely, the concept of 'operational resilience' introduced by the Guidelines refers to a financial institution's ability to perform critical or important functions in the event of a disruption. This capability enables a financial institution, directly or indirectly, including through the use of functions provided by third-party service providers, to identify and protect itself from threats and potential failures, to react and adapt, and to recover and learn from disruptive events, in order to minimise their impact on the performance of critical or important functions in the event of a disruption.

The two definitions are different, in that the definition under DORA contains an explicit reference to the use of ICT services and the ability to withstand interruptions/problems related to ICT services; conversely, the concept expressed in these Guidelines refers to the ability to continue to perform critical or important functions (and here there is a distinction) even in the event of failures/interruptions.

The Sella Group has no comments on the definition of operational resilience.

The Guidelines also modify the concept of essential or important function, which becomes 'critical or important function', borrowed from the DORA Regulation. In this way, the concept of critical or important function becomes unambiguous, eliminating potential differences in the classification of the same function within the same financial entity. Again with a view to guiding financial entities, it is suggested that certain elements be identified which, where they exist, allow entities to consistently qualify 'critical or important' functions, such as the impact on stability, continuity or quality of service provision if the supplier is affected by an operational disruption, as well as the presence of a supply across multiple financial entities belonging to the same group, the degree of substitutability of the third-party supplier, etc.

With regard to entities subject to these guidelines, 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.

Finally, with regard to the transitional period (two years from the publication of the final version of the Guidelines) for the adaptation of contracts, the Sella Group 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. However, an exemption is considered necessary in relation to the obligation to include in the outsourcing register a relationship that is both a provision of ICT services within the meaning of the DORA Regulation and, therefore, included in the relevant register. In fact, due to the current coexistence (and overlap) of the two regulations (EBA for outsourcing and DORA for ICT supplies), an excessive burden is placed on financial entities; this burden, especially in light of the changes that these Guidelines propose to

make, appears disproportionate and unjustified. It is therefore requested that, for this provision, the new Guidelines, which aim to avoid duplication of maintenance and reporting obligations for the same supply, become immediately applicable upon publication.

Question n. 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.'

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.

The Sella Group is in support of introducing a principle of proportionality when qualifying the contractual relationship that takes into account the riskiness and value of the supply (see answer to question no. 1).

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*".

Furthermore, given the intention to create uniform regulatory frameworks for ICT and non-ICT services, and given the need to fill the interpretative gaps caused by the absence of clear and objective definitions, it is considered appropriate that the applicability of the principle of proportionality in identifying the supplies covered by the regulatory scope be clarified by way of interpretation (e.g. through DORA Q&A) also with reference to the ICT services referred to in the DORA Regulation. It would also be appropriate to clarify, from paragraph 33 onwards, which agreements with third parties are not to be considered critical or important functions, in coordination with Delegated Regulation (EU) No 565/2017, which in Article 30(2) lists those that are not essential important functions and includes among these the provision of services related to staff training and the security of the premises and staff of the undertaking.

Question n. 3

Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?

Title III regulates the governance framework for managing risk arising from contractual agreements with third-party suppliers.

Firstly, it emphasises the responsibility of the financial entity's management body, which is responsible for defining and implementing a policy containing the rules and strategy for managing third-party risk, which must be maintained and reviewed at least annually. It then sets out the principle that the financial entity must adopt a policy for managing conflicts of interest.

It reiterates the obligation for the financial entity to prepare, maintain and periodically test its business continuity plans, including in relation to critical or important functions provided by third-party service providers.

The financial entity must also implement an internal audit plan, which should include, in particular, contractual agreements with third parties, where these relate to essential or important functions.

Finally, section 10 regulates 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. With regard to 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, we therefore request that this provision would be removed.

Question n. 4

Is Title IV of the Guidelines appropriate and sufficiently clear?

Title IV of the Guidelines regulates the following elements:

- pre-contractual analysis of the supplier;
- risk assessment of the agreement with the third-party supplier before signing the contract;
- due diligence on the supplier;
- mandatory contractual clauses (which vary depending on whether or not the service provided by the supplier supports a critical or important funtion);
- obligations regarding the subcontracting of essential or important functions;
- rights of access, audit and requests for information;
- rights to terminate the contractual relationship;
- continuous monitoring of the contractual relationship;
- exit strategy.

In terms of content, there are no substantial changes compared to the previous version of the Guidelines.

However, with regard to mandatory contractual clauses, the new Guidelines essentially provide for:

- for agreements NOT supporting critical or important functions, mandatory clauses that the previous version imposed for critical or important functions;
- for agreements supporting critical or important functions, clauses similar to those imposed by DORA (Article 30(3)) for ICT services supporting critical or important functions;

- for agreements supporting critical or important functions for which subcontracting is permitted, contractual clauses (to be included in the agreement between the financial entity and the supplier) in line with those required by DORA, which differ from those provided for in the previous version of the Guidelines.

The Sella Group is favourable to this approach, also with a view to standardising contract templates between ICT and non-ICT services as much as possible, as well as to monitor adequately the risk arising from third parties, regardless of the subject matter of the contractual agreement. In this sense, it is even more evident that such strict and rigorous obligations are justified where the financial entity has the possibility to identify the services subject to the Guidelines on the basis of their actual impact on the financial entity's risk exposure and operational resilience. Otherwise, if this possibility did not exist, the burdens of these Guidelines would be disproportionate and excessively rigid.

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.

Since 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, there are no particular comments on the content of this Annex.