THE SOUND MANAGEMENT OF THIRD-PARTY RISK

EBA'S CONSULTATION ON DRAFT GUIDELINES

AMAFI's answer

AMAFI is the trade association representing financial markets' participants of the sell-side industry located in France. It has a wide and diverse membership of more than 170 global and local institutions notably investment firms, credit institutions, broker-dealers, exchanges and private banks. They operate in all market segments, such as equities, bonds and derivatives including commodities derivatives. AMAFI represents and supports its members at national, European and international levels, from the drafting of the legislation to its implementation. Through our work, we seek to promote a regulatory framework that enables the development of sound, efficient and competitive capital markets for the benefit of investors, businesses and the economy in general.

The European Banking Authority (EBA) is consulting, until 8 October 2025, on its draft Guidelines on the management of risks arising from third-party service providers other than those related to information and communication technologies (ICT) within the meaning of the DORA Regulation.

Through these new provisions, the EBA aims to align the requirements applicable to relationships with non-ICT third-party service providers with those governing ICT providers under DORA.

Although this initiative is presented as an update to the 2019 Guidelines on outsourcing, its scope is significantly expanded. The proposal covers any agreement entered into with a third-party service provider (non-ICT), whether or not belonging to the same group, for the provision of one or more functions, thereby going beyond the concept of outsourcing.

In doing so, it lacks legal basis, going far beyond the CRD and MiFID II. In addition, it adds regulatory complexity to an already crowded framework which the Commission has committed to simplify. For these reasons, **AMAFI calls for the withdrawal of these Guidelines**. Before answering the specific questions of the consultation, our general comments detailing the reasons for this position are set out hereafter.

GENERAL COMMENTS

A. GROUNDS SUPPORTING THE WITHDRAWAL OF THE GUIDELINES

1. The draft Guidelines run counter to the simplification objectives

In the context of the European Commission's stated objective of reducing the administrative burden on businesses, the European institutions are engaged in simplifying the regulatory framework, particularly in financial activities. This simplification work, following the Draghi and Letta reports, aims to curb legislative inflation, which has become an obstacle to competitiveness, innovation, and the clarity of rules needed for good regulation. These reports therefore recommend a reduction in both the number and the complexity of legislative texts.

These draft Guidelines, and the extension of their scope to all agreements concluded with third parties, run counter to this simplification effort, contribute to regulatory inflation, and appear, moreover, to lack justification.

2. The draft Guidelines exceed the requirements of CRD and MiFID II

These Guidelines, in fact, go well beyond the Level 1 and Level 2 provisions applicable to investment firms and credit institutions under the Capital Requirements Directive (CRD) and MiFID II, since:

- Although the EBA is mandated under the CRD to develop guidelines on internal governance, of which outsourcing forms part, this mandate remains general in nature and does not explicitly refer to outsourcing arrangements or, more broadly, to all agreements concluded with third parties;
- Under MiFID II, the European Supervisory Authorities are not mandated to issue guidance on third-party arrangements (including outsourcing), and the subject of outsourcing is already thoroughly addressed in the Level 2 Delegated Regulation, which sets out detailed and binding rules on due diligence, risk control, business continuity, and access rights (*MiFID II Delegated Regulation*[1]*, Art. 31*). Moreover, MiFID II limits its scope to the outsourcing of critical or important functions.

Furthermore, MiFID II and the CRD clearly allow firms to apply a proportionate, risk-based approach, tailored to the nature and scale of their activities. These Guidelines, however, while stating that they take proportionality into account, impose a detailed set of operational obligations applicable to all financial institutions, which in practice amounts to a new layer of regulation (*see also the developments below*).

[1] Commission delegated regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.

Finally, regarding the stated objective of aligning these rules with those of DORA, AMAFI notes that the European legislator did not consider it appropriate to amend the MiFID II or CRD frameworks to incorporate such requirements at the time of adopting the DORA Regulation. In addition, DORA's requirements are laid down at Level 1 (for example, the requirement to maintain a register), whereas these draft Guidelines constitute a Level 3 instrument. The EBA Guidelines are instruments designed to harmonize supervisory practices without creating new substantive obligations. Their role is to support the implementation of Levels 1 and 2, but not to fill legislative gaps or impose additional standards.

For all these reasons, the Guidelines introduce an additional layer of regulation on top of the Level 1 and Level 2 requirements, that is unjustified and creates disproportionate operational constraints.

Consequently, AMAFI respectfully calls for the withdrawal of these draft Guidelines. Instead, to address certain specific implementation issues of MIF 2 or CRD, the EBA could, after prior consultation with the industry, make use of non-binding Questions & Answers.

B. RECOMMENDED ADJUSTMENTS SHOULD AN EBA MANDATE BE CONFIRMED

If the EBA were to be mandated to develop such guidelines, AMAFI is of the view that they should more fully reflect the principles of a risk-based and proportionate approach and duly take into consideration the specificities associated with the use of intra-group service providers.

1. The draft Guidelines are not sufficiently proportionate and risk-based

MiFID II and the CRD explicitly allow firms to apply a proportionate, risk-based approach, tailored to the nature and scale of their activities. AMAFI notes that, although the principle of proportionality is mentioned in these draft Guidelines, its consideration would remain purely theoretical if the text were to be adopted in its current form.

Indeed, this draft reflects an excessively burdensome administrative logic. The objective of enhancing the management of third-party risks results in financial institutions being required to provide an extremely substantial volume of information. The pursuit of exhaustive risk coverage prevails over a targeted and proportionate approach: institution's ability to assess for themselves the severity and materiality of their risks has been replaced by a standardised declaratory framework, both onerous and, at times, of limited relevance.

In practice, no entity, regardless of its size or the nature of its activities, appears able to benefit from any effective relief on the basis of proportionality. For instance, with respect to the register of third-party agreements, while such a record-keeping may in principle be subject to proportionality under the Title I of the Guidelines, the draft nevertheless prescribes a very extensive list of minimum information to be collected and included in the register (*see Draft Guidelines, §63*). This, in effect, excludes any meaningful application of proportionality.

Moreover, under these Guidelines, the use of third parties for the performance of functions that are not considered "critical or important" is nevertheless subject to a regime that is practically identical to that applicable to critical or important functions. However, the use of third parties for such functions does not entail the same level of risk, particularly with respect to business continuity. Thus, apart from the requirements relating to business continuity (*see Draft Guidelines, §8*), which apply only in cases where third parties provide critical or important functions, the remaining obligations apply to all third-party agreements. This leaves little scope for a genuine risk-based or proportionate approach.

AMAFI therefore considers that, if these Guidelines were to be retained, the requirements applicable to third-party agreements not involving critical or important functions should be drastically reduced and allow institutions greater flexibility in implementing them in a proportionate manner.

2. The draft Guidelines are not suited to intragroup arrangements

The use of an intragroup provider is not devoid of risk and must continue to be subject to appropriate assessment, monitoring and documentation

Nevertheless, these Guidelines would subject intra-group service providers indiscriminately to the same regime as external third-party providers, even though the risk profile is structurally lower in the intra-group context.

i. Lower Risk in Intragroup Arrangements

AMAFI considers that the use of an intragroup service provider structurally entails a lower level of risk, which should be reflected in a differentiated and proportionate regulatory treatment. For example:

- **Continuity and dependency risk**

  An external service provider is primarily driven by commercial considerations. External providers may be acquired, change their business strategy, or withdraw from the market. By contrast, an intragroup provider shares the same strategic objectives as the regulated entity. Additionally, intragroup exit plans usually rely on comprehensive wind-down plans on the part of the providing entity to continue providing services to other entities for a period of time, allowing for a smooth transition to another provider. Furthermore, prudential rules already provide for the management of continuity risks on a consolidated basis. The dependency risk is therefore lower in an intragroup context, compared with reliance on an external provider that may hold a dominant market position.

- **Concentration risk**

  Within an EU group, the concentration of critical or important functions is mitigated through consolidated supervision (*see CRD, Art. 109*) and related control mechanisms.

- **Security, data protection and confidentiality risks**

  Concerns regarding data confidentiality and security are also better addressed in an intragroup context. Data remains within the group perimeter and is subject to the same professional secrecy and confidentiality obligations. IT systems are often centralised and apply uniform controls across entities, thereby significantly reducing the risk of data leakage or misuse. Furthermore, ISS and GDPR policies, and sometimes internal regulations, are identical or at least standardised within the group, thus guaranteeing a uniform level of security that complies with existing regulatory constraints (especially since most of the group's entities are regulated entities).

- **Legal and compliance risks**

  Entities belonging to the same group operate within a common legal framework with uniform standards applicable across the group (for instance: contracts models, contractual policy, code of conducts regarding in particular human rights or ESG risks, etc.), regardless of the specific applicable regulation. By contrast, contractual negotiation with an external provider is more complex and monitoring the ability of the TPSP to fulfil the conditions included in the written third-party agreement is also more complex as the financial entity has less control and power over an external provider.

The risks referred to above are further mitigated in the intragroup context by governance and control mechanisms. Specifically:

- Compliance, security and risk management policies are standardised and mandatory for all entities within the group;
- Management bodies benefit from regular and detailed intragroup information flows;
- Internal control functions (audit, compliance, risk management) are coordinated at group level, ensuring effective oversight of intragroup service providers;
- Conflicts of interest are governed by documented mechanisms of governance, ensuring fair treatment between entities.

ii. The draft Guidelines are not adapted to intragroup realities

Moreover, these Guidelines are not adapted to intragroup realities, as their requirements frequently conflict with the organisation of the group, raising significant questions of feasibility and relevance. In practice, the rational organisation of groups, involving both a top-down hierarchical structure and the centralisation of certain activities for reasons of efficiency and internal consistency, does not allow

compliance with all control requirements imposed by these Guidelines, particularly where the delegatee is the parent or a sister entity of the regulated institution. Furthermore, certain controls (notably those relating to market abuse detection) are only meaningful when conducted at group level.

While it is legitimate that the delegating financial institution should have the means to monitor the proper performance of the outsourced activity, it is equally necessary to take into account the group's internal organisation in order not to impose requirements that the institution cannot realistically implement in relation to its own group and whose added value in terms of risk management is not established.

In conclusion, the use of an intragroup provider is not devoid of risk and must continue to be subject to appropriate assessment, monitoring and documentation. Nevertheless, it does not present the same risk profile as external outsourcing. The alignment of interests, the existence of strengthened control mechanisms, the consistency of policies, increased stability, and enhanced data protection all contribute to a significant reduction in overall risk exposure. AMAFI therefore considers that a regulatory approach recognising these differences and applying the principle of proportionality more explicitly would be more consistent with existing prudential principles and would allow supervisory focus to be directed towards areas where risks are truly most significant.

If these Guidelines were to be maintained, at a minimum, requirements relating to the formalisation of an agreement with an intragroup provider, the preparation of an exit plan, and the control of delegated activities should be alleviated in the case of intragroup outsourcing. At the very least, such alleviation should apply where the delegation is entrusted to group entities authorised within the European Union or in third countries subject to an equivalence decision by the European Commission and which, like the delegating institutions, are subject to the full set of European requirements, including those stemming from MiFID, or to rules deemed equivalent.

RESPONSES TO THE CONSULTATION QUESTIONS

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

- **Transitional provisions**

Concerning the transitional provisions, the draft Guidelines provide that: "*Financial entities should complete the documentation of all existing third-party arrangements in line with these Guidelines following the first renewal date of each existing third-party arrangement, but by no later than [date: 2 years from the date of application]*."

AMAFI considers that an additional period would be necessary, considering the experience with the 2019 Guidelines and with DORA (and the compliance costs generated by successive pieces of regulation). At a minimum, and still within the framework of a risk-based approach, entities should be

allowed an additional 12 months to manage the stock of pre-existing contracts that do not concern critical or important functions.

- **Définitions**

The **definition of third-party arrangement** is broadened and does not seem to focus on a risk-based approach. Regarding the definition of « third party arrangement », it does not include the term used in the « outsourcing arrangement » definition: **« *at least on a recurrent and ongoing basis* »**. This term shall be used in both definitions to exclude all arrangements regarding one off or short terms services that does not require the set of rules established in the Guidelines. AMAFI considers clarification shall be granted on this matter.

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

The **wording of footnote 42**[2] is unclear and would benefit from further clarification. Indeed, the Draft Guidelines specify that ICT services are governed solely by DORA. The Draft Guidelines will therefore only apply to non-ICT services. It should be noted, however, that footnote 42 adds confusion for non-ICT services that involve the use of an ICT service, for which the financial institution is required to determine whether the ICT service is substantial for the provision of the service and therefore involves the application of DORA. However, no details are given on how to carry out this assessment, and the criteria are unclear. It also appears that a large proportion of services, even those that are non-ICT in nature according to DORA, use IT components (software, hardware, etc.) or are hybrid services. The rules for determining whether to apply the guidelines or DORA must therefore be clearly established and not based on an assessment lacking objective criteria.

Question n. 3: Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?

With regard to Title III, AMAFI would like to make the following comments:

- **The review of the policy**

With regard to the review of the policy, AMAFI considers that the requirement for the management body to approve the policy once a year is excessive and constitutes an unnecessary administrative

[2] "*In case 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*" (*Draft Guidelines, footnote n.42*).

burden (*Draft Guidelines, §48*). Indeed, in the absence of any duly documented change to the policy, a simple transmission of the information to the management body should be sufficient. AMAFI therefore recommends that this clarification be introduced in the Guidelines.

- **Register-keeping requirements**

AMAFI considers that the **register-keeping requirements** set out in Section 10 are disproportionate (*see the general comments set out above*). Indeed, there is no real proportionality between the information requested for critical and non-critical functions, which again appears to be contrary to the principle of proportionality and leaving an unnecessary burden on financial entities that should be able to focus on the management of critical third-party agreements.

Finally, Paragraph 61 stipulates that states an obligation to retain terminated contracts and related documentation for five years. This obligation is not aligned with DORA that does not, and the EBA does not explain the rationale for it. This paragraph should be deleted to align with DORA.

Moreover, the articulation between the requirements for maintaining the DORA register and those for maintaining a register of non-ICT third-party arrangements (under these Guidelines) is unclear (*§63*).

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

No comment

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

AMAFI considers that Annex I should only be used to categorize functions for the purpose of maintaining the register. This annex should not be used to identify the functions that fall within the scope of the Guidelines. Indeed, AMAFI considers that Annex I, although indicative and non-exhaustive, is not consistent with the functions that may be excluded from the scope of these Guidelines, as set out in paragraph 32 of the draft. Several administrative services could be regarded as having no material impact on the risk exposure of financial entities or on their operational resilience.

AMAFI considers clarification shall be granted on this matter.