Consultation Response

EBA Draft Guidelines on the sound management of third-party risk

October 2025

AFME welcomes the opportunity to respond to the EBA draft guidelines on the sound management of third party risk, published 8th July (EBA/CP/2025/12).

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors, and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

Given the level of interest in this consultation we have responded to each of the questions within the EBA consultation paper, but highlight 3 overarching concerns:

- **The need for greater materiality and a consistent approach to DORA alignment**: we have identified several instances where the draft Guidelines extend DORA obligations to all arrangements, rather than those which underpin Critical and Important Functions. We would encourage the EBA to insert an overarching provision clarifying that the scope of the Guidelines in this regard should directly mirror that of DORA. Alignment with DORA would also be secured through the EBA refraining from adding further specifications which goldplate DORA, as is currently proposed with the definition of Critical and Important Functions (CIFs). The added layers of guidance within paragraphs 33 -37 will inevitably lead to divergence and potentially two sets of CIFs.

- **The need for flexibility on the treatment of hybrid services:** we support the intention of the EBA in bringing about parity in third party risk management between ICT and non-ICT arrangements. The EU's differentiation between the two is a unique development which is not reflected in other major markets and which causes considerable operational burden. We are however mindful that many arrangements can be hybrid in nature, and this creates uncertainty for firms managing complex arrangements involving multiple functions. We therefore propose that the authorities allow for overlap or flexibility in classification, enabling firms to apply a consistent and risk-based approach to oversight without needing to retrospectively reassess existing DORA-classified arrangements or justify their classifications to authorities.

- **The need for the Annex to reflect the scope of the guidelines, and to exclude regulated activities:** it is our understanding that the EBA intended to provide a non-exhaustive and illustrative list of arrangements which are in scope of the Guidelines. We support this goal, but on the basis that the categories and sub-categories within the Annex closely reflect the exemptions set out within the body of the Guidelines, and particularly with regards to paragraph 32. We would also strongly encourage the EBA to include within these exemptions regulated financial services and ancillary services, and entities which are themselves under scope of the Guidelines. This would reflect the position under DORA where it was acknowledged that such services are provided by

highly regulated entities, who must already comply with substantial operational resilience and risk management requirements, and that to include them would bring about significant operational burden, including remediation of contracts, with little to no benefit in terms of risk management.

We remain available to discuss any of the specific answers in further detail.

Consultation Questions

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

Subject matter

- AFME welcomes the decision to update the 2019 EBA Outsourcing Guidelines (the 2019 Guidelines) to take account of DORA. In addition to bringing about a level playing field and fostering supervisory convergence, as noted in the consultation materials, regulatory alignment between ICT and non-ICT arrangements will deliver meaningful operational efficiencies for EU financial entities and support a more streamlined, consistent approach to third-party risk management (TPRM). Nevertheless, the EU framework has evolved in a way that now establishes two distinct regimes across ICT and non-ICT third-party arrangements, creating additional and unnecessary operational complexity for financial entities. Whilst the practical implications of this distinction will likely depend on how supervisors apply these expectations in practice, the dual framework will necessitate firms making subjective assessments to distinguish what is predominantly or materially ICT. This creates uncertainty for firms managing complex arrangements involving multiple functions, despite this having no value for risk management. We therefore propose that the authorities allow for overlap or flexibility in classification, enabling firms to apply a consistent and risk-based approach to oversight without needing to retrospectively reassess existing DORA-classified arrangements or justify their classifications to authorities.

Scope

- We also acknowledge how the extension of scope from outsourcing to all third-party arrangements is consistent with broader TPRM regulatory trends. While we understand the basis of this shift, it means that it is even more essential to ensure that expectations remain proportionate and risk-based – particularly given the volume and diversity of arrangements now in scope – to ensure the expectations remain operationally feasible. We would strongly encourage the EBA to introduce an overarching materiality lens to the Guidelines, by stating explicitly in the scope of the Guidelines and in Title 1 that it is only those services that could, if disrupted, materially impair the financial entity's ability to deliver its critical services or functions which are within scope. This would reflect the helpful clarification provided by the EBA at the recent public hearing that the intention of the Guidelines was to focus on those arrangements which could have a material impact on the financial entities' operational risk or operational resilience. Such clarification, along with additional explanatory language in the recitals, would reinforce the EBA's underlying regulatory objective and help industry better understand the types of arrangements the EBA is seeking to capture. An appropriate materiality threshold would also serve to substantially reduce the burden to firms operationalising the EBA's requirements across the expanded scope of third-party arrangements.
    - We acknowledge the materiality threshold reflected in paragraph 32.f but flag that the current language, with reference to "risk exposures" is potentially too broad and

does not align with the substantially higher threshold of material impact to a firm's operational resilience (which would appear to more appropriately reflect the prudential objectives of the guidelines).
    - The expanded scope of the Guidelines also risks capturing short-term arrangements that may meet the materiality threshold under paragraph 32.f but do not justify the full suite of contractual requirements, given these are not the type of arrangements where the firm is placing continuing reliance on the third-party. For example, sponsorship arrangements are typically short term (i.e. less than a year) and event-specific. Another example is proof of concept or evaluation agreements which are designed to test a supplier's technology or service before a longer term arrangement is entered into. Descoping these arrangements via use of the higher materiality threshold, embodied within the link to a financial entity's operational risk or resilience, would also be consistent with the exemption in Paragraph 30 for arrangements which are not recurrent or ongoing.

- We also see other opportunities to strengthen proportionality in areas such as contractual requirements and the register. Please see Q3. We additionally encourage the EBA to ensure that this shift in approach towards outsourcing is reflected in wider regulatory frameworks, for example the approach to outsourcing under MiFiD.

- Finally, on scope we also seek clarification on the treatment of 3rd country TPSPs contracted through intragroup entities. An explicit and specific illustration / use case would be particularly welcome, using the example of an in-scope entity making use of a third party service, via an intragroup arrangement, where this service is provided by a third country TPSP which exclusively contracts with a third-country parent entity. Experiences to date with DORA-related remediations indicate that an explicit illustration would be very helpful in smoothing some of the contractual negotiations with third country providers who are reluctant to consider their services as in-scope.

Definitions & Drafting

- Regarding definitions, and drafting style more broadly, we encourage the EBA to adhere consistently to the wording and phrasing within DORA. This will help reduce complexity and enable financial entities to leverage internal DORA processes as part of the transition. In a number of instances, the EBA has broadly aligned in principle with DORA, but used hybrid wording by retaining elements of the 2019 Outsourcing Guidelines, to outline a different set of steps or reflect DORA provisions but in a different order. One example of this is in Section 14 of the EBA proposals versus DORA Article 28(8) on Exit Strategies. This layered framework risks introducing expectations that differ or go beyond DORA's requirements, leading to divergent methodologies and unnecessary complexity, potentially undermining the benefits of simplification and convergence. Please see Q2 for substantive feedback regarding the definition of Critical or Important Functions (CIFs) as the key example of this, where we flag that the layering of expectations will complicate firms' efforts to directly apply their DORA Critical or Important Function assessments.
    - On CIFs, we also flag 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[1].

[1]This 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.

- To reduce duplication and ambiguity, we would strongly recommend the EBA (and EU supervisory authorities) adopt and align to a consistent layered terminology:
    - **Function**: refers to the bank's own functions, operations or business lines (i.e., consistently with 'critical or important functions' which are framed around the key services provided by a bank);
    - **Service**: refers to the service delivered by the third-party service provider to support the bank's functions;
    - **Arrangement**: refers to the contractual relationship with the third-party provider under which a service is provided;
    - **Activity**: refers to the specific processes or tasks within a function, which may be supported by third-party services.

  The interchangeable use of this terminology and lack of consistency creates unnecessary complexity, for example:
    - **Para 54:** "*When functions are provided by a TPSP…the conditions…for the service provided by a TPSP..*" – It is unclear whether the EBA intends to distinguish between the outsourcing of a whole function and the provision of a supporting service to that function, or whether the terms are being used interchangeably.
    - ***"critical or important functions provided by TPSPs"*** (multiple references throughout) – This is misleading as third-party providers do not themselves "provide" a bank's function. The appropriate terminology should be "services provided by TPSPs supporting critical or important functions".
    - **Para 63.i.:** *"whether or not (yes/no) the function provided by a TPSP is considered critical or important…"* – It is unclear whether the reference is to the firm's assessment of the criticality the bank function that the third-party service supports, or the firm's risk assessment of the third-party service itself (including whether it is material to that CIF, noting that just because a service supports a CIF, it does not automatically mean it's critical).

Transitional measures

- Finally, we welcome the inclusion of specific transitional measures, which are primarily on the basis of contract remediations occurring at the point of first renewal. We strongly object to the suggestion in the Accompanying Documents (page 70) that there will be negligible additional costs by virtue of the pre-existing implementation of the 2019 Guidelines, and flag that in parallel there is continuing remediation of DORA related ICT arrangements which will exacerbate the operational challenge for firms. We would therefore bolster the transitional measures by calling for a 9 month window between the finalisation of the guidelines, and the incorporation of these obligations in any contract due for renewal. Contractual processes can take 6 months or more, and there will also need to be a period for review, gap analyses and remediation of firms' standard terms of business etc. Thereafter, we would recommend remediation is required by whichever is latest: the next renewal of the contract or two years from the date of application. Not all contracts follow a 1-2 year renewal cycle, and aligning remediation to the next contract renewal as the outer limit would avoid unnecessary administrative burden. In many cases, firms are already substantively compliant, having implemented contractual arrangements aligned with the 2019 EBA Guidelines and member state outsourcing requirements. As such, firms should not be expected to reopen and renegotiate contracts solely to align wording with the updated Guidelines.

- Given the inconsistencies which emerged across NCAs as part of the DORA Register of Information implementation, we would also encourage the ESAs to use the transitional period as an opportunity for explicit advance guidance to fellow authorities, to ensure a consistent approach across the EU member states.

Question 2: Is Title II appropriate and sufficiently clear?

Scope - exemptions

- We welcome the exemptions under Paragraph 30 for the "*mere purchase of a good (eg. plastic cards, card readers, office supplies, personal computers, furniture) which is excluded from the definition of third party arrangement*". Additionally, noting that paragraph 30 states a financial entity should assess whether the function is provided on a recurrent or ongoing basis, when determining if the arrangement is in scope, we seek clarification as to whether the EBA intends the guidelines to apply to very short-term or sporadic services, for example those lasting under one year. The proviso on a recurrent or ongoing basis should also be replicated within the definition of third party arrangement.

- We strongly urge the EBA to reconsider the decision to not provide a broad exemption for regulated financial services and ancillary services, or entities which are themselves under scope of the Guidelines, from its incoming application, in line with the exemption under DORA, through the DORA Q&A[2]. Whilst we appreciate the context under DORA differs, the underlying rationale is still relevant: Such services are provided by highly regulated entities, who must already comply with substantial operational risk and resilience and third party risk management requirements. The application of these Guidelines to those arrangements, will bring about significant operational burden, including remediation of contracts, with little to no benefit in terms of risk management, for example mandating documentation of audit rights and business continuity plan (BCPs) which will already be visible to authorities.
    - An exemption for regulated services would in our view be consistent with the decision of the EBA to exempt under paragraph 32.g basic utilities which are subject to a regulatory framework, and to exempt global network infrastructures, clearing and settlement arrangements and correspondent banking services under paragraph 32.b, .c and .e respectively.
    - A blanket exemption for regulated services would undoubtedly be the most effective way of ensuring a uniform and consistent approach across supervisory authorities and avoids the risk of certain activities being unintentionally captured by the Guidelines, through omission from the list of activities specifically called out within paragraph 32.
    - As an illustration of that risk, we note that custody arrangements are not currently explicitly excluded from the scope of the Guidelines. Custody services[3] including safekeeping, asset servicing, and fiduciary functions, are provided by entities subject to stringent regulatory oversight under sectoral legislation such as MiFID, UCITS, AIFMD, and CSDR. These entities are already required to maintain robust operational resilience, risk management, and transparency standards, which are regularly reviewed by competent authorities. Including such arrangements within the scope of the Guidelines would result in significant duplication of oversight and contractual remediation efforts, without delivering meaningful risk management benefits. For example, mandating audit rights or reintegration assessments for custody services would be redundant, as these are already embedded in the regulatory obligations of custodians. We therefore would urge the EBA to explicitly exempt custody arrangements from the Guidelines, both in the body of the text and in Annex I, to ensure consistent treatment with paragraph 32.c and to avoid unintended regulatory overlap.
    - Given though that custody is only one example of a regulated activity currently omitted from the exemptions in paragraph 32, and that this rationale will

[2] https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en

[3] Custody services which are not investment services in accordance with MIFID2

undoubtedly apply to numerous other services, we would again strongly encourage the EBA to exempt, as an overarching holistic solution, all arrangements which are regulated services or performed by parties themselves within scope of the Guidelines, and to ensure this is reflected (by omission) within the Annex. Such a streamlining of the regulatory burden on financial entities would also represent a tangible instance of the EU putting into practice its recent calls for Simplification in order to boost EU Competitiveness.

- We also seek clarification that all services from legal firms may be considered out-of-scope in light of paragraph 32.f.

Hybrid services

- We noted in Q1 that the EU's distinction between ICT and non-ICT arrangements will continue to cause operational complexity for financial entities, despite the intention of the EBA to align both sets of expectations. While it is stated that the financial entity must determine whether the use of ICT within an arrangement is "material" to trigger the application of DORA, we foresee this assessment causing difficulty on services that can intrinsically have mixed ICT and non-ICT components. We therefore propose that the authorities allow for overlap or flexibility in classification, enabling firms to apply a consistent and risk-based approach to oversight without needing to retrospectively reassess existing DORA-classified arrangements or justify their classifications to authorities. We are keen to avoid the need for subjective assessments and the duplication of processes.

CIF Definition - Divergence from DORA

- A prime example of the divergence from DORA referenced in Q1 is the definition of Critical and Important Functions, where the draft Guidelines in Paragraphs 33 – 37 set out a list of specific functions which must be considered critical or important, at certain times automatically and at others dependent on certain conditions, along with a separate list of factors for consideration. While we acknowledge the EBA's clarification at the recent public hearing that this is intended as helpful supplementary guidance, in practice it will inevitably undermine the EBA's stated intention to align the definition of CIFs under the Guidelines with that under DORA. Experience to date strongly suggests that supervisory authorities will instead treat the considerations at paragraphs 33 – 37 as de facto requirements.

- We would urge the EBA to remove these provisions from the Guidelines and align exclusively to the definition within DORA, which we acknowledge is outlined in the definitions of the Guidelines[4]. This would both protect against unintended divergence and reflect the EU's wider Simplification Agenda. Retaining these provisions would lead to either:
    - firms needing to maintain two separate approaches to their classification of CIFs for ICT and non-ICT functions, which would be needlessly confusing, complicated and operationally burdensome – and not in keeping with the intended purpose of the Guidelines; or
    - Firms needing to revisit their approach to CIF identification for DORA based on the provisions of this GL. This would amount to a retrospective change in the legislative definition, which would both create significant disruption to firms' DORA programmes, and likely be beyond the EBA's mandate and authority regarding DORA.

CIF definition – Impact of broad scope of CIFs

[4] *A critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.*

- Further, collectively the supplementary provisions within paragraphs 33 – 37 give rise to the impression that a CIF could incorporate not only core services, but any regulated service or activity of the bank, leading *de facto* to the assessment that almost all functions should be considered critical or important.

- In practice, financial entities are likely to address this by creating a multi-tier structure of "functions" considered CIFs for the purpose of compliance, and those which are considered CIFs for the purpose of truly managing the resilience of the entity. This creates additional governance and complexity for financial entities while not benefitting risk management or resilience. Again, we recommend the deletion of paragraphs 33 – 37.

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

TPRM Policy

- We question the need to explicitly differentiate, under paragraph 50, ICT services against non-ICT services as part of the third party risk management policy. In light of the intention of policymakers to remove this distinction in EU regulation, such differentiation should become negligible in practice and removing the requirement would help reduce unnecessary operational complexity.

- Paragraph 56 includes the term "unacceptable level" which is currently undefined. We would recommend this is replaced with existing definitions of business impact.

- Under paragraph 57, firms are required to list the specific causes of disruption in their BCPs. This is redundant. Effective BCPs focus on maintaining continuity of critical services regardless of the cause of disruption. Detailing potential causes adds no practical benefit to resilience outcomes and risks turning BCPs into box-ticking exercises. This requirement should be deleted and the focus should be on recovery objectives, testing, and governance to ensure continuity regardless of the disruption source.

- Paragraph 58 also introduces an explicit requirement that BCPs related to third-party arrangements align with EBA GLs on internal governance. This deviates from DORA contractual expectations and we would urge the EBA not to goldplate non-ICT arrangements. Furthermore, paragraph 55 seems to imply that each CIF will have a singular BCP. However, in practice there may be multiple BCPs relevant for a CIF, or multiple CIFs under a single BCP. The EBA should clarify that these approaches are allowed.

The Register

- We support the intention within paragraph 63 on Documentation Requirements that the outsourcing register should be merged where possible with the DORA Register of Information, but repeat the need for greater proportionality with regards to the arrangements which should be included within the Registers. Without the clear and robust materiality lens recommended in Q1, the expanded scope represents a significant expansion of reporting relative to previous regulatory expectations and potentially will introduce a substantial operational burden without an obvious value add to risk management or supervisory objectives. To this end, there should be an explicit reference within Title III that only subcontracting arrangements which *effectively underpin* CIFs

should be included, reflecting the final position within the DORA delegated act on subcontracting.

- Further, to enable a merging of non-ICT arrangements within the DORA Register, we request that the information requirements, including the fields, fill-in options, and their mandatory nature, be aligned with the DORA register ITS. Whilst we acknowledge the flexibility offered by the Guidelines in terms of the alignment with the DORA register and the EBA's intention to have a "lighter register" given the expanded scope of services, we are concerned that this approach will drive complexity and risks divergence in implementation across firms and member states. The industry objective is unified around the desire for an EU-wide third-party register framework that captures both ICT and non-ICT arrangements. This should be achieved through a single aligned register, with data field requirements adapted to reflect proportionality and risk-based principles. This would include:

  - ensuring the broader population of third-party arrangements are not subject to unnecessary reporting requirements – i.e., flexibility or exclusion of data requirements for lower-risk arrangements; and

  - optionality for data fields that are not applicable to all third-party arrangements – i.e., ensuring any data-related or ICT-specific fields are optional where not applicable;

  Industry is concerned that otherwise firms may face supervisory scrutiny and pressure to justify decisions not to merge or fully align registers, undermining rather than supporting the broader EU simplification and convergence agenda. Specific data points causing concern are as follows:

  - subparagraph d. – The requirement to provide *the outcome and date of the last assessment performed of the TPSP's substitutability* should be removed as it goes beyond both the DORA and CASPER register requirements. Additionally, the date of the last criticality assessment is already provided, which should sufficiently evidence this data field.

  - subparagraph g. – This requirement goes beyond DORA by asking for "*other relevant contact details*" and "*name of its ultimate parent company*". It is unclear what the benefit to supervisory oversight and objectives TP contact details provides – noting that these are also constantly changing. These should be removed.

  - subparagraph h. – The *estimated annual budget cost of the third-party arrangement* is operationally challenging to assess – particularly at service level – and is potentially commercially sensitive. It is also unclear what supervisory value this information provides. The cost of a third-party arrangement does not meaningfully reflect its inherent risk or criticality (i.e., a high-cost contract may relate to non-critical service, while a lower-cost contract may underpin essential services). Cost also does not reliably indicate the degree of operational dependency or the extent to which a service may be substitutable. As such, cost should not be treated as a proxy for risk exposure and it is unclear what supervisory value this data provides – particularly given the challenges of accurately apportioning service-level cost across multiple legal entities.

- In Q1 we also flagged the lack of consistency in layered terminology throughout the guidelines. With regards to the register data fields under paragraph 63 we call out as further examples:

    - subparagraph a. – Regulatory requirements such as this at times appear to conflate the third-party *service* with the *contractual arrangement* through which it is delivered. These are distinct concepts and conflating the two can lead to operational and compliance challenges for firms, particularly where a single contract covers multiple services. Oversight, classification and register reporting requirements should attach to the service, not the legal contract that gives effect to it. We encourage regulatory expectations to reflect this distinction more clearly.

    - subparagraph e. – The requirement to provide *a brief description of the functions provided by the TPSPs* should be amended to refer to the "services" provided by the TPSPs for clarity.

    - subparagraph g. refers to *where the function is to be performed* and, as above, should be amended to refer to the "services" performed by the TPSPs to avoid ambiguity.

    - subparagraph h. – The reference to the criticality of the "*function provided by a TPSP*" is misleading and creates ambiguity as to whether the EBA is referring to the firm's assessment of the criticality of the function that the third-party service supports. This should be amended to "whether the function is considered critical or important".

- Additionally, we note that the register requires financial entities to assign a category that reflects the nature of the service being provided, with Annex I to be "considered as a list of non-exhaustive examples". The development and use of taxonomies of services creates a significant administrative burden for firms who are required to retrofit and align their internal classifications to the granular service categories developed by the authorities. This is exacerbated by a lack of consistency across different regulatory regimes. We support the EBA's flexible approach and would urge the ESAs – in connection with their supervisory convergence mandate – to ensure that the flexibility for firms to maintain their own classifications provided by the EBA is upheld consistently across national competent authorities. Given the inconsistencies which emerged across NCAs as part of the DORA Register of Information implementation, we would encourage the ESAs to reinforce in advance to fellow authorities that financial entities are free to use their own internal classifications if they deem these more appropriate. In fact, this categorisation in general is often seen as unhelpful and unduly burdensome, and it is the views of our members that the categorisation fields should be removed, with information on the nature of the service included in the service description.

- We support the use of LEIs to support supervisory and oversight objectives. However, industry is concerned that extending the requirement to procure LEIs for all third-party arrangements will present significant challenges in practice. Notably, there is currently no standardised approach to the information entities could be required to submit to obtain an LEI – in some cases, the information requested is onerous and has no bearing on LEI issuance. This is particularly problematic for private companies. To ensure the requirement remains proportionate and does not impose an undue operational burden on financial entities (whilst also supporting supervisory objectives), we propose limiting mandatory LEI collection to third-parties delivering services supporting CIFs, and/or introducing flexibility in the requirement for non-CIFs (e.g., "if applicable").

- We also note the draft guidance in paragraph 61 requires firms to retain documentation for terminated contracts for "for an appropriate period of at least 5 years". Requiring this level of information for historic arrangements would likely be extremely burdensome, both for financial entities but also for the TPSPs themselves. A large number of requests from FEs coming at the same time could well overwhelm smaller EU TPSPs, which could have a significant negative effect on EU competitiveness. The retention period for terminated contracts was deliberately removed from DORA during the legislative process, given the lack of relevance to risk management. Reintroducing such a requirement would therefore not align with DORA and be seen as gold-plating the regulation. We therefore recommend to delete it. As part of this we urge the deletion of the requirement to provide an end date and reason for the termination as services that have been terminated during the reporting period would not be captured in the register. There is no clear risk management benefit, and historical versions of the register could be reviewed by authorities if needed. Retaining this requirement adds unnecessary complexity and should be removed.

- We also ask whether there are standardised expectations regarding notification thresholds for competent authorities under paragraphs 67 and 68, relating to upcoming contractual arrangements or material changes to existing arrangements.

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

Supervisory conditions for contracting with third-party services providers

- There is concern over the stipulations in paragraph 72 on the use of third country TPSPs who are providing banking activities, payment services, issuance of ARTs or investment services. A co-operation agreement between competent authorities may not always be published or visible to market participants, thereby creating considerable difficulty to firms in demonstrating compliance with 72.c.

Risk Assessments

- We flag how the new guidelines expands the pre-contractual risk assessment beyond merely operational risk considerations to expressly consider reputational risk, legal risk, and concentration risk as separate risk attributes (paragraph 73 and expanded at paragraph 74). While these risks are referenced under DORA, with which we support alignment, we stress that the guidelines have not adopted a corresponding level of proportionality, in that these are expectations which apply to all arrangements rather than only those supporting CIFs. The inclusion of additional risk criteria should be subject to the principle of proportionality.

- Similarly, we note that requirements on substitutability and reintegration assessments for all TPSPs is disproportionate and not risk sensitive. A large proportion of firms' TPSPs will be immaterial from a risk perspective, and requiring this level of data to be recorded for all of these will be extremely operationally demanding and costly for limited benefit. These data fields should only be required following a risk-based approach, and in any case only for material TPSPs supporting CIFs or material parts thereof. As an overarching point, this exact wording is recommended as opposed to that within paragraph 79 which refers to the criticality or importance of the function. CIF status is generally understood to be binary, so this could lead to significant confusion.

- While we acknowledge the importance of identifying and managing concentration risk, it is important to recognise that third-party arrangements are often contracted at group

level. As such, meaningful assessment of concentration risk is typically most effective at the group level. Requiring individual legal entities to conduct entity-level concentration risk assessments may therefore not materially improve risk outcomes, particularly where those entities have limited ability to manage or mitigate group-level arrangements. We therefore propose a proportionate approach that allows entities to rely on group-level assessments where appropriate – otherwise, this could result in a compliance exercise with limited value for actual risk management and supervisory oversight.

- In paragraph 83, the requirements to consider ESG risks fails to recognise the varying level of development of ESG risk understanding, methodologies and data between the various sub-factors of ESG. The EBA's own ESG Risk Management GLs explicitly state that firms should initially focus on Climate risk, and expand into other areas of Environmental and ultimately 'S' and 'G' risks as these areas develop. These same considerations should be incorporated into paragraph 83.

Contractual phase

- We note that the contractual provisions for arrangements, as outlined within Section 12 (paragraphs 84 – 87), have been updated largely in line with those set out within Article 30 of DORA, but that the order and wording differs with certain elements from the 2019 guidelines retained. There should be total consistency in substance between DORA and the 2025 GLS, except to the extent that the provision is very ICT specific. In this regard, we welcome the omission of the additional Data Security terms and pen testing requirements from the 2019 GL, as well as the ICT risk related scenarios that were in DORA. However, there is little logic to retain legacy 2019 wording for a provision which conceptually is the same as in DORA (e.g. "*impediments capable of altering the performance*…" should be replaced with Art 28(7)(c) of DORA: "*circumstances evidenced throughout monitoring deemed capable of altering performance*". Consistency in expectations across frameworks will help secure the EBA's goals on supervisory convergence and ensuring a level playing field. Additionally, we caution against further prescription which could be regarded as gold-plating DORA and going beyond those parallel obligations, for example the additional requirements on the governing law of the agreement. Further, given the broad number of arrangements now within scope, even beyond the outsourcing baseline, we are concerned that some of the requirements simply will not work in all contexts. For example, 85.c, .g and .h on data processing and storage location, data confidentiality and data access.

- We also stress that by extending the obligation under paragraph 85.j on monitoring the performance of the TPSP to all arrangements, rather than only those supporting CIFs, the Guidelines have again extended the scope and burden of DORA. The revised guidelines would consequently trigger significant increased workload in terms of updating contracts and instead we encourage greater proportionality, in line with DORA and the 2019 Guidelines. We again stress that as part of the overall materiality lens, the Guidelines are amended to recognise that financial entities are only expected to monitor *material* risks across the wider supply chain.

- More broadly, we support the approach taken to the Guidelines to distinguish between contractual requirements for arrangements that support CIFs and those that do not. However, the current baseline expectations may still prove overly burdensome when applied to third-party services more broadly. Certain lower risk non-outsourcing arrangements will now fall in scope of the Guidelines but may not warrant certain

contractual standards. We recommend strengthening the language to clarify that financial entities may adopt a proportionate and risk-based approach when determining appropriate contractual provisions for the broader population of non-CIF third-party arrangements. That is, provided a legally binding agreement is in place defining the role and responsibilities of each party, certain contractual mitigations would not be necessary for all third-party services. For example, a sponsorship arrangement which may now fall within scope would not merit contractual requirements relating to data location or certain termination rights.

- An extension in scope, from arrangements supporting CIFs to all arrangements is also evidenced in paragraphs 97 – 108 on access, information and audit rights, with paragraph 98 explicitly stating that regardless of criticality there is an obligation on documenting within the arrangement the information gathering and investigatory powers of authorities. In practice, this could imply a differentiated and more robust treatment for non-ICT services than for ICT services, which we understand is not the EBA's intention.

- Finally, regarding subcontracting, AFME again calls for greater materiality and proportionality in short by adopting the final position of the DORA delegated act on subcontracting, namely that financial entities should have "*a particular focus on those subcontractors that effectively underpin ~~(ICT)~~ services supporting critical or important functions*". As noted in AFME advocacy in connection with DORA's Register ITS and Subcontracting RTS, treating every subcontractor supporting a CIF as equal, regardless of their role, level of importance or potential impact to the provision of the CIF diverges from a risk-based approach. This is unhelpful for supervisory and oversight objectives and diverts risk management resources away from monitoring providers that present the most material risks. In order to properly reflect a risk-based approach to supply chain scope, the 2025 GLs should align in terminology and/or conceptually with DORA to support a consistent approach across regimes. This adjustment should be reflected in the definition of subcontracting.

Exit strategies

- Finally, reinforcing the point in Q1 on divergences within expectations leading to gold-plated requirements that go beyond DORA, we flag that the draft 2025 GLs introduce additional criteria/factors and greater prescriptiveness when developing Exit Strategies, for example the suggestion that a Business Impact Analysis assessment is required. (Section 14, paragraph 119). We would call for additional prescription to be removed and flag that further clarification would be welcome in respect to the situation whereby alternative suppliers may not exist or fail to provide a feasible solution.

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

- The inclusion of the Annex could represent a welcome addition to the Guidelines, which helps clarify the intended scope of arrangements, provided the purpose is clear and there is consistency between the categories listed and the scope of the Guidelines as set out in the body of the text. The rationale for the Annex, as stated within paragraph 63.f should

also be repeated within the Annex for the avoidance of doubt[5]. In order to ensure that the exemptions referenced in the Guidelines, especially those under paragraph 32, are reflected in the Annex we strongly recommend the following categories are removed:

Category / Sub-category	Rationale
Travel & entertainment services	Travel services are explicitly excluded under Para 32.f of the draft guidelines.
Secretarial Services	This is also explicitly excluded under Para 32.f of the draft guidelines, and should encompass administrative support to the board, record-keeping, translation and compliance with laws and regulations assistant, potentially renominated as Corporate Secretary or Company Secretary.
• Advertising & Marketing; • Document Management & Archiving; • Insurance Services; • Payroll Services; • Pensions & benefits; • Postal services & Mailing; • Procurement & purchasing of services; • Talent acquisition & hiring.	Considering the exclusionary text noted in paragraph 32.f: "*As a general principle, the following functions are excluded from the scope of these Guidelines… the acquisition of services that do not have material impact on the financial entities' risks exposures or on their operational resilience*", most if not all of these subcategories under "Administrative services" should be excluded on the basis that they do not have a material impact on risk or operational resilience.
Depositary tasks & administration for UCI	Functions that are "legally required to be performed by a TPSP" are explicitly excluded under Paragraph 32.a of the draft guidelines. Under UCITS rules, UCITS funds are legally required to appoint a depositary.
• Asset servicing; • Clearing, settlement & reconciliation; • Proxy voting; • Safekeeping and Custodianship; • Trustee, depositary & fiduciary services.	These functions are generally part of the services provided by Settlement institutions to their clients, which are deemed out-of-scope according to Para 32.c.
Credit decision making	A bank may not delegate the final decision on whether to grant a loan (amount, terms and risk assumption) to a third party service provider.
Insurance	In summary, the purpose of financial entities contracting insurance policies is to mitigate

[5] 63.f: *a category assigned by the financial entity that reflects the nature of the functions covered by the third-party arrangement as described where available, in Annex I, which should facilitate the identification of different types of arrangements; if the category is not available under Annex I, the financial entity should provide its own internal categorisation. If an arrangement covers multiple functions, then the financial entity should report as many categories as the functions provided;*

	and/or transfer risks. Therefore, including them in the scope would not be consistent with the spirit of these third-party risk management guidelines.

AFME Contacts

Marcus Corry
Director, Tech&Ops
marcus.corry@afme.eu
+44 (0)20 3828 2739

Stefano Mazzocchi
Managing Director & Deputy Head of Advocacy
Stefano.mazzocchi@afme.eu
+32 2 8835546