Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ABBL's Reply to the Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk (EBA/CP/2025/12)

8 October 2025

We welcome the EBA's objective of harmonising third-party risk management (TPRM) across the EU and aligning non-ICT arrangements with the Digital Operational Resilience Act (DORA). A convergent framework can support supervisory consistency, reduce duplication and strengthen operational resilience.

However, the draft Guidelines re-introduce elements of the 2019 Outsourcing Guidelines, creating a hybrid model that blurs the line with DORA, risks gold-plating and undermines simplification. The expansion of scope to all third-party arrangements further magnifies the need for clear, risk-based proportionality, so that firms are not required to apply the same level of detail to low-impact contracts as to genuinely critical functions.

We encourage the EBA to rely fully on DORA's streamlined concepts, especially for the definition and assessment of critical or important functions, subcontracting and contractual requirements. Legacy obligations should be removed to avoid unnecessary complexity.

A risk-based, DORA-aligned framework will reduce administrative burden, ensure supervisory focus on material risks, and preserve a level playing field across EU Member States while enhancing resilience where it matters most.

To effectively harmonise TPRM expectations across the EU, it is essential that Member States implement and supervise the Guidelines consistently, without introducing additional requirements at the national level. The ESAs should actively guide NCAs to ensure uniform application, supporting regulatory simplification and reducing unnecessary burdens as firms adapt to the expanded scope of third-party arrangements.

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

We agree with the objective of broadening the framework from outsourcing to all third-party arrangements and with aligning non-ICT services to DORA. This is consistent with supervisory developments across other sectors.

However, the scope expansion increases the importance of proportionality. Obligations such as the register and minimum data fields (paras. 61–64) would impose significant administrative burdens.

Proposal: To help ease the operational burden on firms given the expanded scope, we urge the EBA to require remediation by the next contracting event, rather than a fixed two-year period post-application. This approach reflects varied contract cycles and avoids unnecessary administrative

burden. In most cases firms are already substantively compliant, so they should not have to re-negotiate contracts just to update wording for the new Guidelines.

The obligation to distinguish ICT from non-ICT arrangements (paras. 7 and 50(a)) is also problematic. In multidisciplinary contracts, the classification can be subjective and resource-intensive without producing tangible supervisory benefits – particularly given regulatory expectations are substantively aligned.

Proposal: We therefore propose that the authorities allow for flexibility in classification, enabling firms to apply a consistent and risk-based approach to oversight without needing to retrospectively re-assess existing DORA-classified arrangements or justify their classifications to authorities.

Furthermore, we would like to draw EBAs attention to the fact that the inconsistent and interchangeable use of terms like "function", "service" and "activity" throughout the Guidelines creates confusion and does not align with the approach taken under DORA. 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".

Proposal: 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 – including its processes, services or activities (i.e., consistently with 'critical or important functions' which are framed around the key services provided by a bank)[1];
- **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.

We, therefore, invite the EBA to ensure consistent use of 'function', 'service', 'arrangement' and 'activity' throughout the final Guidelines, aligning with Definitions para. 16 and the treatment in Title II para. 36.

[1] This aligns with the concept of 'critical operations' in the BCBS POR (capturing the FSB's definition of 'critical functions') and the BRRD's concept of 'critical functions' (distinct from the BRRD's 'core business lines').

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

Question 2 – Is Title II appropriate and sufficiently clear? (Assessment of third-party arrangements)

We support the use of DORA's definition of "critical or important function" (CIF) (Art. 3(22) DORA; para. 33).

However, the draft Guidelines also bring back the 2019 assessment criteria and a non exhaustive list of functions that could be provided by a third-party service provider (para. 37, Annex I). This creates a "dual test" that re-introduces complexity and undermines the simplification that DORA deliberately achieved. Firms would have to map CIFs onto both old and new criteria, increasing confusion and the risk of inconsistent application. We appreciate that it may be the regulatory intent to align the CIF assessment with DORA, and provide non-mandatory considerations to support firms in their assessments under the EBA Guidelines. However, in practice, supervisory authorities may nonetheless treat these considerations as requirements *de facto* – and historically this has been the case. This could lead to inconsistent expectations across Member States and divergence in how firms classify CIFs under DORA and the EBA Guidelines – which goes directly against the objectives of the ESAs.

Proposal: Rely exclusively on DORA's definition and remove the re-imported 2019 criteria set out in para. 37 and indicative categories in paras. 34 to 36, which are unnecessary for harmonisation and supervisory convergence.

We acknowledge the helpful materiality threshold introduced in para. 32(f) and the clarification provided by the EBA at the recent public workshop that the prudential objective is to focus on a more narrow scope of arrangements that have a material impact on a firms' operational risk and operational resilience. However, the reference to "risk exposures" is potentially too broad – particularly in contrast to the substantially higher threshold of material impact to operational resilience.

Proposal: We urge the EBA to clarify the regulatory intent, including in the recitals, to ensure the threshold is understood to be relatively high and ensure that the framework remains focused on services that meet the EBA's prudential objectives and ensures the operational burden to firms remains manageable.

Finally, we would encourage the EBA to consider extending the scope of the exclusion of certain regulated financial services. The current draft excludes only a limited set of services but many financial regulated services – such as custody – are subject to dedicated regulatory frameworks and supervisory oversight. Including these services would be duplicative and will unnecessarily expand the scope the framework which is inconsistent with the objective of the Guidelines.

Proposal: We recommend that the exclusion be extended to cover a broader range of financial regulated services, provided those services are already governed by other sectoral regulation and oversight. This would align with the proportionality principle and harmonise the approach with the exemption granted by the EU Commission under DORA.

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

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

We agree that governance must remain strong when third-party providers are used. However, two provisions go beyond DORA and risk creating national overlays:

- Business continuity (para. 58): Linking TPRM continuity planning to the Internal Governance Guidelines could amount to gold-plating, echoing practices already seen in some jurisdictions.
- Documentation (para. 61): Reinstating a five-year retention requirement for terminated contracts contradicts DORA negotiations, where this obligation was deliberately removed.

Proposal: Avoid introducing obligations that were expressly excluded during the DORA process. Remove the cross-reference in para. 58 and the retention rule in para. 61 to ensure consistency with DORA and to prevent divergent national practices.

Documentation / Register requirements:

We acknowledge the flexibility offered by the Guidelines in terms of the alignment with the DORA register and appreciate the EBAs intention to take a "lighter touch" to the reporting requirements given the expanded scope of the Guidelines.

However, in practice, this approach risks creating complexity for firms and the possibility of divergence in implementation across firms and member states. A unified third-party register should be the objective, with data field requirements adapted to reflect proportionality and risk-based principles. We note that para. 63 of the CP already allows merging (or at least aligning) the non-ICT register with the DORA register and encourages avoiding discrepancies; we therefore ask the EBA to confirm that merging is permitted and that ICT-specific data fields remain optional where not applicable to non-ICT arrangements.

Specifically, this could be achieved by:

- 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
- providing 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.

Without the expectation of an aligned approach, 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.

Question 4 – Is Title IV of the Guidelines appropriate and sufficiently clear? (Third-party arrangement process)

We broadly agree with the structure of the contractual and due diligence provisions. However, several points deviate from DORA in ways that reduce clarity and proportionality:

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

Contractual provisions:

- There should be absolute consistency between DORA and the 2025 Guidelines, except to the extent that the provision is very ICT specific, or where the requirements simply do not work in all third-party context when applied to the broader population. For example, the 85 (c) as well as (g) and (h) data processing and storage location, data confidentiality and data access will not be relevant for all non-ICT service arrangements especially where there is only an inbound flow of data. The Guidelines should allow for some flexibility or optionality in the application of these requirements.
- Termination of contracts (para. 109): Although broadly consistent with Article 30 DORA, legacy wording such as "impediments capable of altering the performance" has been re-introduced. This undermines the clarity of DORA's simpler formulation.
- We support the proportionate, risk-based approach applied to contractual expectations for CIFs and non-CIFs. However, the current baseline expectations may still prove overly burdensome when applied to third-party services more broadly than outsourcing arrangements. If a legally binding agreement defines roles and responsibilities, not all contractual controls should be required—for example, data location or termination rights may not be relevant for sponsorship arrangements.

  Proposal: We suggest the EBA strengthen 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.

Subcontracting:

- Subcontracting (paras. 88–96): We note that the Guidelines did not adopt DORA's framing of subcontractors that "effectively underpin services supporting CIFs (i.e. "material subcontractors"). It is important to note that not every subcontractor linked to a CIF is deemed material – it depends on whether the subcontractor plays a material role (i.e., "effectively underpins") the service supporting a CIF). There is therefore a risk that the Guidelines diverges from DORA's risked-based focus on "material subcontractors", dilute supervisory attention, and misallocates risk management resources.

Risk assessment & Due diligence requirements:

- The EBA broadens the expectation to conduct a risk assessment beyond DORA's focus on services supporting CIFs (i.e. Article 5 of the RTS on the ICT Policy), by applying the requirement to all third-party services. This diverges from a risk-based and operationally feasible approach.

  Proposal: The risk assessment requirements should support clear alignment with DORA and a proportionate approach by limiting application to services supporting CIFs.

- Due diligence (para. 81): The requirements diverge from DORA. Whilst firms 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.

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu

Proposal:

- Limit enhanced obligations to subcontractors that are material, in line with Article 30(2)(d) DORA.
- Remove legacy 2019 wording from contractual provisions and use DORA's cleaner language.
- Clarify the rationale for the divergence in para. 81; if intentional, specify what additional supervisory benefit it delivers.

Exit strategies (Policy para. 49(h); Title IV paras. 117–119):

- We understand that documented exit strategies are required for services supporting critical or important functions only, and that testing is risk-based ("where appropriate"). We support this scope and ask the EBA to confirm this explicitly in the final text, to avoid supervisory drift into non-CIF arrangements.

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

We agree that Annex I can be useful as a classification tool.

However, in practice it risks functioning as a presumptive list, particularly when combined with the re-introduced 2019 criteria. This undermines DORA's principle-based approach, which intentionally simplified the identification of critical or important functions.

Proposal: Make clear that Annex I should not serve as a parallel CIF test. Reliance should rest solely on DORA's definition.

ABBL a.s.b.l.
R.C.S. Luxembourg: F352
EU Transparency register: 3505006282-58
Postal address: P.O. Box 13, L-2010 Luxembourg
Office address: 12, rue Erasme, L-1468 Luxembourg
+352 46 36 60-1
mail@abbl.lu
www.abbl.lu