BPFI response to EBA consultation paper on the sound management of third-party risk

October| 2025

Introduction

Banking and Payments Federation Ireland (BPFI) is the voice of banking, investment firms and payment providers in Ireland. Representing over 100 domestic and international member institutions, we aim to mobilise the sector's collective resources and insights to deliver value and benefit to members, enabling them to build competitive sustainable businesses which support customers, the economy and society.

We welcome the opportunity to comment on the European Banking Authority's (EBA) draft Guidelines on the sound management of third-party risk. Our members fully support the EBA's objective of strengthening governance and operational resilience and harmonising expectations for third-part risk management (TPRM) across the EU financial sector. We note, however, that the proposed extension from outsourcing to all third-party arrangements marks a major expansion of the regulatory perimeter. While conceptually aligned with broader third-party risk management developments, this shift will only be effective if the framework is proportionate, truly harmonised, and operationally feasible. Without adjustment, the Guidelines risk creating inconsistency and additional compliance burden without commensurate resilience benefits.

In our view, the EBA's final Guidelines should be an enabler of harmonisation and simplification. Alignment with DORA, risk-based proportionality, and consistent implementation across Member States will ensure that the new framework strengthens Europe's operational resilience landscape. BPFI and its members stand ready to support the EBA in achieving these objectives. You will find more details within our submission, but we would like to highlight the following in particular:

- **Embed Further Proportionality.** While we welcome the inclusion of proportionality within the Guidelines, we believe that this could be further embedded within the framework to ensure the application of the requirements to the expanded scope is feasible. It is important that requirements should reflect the nature, scale and complexity of firms and arrangements. Proportionality should therefore be further built into expectations for contractual clauses, due diligence, intragroup arrangements and the Register of Information (RoI).

- **Ensure Full Alignment with DORA.** The Guidelines should more closely mirror DORA definitions, exclusions, concepts and structure, removing residual elements of the 2019 EBA outsourcing framework in order to avoid complexity and firms having to create two sets of CIF identification criteria for ICT and non-ICT TPSPs. In particular, the additional CIF criteria in paragraphs 34–37 should be deleted or clearly marked as illustrative only to prevent dual CIF regimes.

- **Materiality and Scope.** The new coverage of all third-party arrangements constitutes a material perimeter change. We therefore believe that the guidelines should focus only on those arrangements that have a material impact on a firm's operational risk and operational resilience. As drafted, we remain concerned that in parts the guidelines do not clearly convey a materiality threshold aligned with the stated prudential objectives. The EBA should, in the final draft, clarify this material threshold. Such an approach will help to reduce the burden on firms operationalising the requirements across the expanded scope of third-party arrangements. In addition, the requirements relating to subcontracting should only focus on material subcontractors.

- **Promote Consistent Implementation.** The EBA should emphasise the need for faithful implementation by NCAs and discourage national gold-plating. Supervisory convergence is essential to achieve the Guidelines' harmonisation objective and avoid fragmented expectations across Member States.

- **Adjust Transitional Arrangements.** The proposed two-year remediation period is insufficient given the scale of impact. We therefore urge the EBA to amend the transitional arrangement so there is a 9-month window between publication of the guidelines and the incorporation of the obligations into contracts due for renewal. Thereafter, we would recommend that remediation is required by whichever is latest: the next contracting event or two years from the date of application.

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

While overall the subject matter, scope of application and some of the definitions are sufficiently clear, we do have some high-level comments on the approach being taken in these draft guidelines (the "guidelines") that we would like to highlight. The executive summary of the guidelines makes clear that the expansion of the prior outsourcing guidelines to cover all TPSPs is intended to ensure "financial entities to continue to effectively strengthen their governance arrangements including their operational resilience". While we understand that the extension of the EBA outsourcing guidelines from ICT to all third-party arrangements is consistent with broader TPRM regulatory trends globally, we believe it is essential that the final guidelines embed much more proportionality within them, while remaining risk-based. In our view, this is essential given the heterogeneous types of firms falling under scope and the volume of arrangements as well. This will help ensure that the framework remains operationally feasible for firms and supervisors and allows for the most material services to be managed and overseen effectively, aligned with the nature, scale and complexity of firms. To support this objective, we believe that there are opportunities to strengthen the proportionality embedded within the requirements related to contractual arrangements and the Register of Information among others. Such an approach would also align with the EU's current simplification agenda, which is a unique opportunity for EU institutions to rationalize their approaches to the risks posed by the EU financial sector in order to ensure controls remain strong, but also not unduly burdensome.

In this regard, we welcome the objective of trying to align these draft guidelines with DORA, which can help harmonise regulatory requirements and supervisory expectations on third party risk management across ICT and non-ICT arrangements. To better achieve this objective, however, we believe that the guidelines could be further adapted by removing elements of the 2019 outsourcing guidelines to more fully align with DORA (see below). At present, we believe the layered approach risks introducing further complexity into the regime that goes beyond DORA and which undermines the wider EU effort around regulatory simplification. In particular, the current approach to CIF identification could complicate firms' efforts to streamline their assessments and maintain consistency with DORA. We would also highlight challenges with:

- **Scope & Exclusions:** More broadly we would underline that because the guidelines now extend beyond outsourcing arrangements to all third-party arrangements, this constitutes a material change in the regulatory perimeter contrary to what has been outlined in the impact assessment of the draft guidelines, as institutions will be required to apply risk assessments, monitor and renegotiate the terms of a significantly larger universe of contractual relationships than under the original framework. This expanded scope will capture both many of the already regulated financial services that a firm receives and already assesses pursuant to existing risk calibrated criteria as well as numerous providers of

ancillary/low risk services, generating disproportionate compliance burdens on firms compared to the risks involved. We therefore believe that the scope of the updated guidelines should embed significantly greater proportionality so that the concept of risk-based regulation is retained. Additionally, we believe greater clarity is required on the categories of services that can be excluded. While paragraph 32f makes clear certain low risk services are out of scope of the Guidelines, it would be useful if it was clarified that the list of services outlined are only illustrative and that firms can take a risk-based approach to the exclusion of other low-risk services provided they are justified and can be demonstrated. This would help reduce the compliance burden for firms with multiple intra-group arrangements, without detriment to sectoral resilience given existing regulatory coverage and oversight of these services.

- **Faithful implementation by NCAs.** We also believe that the EBA strongly encourages NCAs to closely implement their requirements and avoid the imposition of additional requirements or deviations. In our view, one of the main objectives of the guidelines is to harmonise TPRM expectations across the EU. It is therefore critical that NCAs implement the GLs in a consistent manner. Differences between NCA implementation can have an impact on firms operating across multiple member states, as has been shown as part of firms' implementation of the DORA requirements. As such, during the implementation phase we would encourage the EBA to monitor and guide NCAs in the implementation as a way to support supervisory convergence and avoid any goldplating measures that go beyond the framework established by the EBA. This will be particularly important as firms operationalise requirements for the broader population of third-party arrangements now in scope. Such consistency is also essential to delivering on the EU's broader objective of regulatory simplification and reducing unnecessary burdens on firms.

Additional comments on specific aspects of the guidelines:

- **Critical or important functions.** While the definition of CIFs reflects the definition in DORA, the guidelines retain the 2019 test and the categories of functions that should be presumptively considered CIFs (e.g., certain internal control functions or authorized banking and payments activities), adding prescriptive requirements not within DORA. In our view, this risks inconsistent assessments of CIFs and diverges from the objective of aligning the EBA guidelines with DORA. Moreover, this approach is likely to complicate firms' efforts to streamline their CIF assessment. The test should be fully aligned with DORA for consistency and simplicity. Having this aligned would be helpful to avoid any interpretation issues left to financial entities. Alignment will help drive consistencies in the process and the way risk is managed. As proposed it is likely that firms will either have to maintain two separate definitions of CIF for DORA and the TPRM requirements, or that they will have to fundamentally change their approach to identifying CIFs for DORA, which would be extremely disruptive for limited benefit. Although the Guidelines stress that these criteria are optional and meant only to guide firms, in practice supervisors often treat such guidance as binding obligations. By now, most institutions have already built their CIF identification frameworks around the DORA standard, and reopening the exercise would undermine consistency and add unnecessary complexity. For this reason, we recommend that paragraphs 34–37 be deleted so firms can continue using and refining their DORA-based approach. If the EBA decides to preserve this material, it should issue an explicit clarification that the extra criteria are illustrative only, that they

do not expand the DORA definition, and that they should not be applied as mandatory. Without such reassurance, firms will face overlapping approaches to CIF assessments across third-party risk management and CIFs within an operational resilience framework, creating avoidable complexity and divergent supervisory practices.

- **Definition of Subcontracting.** The Guidelines continue to use the 2019 definition of subcontracting, whereas within DORA it applies only to material subcontractors underpinning CIFs or material parts thereof. Treating all subcontractors as material is not proportionate or risk-based, which will ultimately divert resources away from other internal projects, while diverging from the DORA framework. In our view, the guidelines should align terminology and approach with DORA to ensure harmonisation and consistency.

- **Contractual provisions.** The expectations on contractual provisions in the GLs closely align with the requirements set out in Article 30 of DORA, including in the application of enhanced requirements for arrangements supporting critical or important functions (CIFs). At the same time, the GLs retain certain elements from the 2019 EBA Guidelines, and certain provisions only partially reflect DORA's expectations or language and form. This includes phrases such as "*impediments capable of altering the performance (...)*"; for clarity, these carry-overs should be swapped for the DORA wording "*circumstances evidenced throughout monitoring deemed capable of altering performance*" under 28(7)(c). The EBA should ensure absolute consistency between the GLs and DORA, except to the extent that the provision is ICT-specific. In this regard, we welcome the removal of the 2019 data security terms, penetration testing requirements and ICT-specific termination triggers from the 2019 EBA Guidelines that have no DORA counterpart.

- **Register of information** Requirements related to the data to be maintained in the register of information should not exceed nor deviate from the requirements for the DORA RoI. More specific comments about the RoI can be found under Title III.

Further clarification would also be welcome in several respects:

1. **ICT vs non-ICT delineation**. The obligation to distinguish between predominantly ICT and non-ICT services is artificial in the context of contracts for multiple services and adds administrative complexity and burdens without risk-management benefits. In practice, because of the subjective nature required in the designation process, this could result in supervisors applying different expectations in this regard. This creates uncertainty for firms managing complex arrangements involving multiple functions and will necessitate firms making subjective assessments to distinguish what is "predominantly" ICT and justifying their classifications. In our view, the approach outlined in the draft has limited value from a risk management perspective where oversight expectations are aligned and risks are comparable. This introduces unnecessary complexity and operational burden, especially for multi-functional services that span both ICT and non-ICT elements. 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.

2. **Third-party arrangement definition**: The definition of a "Third-party arrangement" should consider the aspect of a "recurrent or an ongoing basis" for the services provided, in line with the definition of outsourcing arrangement. A third-party arrangement should qualify as such only when the third-party service provider provides it on an ongoing basis.

3. **Application and transitional period**: The proposed two-year remediation period for all in-scope arrangements is going to be operationally challenging based on experience from DORA. Although the EBA impact assessment suggests the Guidelines will have limited overall impact, we believe this is underestimated given the number of new arrangements potentially falling in scope. We therefore urge the EBA to amend the transitional arrangement so there is a 9-month window between publication of the guidelines and the incorporation of the obligations into contracts due for renewal. Thereafter, we would recommend that remediation is required by whichever is latest: the next contracting event or two years from the date of application. As not all contracts follow a 1–2-year renewal cycle that would neatly align with the 2-year transitional arrangement proposed, by aligning it with the next contracting event as an outer limit (provided it was after the two-year transition) would avoid unnecessary administrative burden. In the majority of 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.

4. **Use of a TPSP for the provision of CIFs**. There are a number of points in the proposed requirements where the EBA refer to firms using a TPSP for the provision of a CIF, or the provision of banking services. It is unclear in these instances whether the ESAs intend that such provision apply only to where an entire CIF / banking service is provided by a TPSP, or if any TPSP supporting such a service would be considered to meet this definition. The latter would be extremely disproportionate in our view. We would encourage the EBA to leverage wording similar to that provided under DORA (e.g. TPSPs providing a CIF / banking service or material parts thereof) to delineate which TPSPs are material to those services and also adopt and align consistency in terminology. We would see the following as particularly relevant from this perspective:

- **Function:** refers to the financial entities own functions, operations or business lines (i.e., consistently with 'critical or important functions' which are framed around the key services provided by a financial entity);
- **Service:** refers to the service delivered by the third-party service provider to support the entities 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.

Without such clarity and alignment, the interchangeable use of this terminology will likely create unnecessary complexity, for example:

- **Paragraph 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 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).

- **Intragroup vs external third-party service providers.** The GLs do not sufficiently reflect the generally lower risk profile of intragroup outsourcing compared to external TPSPs. The somewhat unbalanced approach may discourage the use of efficient and well-controlled intragroup models. It should be ensured that supervisory expectations are proportionate to the actual risk profile, avoiding unnecessary burdens on intragroup arrangements that already benefit from integrated oversight. In the "Background and rationale" Section of the GLs Consultation paper, concerns over concentration risk, subcontracting, and operational complexity are more valid in the context of external TPSPs, where oversight is more limited and contractual enforcement may be weaker. Supervision and concentration risks raised in paragraphs 34 and 35 of the Section are in fact more manageable in intragroup arrangements. Such arrangements benefit from shared governance structures, aligned incentives, and integrated compliance frameworks, which significantly reduce these risks. In practice, intragroup arrangements offer greater transparency, control, and responsiveness, which mitigate many of the risks that are more pronounced in external TPSP relationships. Currently, the GLs do not sufficiently distinguish between these fundamentally different contexts. While it is briefly acknowledged in the rationale and objectives of the consultation paper that financial entities may have a higher level of control over intragroup TPSPs, this point is underemphasized and not reflected in the overall tone of the guidelines. We therefore urge the EBA to clarify in the GLs that intragroup TPSP arrangements are not only viable but often preferable, particularly for critical or important functions, when supported by robust group internal governance and risk management. This adjustment would better reflect the realities of group structures and support a more balanced and risk-sensitive regulatory approach.

2. Is Title II appropriate and sufficiently clear?

We would make the following observations and recommendations in relation to Title II.

- **Hybrid ICT and non-ICT services**. As outlined above, the guidelines establish that where a non-ICT service involves the use of ICT components, the financial entity must assess whether the ICT element is "material" in order to determine whether DORA applies. This approach creates uncertainty and operational complexity for firms managing multidisciplinary arrangements. Entities would be required to make subjective determinations as to whether a service is "predominantly ICT," leading to dual classification and duplicative oversight processes for inherently hybrid services. The proposed differentiation adds little risk-management value where oversight expectations are already aligned, and risks are comparable. We therefore propose (as outlined above) 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.

- **Exclusions from scope.** We acknowledge the helpful clarification provided by the EBA that the prudential focus, and intent of the exclusion at paragraph 32.f is to focus the scope of the Guidelines on those arrangements that have a material impact on the firm's operational risk and operational resilience. However, we remain concerned that the current language in this section, paras 30-32, may not clearly convey a materiality threshold aligned with that stated prudential objective. The reference to "risk exposures" at 32.f is potentially too broad – particularly in contrast to 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). If the intention is to exclude services that are not material from a prudential risk management perspective and to therefore set a relatively high bar and – focusing on services that could, if disrupted, materially impair the financial entity's ability to deliver its critical services or functions – we urge the EBA to clarify this threshold. 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 would also add that:
    - the drafting of paragraph 32 does not make clear whether regulated financial service providers (e.g., payment institutions such as Bizum, Swift, RedSys, FinTechs, market information service providers and electronic money institutions) are excluded where they provide functions falling within the exclusions. Clarification is needed to confirm that such providers are out of scope for those functions. Additionally, we believe that the updated guidelines should also align with the European Commission clarification in respect to the provision of ICT services from regulated financial service providers under DORA, which fall out of scope of that Regulation. Should a full exemption for regulated financial services not be possible, however, we would encourage the EBA to consider a more proportionate and risk-based approach to the contractual and oversight expectations applied to such arrangements. A simpler application of the Guidelines in these cases would support operational feasibility, whilst preserving supervisory objectives.

    - Further clarification would also be useful with respect to the list of functions which are excluded from the scope of the guidelines. For example:
        - Part a - there are numerous functions which are required by regulators to be performed by a specific third party - are they excluded under part a, like a function that is legally required to be performed by a TPSP. For example, where the regulator requires that a regulatory report is submitted by a regulated entity and only a small number of entities are regulated to perform the service. Another example would be a triparty agreement whereby its nature requires the engagement of a TPSP to enable the triparty component.
        - Part b - "global network infrastructures" is broad and it is unclear where this would apply and where it would not apply. For example, if there is a network infrastructure which is country or region specific e.g. a direct debit scheme - would the exclusion apply on this basis.

- **Critical or Important Functions.** Please see response to Q 1 where we provide further information supporting our position on the need for alignment between DORA and the GLs in respect to CIF

identification. However, if the EBA ultimately decides to maintain the additional criteria set out in paragraphs 34–37, it is essential that the Guidelines clearly state three points: first, that CIF assessments are to be interpreted strictly in line with DORA; second, that the considerations listed are intended as supporting factors rather than binding or exhaustive requirements; and third, that they must not be construed as extending the scope of CIFs beyond what DORA provides. Even with such clarification, however, there remains a real risk of divergence between CIF determinations in a third-party risk management context and those used in operational resilience, which could complicate firms' compliance frameworks.

- **The impact of the CIF assessment on operational resilience.** Introducing additional criteria for determining CIFs risks stretching the definition far beyond what was originally intended in DORA. It also risks conflating two very different categories: activities that are genuinely essential to preserving operational continuity, and those that are primarily about meeting compliance obligations. The definition is already expansive because of paragraph 33.a, which captures any function whose failure could materially undermine a financial entity's ability to meet its legal obligations. Given the wide scope of applicable laws – ranging from tax and employment legislation to environmental requirements – many day-to-day operations within a bank could technically fall under this description. While such functions are undeniably important in a control and compliance context, the threshold for CIF designation is set very low. This has the unintended effect of sweeping in functions that may involve high inherent risks but that do not underpin resilience-critical activities when one considers controls and residual risks. Applying resilience measures such as scenario testing, joint resilience exercises, or detailed incident reporting to these functions would be disproportionate and resource-intensive, without meaningfully enhancing stability. The proposed additional guidance in paragraphs 34–37 heightens this risk of an overly broad scope. For example, the internal control functions are crucial for good governance and risk oversight, yet not every control activity warrants classification as a CIF. Internal audit provides valuable assurance that systems are working effectively, but its disruption would not compromise a firm's capacity to continue core operations. By contrast, a payment processing system directly supports the functioning of the financial system and is therefore resilience-critical. Treating these two very different types of functions as equally "critical" creates the risk of misaligned regulatory requirements. In practice, firms may feel forced to establish two parallel lists of CIFs: one to satisfy regulatory expectations and another to guide actual resilience management. This dual system would add complexity and governance overheads without strengthening either risk management or operational resilience.

- **Use of TPSPs.** We fully acknowledge that in the event firms use TPSPs for certain functions/services, responsibility remains with the management body through appropriate oversight of such entities and proper internal controls. Separately, we would request further clarification might be provided with respect to the language "within an appropriate timeframe" in paragraph 47f. Does this mean the RTO or some other time period.

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

Overall, we believe this section of the guidelines is sufficiently clear and appropriate, but we would make the following observations, which we hope can be taken on board in the final draft.

- **Third Party Risk Management.** To reduce unnecessary operational complexity for financial entities we request the removal that the policy on third part risk specifically differentiates between all the limbs in paragraph 50 of the draft GLs. Many of the requirements apply consistently across the third-party types, therefore financial entities might choose to integrate parts within their policies to reduce duplication and ambiguity. In our view, this is aligned to the wider intention of alignment with DORA and reducing duplication and complexity in the regulatory framework.

- **Business continuity plans.** Paragraph 58 requires that firms implement business continuity plans with regard to TPSPs that align with the EBA Guidelines on internal governance. This represents a layer of additional obligations not foreseen under DORA and effectively constitutes regulatory "gold-plating." In order to ensure consistency with DORA and avoid divergence across Member States, this requirement should be removed. We would also point out that the current drafting of the requirements for BCP seems to assume that firms will have individual BCPs for each CIF. In practice there may be multiple BCPs relevant for a CIF, or multiple CIFs under a single BCP. We would welcome clarification from the EBA that they do not require individual BCPs per CIF, and that firms are able to structure their BCPs as fits their organisation. Finally, we assume the requirement in paragraph 55 to have in place and test appropriate business continuity plan with regard to critical or important functions provided by TPSPs only applies where the TPSP is critical to the provision of the critical or important function. There may be TPSPs which are not critical but support a CIF and assume no plan is needed in this instance.

- **Internal audit function.** It is unclear whether the audit plan should explicitly include the testing of third-party arrangements of CIFs or if the audit plan can be restricted to the entities oversight and management of such third parties. Further clarity would be welcome.

- **Data Retention.** Under the documentation requirements in para 61 the EBA include a requirement to maintain records for 5 years. A similar requirement was specifically removed from DORA on the basis that it was disproportionate, and there is no clear justification in the EBA's proposals for why this is warranted for all non-DORA TPRM. We would therefore seek its removal.

- **Documentation Requirements / Register of Information.** The guidelines seek to align the non-ICT Register of Information (RoI) with the DORA RoI for ICT services, which is welcome. We understand this aligns with the ECB's letter to significant institutions confirming that:

    - a single, unified RoI should replace the existing ECB outsourcing register from 2025;
    - scope, template and definitions will follow the DORA Implementing Technical Standards (ITS); and

- this set-up is intended to create a single point of data collection for all third-party dependencies.

However, we are concerned that the approach outlined in the CP 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 template, with data field requirements adapted to reflect proportionality and risk-based principles. Key elements of a single RoI template 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, especially non-ICT, non-outsourcing 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;

This will give an opportunity for the ESAs, EBA and NCAs to align during their implementation e.g. share common validation rules. Industry is concerned that 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.

Further detailed comments on data requirements for arrangements are outlined below:

- Para 61: The guidelines require retention of terminated third-party arrangements for five years. This obligation was removed from the final DORA text. Given existing record retention requirements generally, consistent with the principle of simplification we think this requirement could be moved completely from the guidelines.
- para 63 (b): The requirement to provide an end date and reason or the termination should not apply 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. With the register templates constantly evolving, gathering backdated information for terminated contracts would be impractical in certain cases.
- Para 63 (e): As noted above, this should be amended to refer to the "services" provided by the TPSPs.
- Para 63 (g): We support the use of LEIs for supervisory and oversight objectives. However, industry is concerned that extending the requirement to procure LEIs for all third-party arrangements, in particular non-outsourcing arrangements, will present significant challenges in practice without a clear risk management benefit. 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. 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", or allowing the use of other identifiers). This flexibility should be extended to subcontractors and their parent companies with whom financial entities do not have a direct relationship with.

- Para 63 (h): As noted above, this should be amended to refer to the "services" performed by the TPSPs to avoid ambiguity.
- Para 63 (I): 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".
- Para 64 (b): requires reporting of "dates of the most recent audits." Clarification is needed on (i) the type of audit envisaged (internal, external, supervisory, or TPSP's own audits), and (ii) whether both the last and next audits are to be reported.
- Para 64 (d): This requirement should be removed as it goes beyond both the requirements under DORA, as well as the ECB Outsourcing Register for Significant Institutions and the Central Bank of Ireland's Outsourcing Register. Additionally, the date of the last criticality assessment is already provided, which should sufficiently evidence this data field.
- Para 64 (h): This requirement is operationally challenging to assess – particularly at service level – and is likely to be commercially sensitive and the third party's confidential information. 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.

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

Broadly speaking, Title IV is sufficiently clear but we would highlight the following:

Contractual phase remarks:

- **Contractual provisions.** The expectations on contractual provisions in the 2025 GLs, closely align with the requirements in Article 30 of DORA, including in the application of enhanced requirements for arrangements supporting CIFs. At the same time, the GLs retain certain elements from the 2019 GLs, and certain provisions only partially reflect DORA's expectations or language and form. There should be absolute consistency between DORA and the 2025 GLS, except to the extent that the provision is very ICT specific. In this regard, it is good to see that the EBA has omitted the additional Data Security terms and pen testing requirements from the 2019 GL, as well as omitting the termination for ICT risk related scenarios that were in DORA. However, there is little logic to retain legacy 2019 GL wording for a provision which conceptually is the same as in DORA (e.g. "impediments capable of altering the performance…" should go and the termination right should instead repeat 28(7)(c) DORA's "circumstances evidenced throughout monitoring deemed capable of altering performance" concept). Further, given the broad number of TP arrangements now caught, even beyond the outsourcing baseline, we should be concerned that some of the requirements simply don't work in all third-party contexts. For example, the 85 (c) as well as (g) and (h) data processing and storage location, data confidentiality and data access aren't going to be

relevant for all non-ICT service arrangements especially where there is only an inbound flow of data.

- **Contractual requirements & proportionality:** 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 than outsourcing arrangements. 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, especially non-outsourcing arrangements. That is, provided a legally binding agreement is in place defining the role and responsibilities of each party, certain contractual controls would not be necessary for all third-party services.

- **Subcontracting & materiality:** The 2025 GLs retain the 2019 definition of subcontracting (previously 'sub-outsourcing', referring to subcontractors providing or supporting CIFs; however, do not adopt DORA's framing of subcontractors that 'effectively underpin services supporting CIFs' (i.e. material subcontractors). This risks a broader interpretation of what might be considered a 'material subcontractor'. As noted in industry 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. In addition, Paragraph 90 (i) requires third-party service providers (TPSPs) to notify financial entities of material changes in subcontracting arrangements "in a timely manner and as soon as possible." The guidelines should specify whether an indicative timeframe is expected, or whether financial entities retain discretion to define what constitutes "timely" in light of the service and associated risks. Additionally, we would underline that while the requirements in paragraph 91 align with DORA and current contract templates, in practice many suppliers have pushed back on this element or proposed alternative notification via consultation on suppliers websites.

- **Contractual Phase.** We would like to underline that requiring a contractual phase for every TPSP contract is inherently disproportionate and mis-aligned with actual risks in our view. Equally, given the substantial expansion of scope to all third-party arrangements, certain contractual requirements are not appropriate in every context. For example, Paragraph 85(c), (g) and (h), which mandate provisions on data processing, storage location, confidentiality, and access, are not relevant to all non-ICT service arrangements – particularly where the service involves only an inbound flow of information and no processing of client or confidential data. To maintain proportionality, such requirements should apply only where the nature of the service makes them relevant. We would also underline that the "single contract" requirement outlined in paragraph 84

is not practical. Many firms leverage a more complex legal structure such as having master agreements in place, with individual contracts or service agreements for individual services. It is not clear what benefit having a single contract would provide, however this requirement would be extremely disruptive and disproportionate. Furthermore, under DORA only TPSPs supporting CIFs were required to include specific contractual agreements, rather than all TPSPs. Requiring this for all TPSPs is disproportionate with limited benefit.

Risk assessment remarks:

- **Pre-Contractual Analysis.** Compared to the 2019 EBA Guidelines, risk-assessment duties (Paragraphs 73 and 74) now span beyond merely operational risk consideration to expressly consider reputational, legal and concentration risks as separate risk attributes. This broadens the expectation beyond a risk-based and operationally feasible approach. Under DORA (Article 5 of the RTS on the ICT Policy), these risk factors are explicitly scoped to the provision of ICT services supporting CIFs. By contrast, paragraph 74 sets out a broad expectation for the financial entity to assess the impact of third-party arrangements on all relevant risks. The risk assessment requirements should support clear alignment with DORA and a proportionate approach to scope to reduce operational complexity for firms. The draft could also spell out how institutions should calibrate those factors so that assessments do not become box-ticking exercises. We also believe that the requirement of developing scenarios of possible risk events should be removed as no such requirement exists in DORA. This will help ensure consistency.

- **Supervisory conditions for contracting with TPSPs.** As drafted paragraph 72 applies to non-EU TPSPs providing regulated services – including banking, payment services, MiFID investment services – to EU financial entities. Before any such service can be provided, there must be an effective co-operation agreement between the supervisory authorities of the EU financial entity and the relevant third country authority. This agreement must meet minimum criteria (e.g. access to data, documents, premises or personnel in third country, notification of regulatory breaches and co-operation). In our view, while we understand that supervisory authorities may wish to have such memorandums to support the exchange of information etc, we do not believe it is necessary in the context of the updated GLs. Many financial service entities receive services from TPSPs located in non-EU jurisdictions where contractual arrangements would already contain provisions allowing supervisory cooperation/exchange of information. And although many such MoUS may exist at present, such a requirement will only add additional complexity and delay to the provision of such services, with little added benefit from a risk management perspective. We believe that paragraph 72 (b) and (C) can be removed.

- **Due diligence.** The due diligence expectations should support clear alignment with DORA to avoid gold-plated expectations. Otherwise, this will create regulatory divergence, leading to operational complexity for firms. For instance, paragraph 81.c requires firms to assess geographic risk dependencies (i.e. relating to the economic, financial, political, legal and regulatory jurisdictions where the service is provided). Whilst financial entities routinely assess location-related risks (including risks linked to the jurisdiction where services are delivered and data is processed / stored) this requirement introduces a granular and disproportionate burden. This level of due diligence

goes beyond current practice and is not required under DORA. Additionally, in paragraph 79 the EBA state that due diligence should be proportionate to the criticality or importance of the relevant function. This is likely to create significant confusion, as under both DORA and the rest of the GLs, the determination of whether a function is a CIF is a binary one, rather than a sliding-scale assessment. We would suggest to maintain a binary approach for simplification.

- **ESG Risks.** In paragraph 83 the EBA require that firms consider TPSPs' ESG risks, with no consideration of prioritisation of ESG factors. In their guidelines on ESG Risk Management, the EBA specifically recognise that understanding of Climate risks is materially more advanced than other ESG factors, and that firms should take a phased approach to incorporating other factors. We would request that the EBA recognise this necessary phasing in these GLs as well.

- **Access, Information and Audit Rights.** In our view, the guidelines diverge from DORA by extending access and audit rights beyond providers of critical or important functions. Paragraph 97 requires institutions to ensure that their internal audit function may review TPSPs using a risk-based approach, and paragraph 98 requires contractual recognition of competent authorities' investigatory powers under CRD/BRRD, regardless of the criticality of the function performed. This creates a regime where non-ICT services may be subject to more onerous requirements than ICT services under DORA, which limits mandatory audit and access clauses to critical TPSPs. To ensure consistency, and to avoid over-extension of obligations with limited risk-management benefit, the contractual requirements of the GLs should be aligned with DORA.

- **Exit strategies.** Further clarification would be welcome in respect to the requirement to finding alternative suppliers in the case a firm needs to exist a third-party arrangement. At times, alternative suppliers may not exist and in such circumstances, it would be useful to have a clearly defined exemption process for firms.

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

We would like to highlight the following observations for consideration:

- **Concentration risk.** 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.

Separately, the list of examples in Annex I includes “Secretarial services” and “Travel and entertainment services.” Both are expressly excluded from the scope of the Guidelines under Paragraph 32(f), which exempts services without material impact on a financial entity’s risk exposures or operational resilience (e.g. legal opinions, cleaning, catering, clerical services, travel services, reception, secretarial support). To ensure consistency, Annex I should be amended to remove these categories or, at minimum, clarify their exclusion. Annex I lists types of services – such as “Insurance services” and “Talent acquisition & hiring” – that do not lend themselves to treatment under a risk-based third-party risk management framework. More specifically:

- **Insurance services:** The contracting of insurance policies is a legal agreement by which risk is transferred to the insurer. It does not require continuous performance by the provider and has no bearing on the continuity of critical functions. Including insurance contracts within scope is therefore inconsistent with the purpose of these Guidelines, which is to address risks arising from ongoing third-party dependencies.

- **Talent acquisition and hiring:** Such arrangements typically involve one-off or short-term services without long-term dependency or operational resilience implications.

Finally, to reinforce legal certainty and proportionality, Annex I should be amended to introduce explicit exclusions of services that are inherently low-risk and should not be captured. Such a list could include, among others: legal services, regulatory advisory, insurance policies, office premises, memberships and subscriptions, office supplies and administration, energy and infrastructure services, and standard HR-related services.