France Post Marché – EBA Consultation Response

EBA Consultation – Draft Guidelines on the sound management of third-party risk (non-ICT services)

Reference: Consultation Paper — Draft Guidelines on the sound management of third-party risk (non-ICT)

Date: 07/10/2025

From: France Post Marché (FPM)

Executive Summary

- France Post Marché welcomes the EBA's initiative to provide a coherent, risk-based framework for non-ICT third-party risk management that complements DORA and replaces legacy approaches focused solely on "outsourcing."
- We support the broad policy objectives and, from a post-trade perspective, recommend the following adjustments to ensure clarity, feasibility and consistency with sectoral laws governing financial market infrastructures (FMIs) and regulated post-trade services:
  - Scope & proportionality: Clarify the delineation between outsourced functions and procured regulated services, and calibrate obligations using a risk-based proportionality principle.
  - Interplay with DORA: Avoid duplication with DORA registers and controls; rely on DORA artefacts where equivalent controls exist.
  - Access & audit rights: Replace direct audit/access requirements with alternative assurance and supervisory cooperation for regulated utilities.

General Comments

A. Purpose and scope (non-ICT arrangements)

We welcome the EBA's effort to bring non-ICT third-party relationships into scope, with lifecycle controls. To prevent overlap, the final text should commit to DORA-consistency and allow reuse of DORA artefacts.

B. Regulated and post-trade services

We suggest explicitly distinguishing between outsourced internal functions and procured regulated services (e.g., FMIs, depositaries, CCP access), which are subject to sectoral legislation and supervisory oversight, to be explicitly excluded from the scope of the Guidelines

In post-trade, many third parties are regulated entities or FMIs. The Guidelines should establish an assurance equivalence concept, permitting reliance on regulatory oversight, recognized assurance reports, and certifications. We strongly recommend that custody arrangements be explicitly excluded from the scope of the Guidelines, in line with the principle of proportionality and existing regulatory frameworks.

Clearing and custody services, including safekeeping, asset servicing, and fiduciary functions(which are not investment services in accordance with MIFID2), 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 (according to EBA – page 5 of the CP – no mandate to provide GL has been given to the EBA by an article of MIF2). 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

36, rue Taitbout - 75009 Paris - France
Tél. 01 48 00 52 01 - e-mail : secretariat@france-post-marche.fr - www.france-post-marche.fr
Association Loi 1901 - Siren 400 427 910 • Siret 400 427 910 00023 • Code NAF 8559A

regulatory obligations of custodians. We therefore urge the EBA to explicitly exempt clearing and custody services from the Guidelines, both in the body of the text and in Annex Iand to avoid unintended regulatory overlap.

C. Intragroup and "offshoring" framing
Expectations for intragroup services should be tailored to control realities and harmonized with DORA to enable consistent lifecycle implementation.

Specific comments

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

France Post Marché broadly supports the subject matter and objectives of the Draft Guidelines. The overall scope and definitions are generally clear; however, we recommend the following clarifications to ensure legal certainty and operational feasibility:

1. Subject matter and scope
    - The Guidelines correctly extend beyond ICT outsourcing to cover non-ICT third-party arrangements.
    - We suggest explicitly distinguishing between outsourced internal functions and procured regulated services (e.g., FMIs, depositaries, CCP access), which are subject to sectoral legislation and supervisory oversight. This distinction would prevent misclassification and unrealistic contractual expectations.
2. Definitions
    - The term "third-party arrangement" should be defined and clarify whether it includes market infrastructure relationships and statutorily mandated services.
    - Consider adding a definition for "Procured Regulated Services (PR-Services)" to reflect arrangements where assurance relies on regulatory oversight rather than bilateral audit rights.
3. Transitional arrangements
    - The proposed two-year transition period is appropriate and pragmatic.
    - We recommend confirming that legacy contracts are grandfathered until renewal or material change, with priority given to high-risk relationships.
    - Supervisory Q&A and implementation guidance within six months of final publication would support consistent application across the industry.

In summary, while the framework is directionally sound, these refinements would enhance clarity, reduce interpretative uncertainty, and ensure proportional implementation across post-trade services.

Question 2 : Is Title II appropriate and sufficiently clear?

France Post Marché acknowledges that Title II provides a structured framework for governance, risk assessment, and lifecycle management of non-ICT third-party arrangements. Overall, the principles are sound and aligned with the objective of strengthening operational resilience. However, we believe certain refinements would improve clarity and proportionality:

1. **Governance and accountability**
    - The allocation of responsibilities between management body and senior management is broadly appropriate.

- We recommend clarifying that institutions may leverage **group-level governance frameworks** where these meet equivalent standards, to avoid duplication and to ensure a greater simplification and harmonization of obligations regarding intra-group outsourcing.

2. **Risk-based approach**

   - Title II rightly emphasizes materiality, but the criteria for determining "critical or important" functions should explicitly reference **non-ICT contexts** and allow for proportional application.

   - For regulated post-trade services (e.g., FMIs, depositaries, custodians), the Guidelines should confirm that reliance on **regulatory oversight and assurance reports** satisfies due diligence and monitoring expectations.

3. **Contractual requirements**

   - While the list of mandatory clauses is comprehensive, some obligations (e.g., unrestricted audit rights) are **not feasible for FMIs or market utilities**. We suggest introducing an **"assurance equivalence" concept** to permit alternative mechanisms such as supervisory cooperation and recognized assurance reports.

4. **Consistency with DORA and sectoral law**

   - To avoid fragmentation, Title II should explicitly state that institutions may **reuse DORA artefacts** (registers, risk assessments, testing) for non-ICT arrangements where appropriate.

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

Overall, Sections 5–10 are directionally sound and provide a workable lifecycle for non-ICT third-party arrangements. That said, several clarifications would materially improve clarity, proportionality and consistency with DORA and sectoral post-trade laws. Our detailed comments by section follow.

Section 5 — Risk assessment & due diligence

- Clarity: The risk-based approach is appropriate, but the criteria for materiality in a non-ICT context should explicitly recognise arrangements with regulated market infrastructures and post-trade fiduciary services (e.g., CSD/ICSD access, CCP clearing access via GCMs, depositary services). For these "procured regulated services," institutions often rely on regulatory oversight and recognised assurance rather than bespoke bilateral testing. We recommend codifying an assurance-equivalence option where direct audit/access is impracticable.
- Consistency: Allow explicit reuse of DORA artefacts (registers, classifications, resilience testing outputs) for non-ICT services to avoid duplication and ensure one enterprise view of third-party risks.

Section 6 — Contractual requirements

- Appropriateness: The list of mandatory clauses (incident notice, change control, confidentiality, termination, sub-outsourcing transparency) is sound. However, unrestricted audit and on-site access are rarely feasible for FMIs and certain post-trade utilities; supervisory regimes and market rules limit negotiability. We suggest stating that alternative assurance (supervisory reliance, SOC/ISAE reports, public disclosures) meets the objective where bilateral audit is not available.
- Editorial suggestion: Add a note that for depositary functions (which the consultation materials flag among examples), obligations should reflect the UCITS/AIFMD framework and ESMA Q&As rather than a pure "outsourcing" lens.

Section 7 — Documentation & registers

- Clarity: The requirements would benefit from a sentence confirming that, where an institution maintains a single enterprise register under DORA (ICT and non-ICT), it may integrate non-ICT arrangements into that register rather than maintain separate ones.
- Industry feedback alignment: Industry working groups are specifically assessing the practicality of merging registers and favour a unified approach; referencing this option in the Guidelines would prevent divergent supervisory expectations.

Section 8 — Ongoing monitoring, performance, incidents

- Appropriateness: The focus on performance KPIs, service reviews, and incident management is welcome and aligns with current Group practice (including the use of cyber KPIs and structured incident triggers). For PR-Services and FMIs, allow monitoring via regulatory reporting and recognised third-party assurance where direct testing is constrained, while ensuring robust escalation pathways.

Section 9 — Sub-outsourcing

- Clarity: The section should emphasise transparency and timely notification of material sub-contractors and changes, with proportionality for PR-Services where components of the chain are non-negotiable due to market structure. Reiterate that the objective is outcome-based resilience (continuity, incident escalation, data safeguards), not one-size-fits-all contracting.

Section 10 — Exit and termination (incl. continuity)

- Appropriateness: Exit strategy expectations are appropriate for ordinary vendors, but for FMIs and certain post-trade services, substitution can be structurally constrained. The section should expressly allow resilience playbooks (graceful degradation, manual fallbacks, reconciliations, coordinated crisis communications) as acceptable “exit outcomes” when a like-for-like switch is not realistic. This mirrors DORA-oriented training and internal standards that emphasise continuity planning and exit playbooks.

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

Title IV is broadly appropriate and provides a workable framework for implementation and supervisory interaction. A few focused clarifications would materially improve consistency, proportionality, and practicality—especially where institutions already operate integrated third-party risk frameworks aligned with DORA and sectoral rules.

1) Supervisory engagement and notifications

What works: The emphasis on dialogue with competent authorities and on keeping supervisory artefacts up to date is welcome. It aligns with established governance and reporting channels many firms already use (e.g., Group-level risk committees that receive periodic summaries of outsourcing/third-party risks and material incidents).

Where to clarify:

- Notification thresholds & timing. Specify notification triggers and expected timelines for non-ICT arrangements (e.g., material incident, provider change, sub-outsourcing affecting critical services) and allow supervisory reliance on existing incident frameworks. Internal cyber-incident standards already define structured reporting flows to Risk, Compliance, and Legal; Title IV could explicitly recognise such frameworks as meeting expectations where they are documented and tested.
- Reuse of registers/artefacts. Confirm that firms may reuse DORA artefacts (registers, incident logs, resilience testing outputs) for non-ICT services, rather than maintaining parallel sets. This mirrors the consultation’s stated intent to align the non-ICT guidelines with DORA.

2) Proportionality and group approach

What works: Title IV acknowledges proportionality and group-level implementation. This is crucial for intragroup services and for entities operating a centralised TPRM/outsourcing policy (with Board-level and executive committees overseeing critical/important functions). [

Where to clarify:

- State explicitly that group-level governance, risk methodologies, and registers can satisfy Title IV where they meet equivalent standards, avoiding duplicative local overlays that add burden without improving risk outcomes.
- Encourage supervisors to assess whether the control outcomes (e.g., risk assessments completed, issues remediated, service continuity validated) are met, even if institutions use group tools and shared processes.

3) Data model and reporting consistency

What works: Alignment with DORA reduces fragmentation; a single enterprise view of third-party relationships is operationally efficient. Industry working groups are actively discussing unified registers; Title IV could explicitly permit a “single-register” option covering ICT and non-ICT, provided fields required by both frameworks are captured.

Where to clarify:

- Provide an indicative data field mapping (Annex/Appendix) showing how non-ICT entries align with DORA registers (e.g., service criticality, location, sub-outsourcing, exit strategies). This would promote consistent supervisory expectations across the EU.

4) Implementation practicality and transition

What works: Title IV’s implementation provisions are pragmatic in principle.

Where to clarify:

- Milestone-based transition. Confirm that legacy contracts can be prioritised by risk, with phased remediation and grandfathering until renewal or material change, to avoid mass renegotiations that strain operational capacity without commensurate risk reduction. Industry bodies (e.g., EBF, AFME) are coordinating input on practical staging; Title IV could reference the value of supervisory Q&A during rollout.
- Assurance leverage. Where bilateral audit/access is constrained (e.g., regulated utilities or market infrastructures), allow assurance-equivalence via supervisory reliance and recognised assurance reports, documented in the firm’s Title IV implementation plan and referenced in supervisory reporting. This dovetails with existing third-party security standards that already mandate enhanced assessments and audits for higher-risk services.

5) Incident management and continuity

What works: Emphasis on continuity and exit is consistent with operational resilience objectives.

Where to clarify:

- Interoperability with existing playbooks. Recognise that many firms run standardised cyber/operational incident playbooks and “follow-the-sun” response models; Title IV should state that documented, tested playbooks (covering escalation, communication, forensics, and recovery) meet expectations for non-ICT incidents affecting critical services.

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

We understand Annex 1 contains examples of third-party services. For sake of clarity, we recommend adding a new exemption in Article 32 that would specifically exclude Procured Regulated Services (PR-Services). Consequently, regarding Annex I, PR-Services (including Depositary tasks and administration for collective investment schemes and securities) should be removed from the list. This list is intended to present functions captured by the Guidelines, and regulated safekeeping duties (Depositary tasks for UCI - Cash flow monitoring and Depositary tasks for collective investment schemes - Oversight duties) are by nature not outsourcable (UCITSD, article 22a paragraph 1 and AIFMD, article 21 paragraph 11).

As well, asset servicing functions (such as central administration for collective investment schemes - Client communication, net asset value calculation and accounting, transfer agency services) should be excluded to ensure a proper level playing field : these services can be provided by entities that do not have the status of banks or investment firms. There would therefore be a difference in treatment between banks offering these services (and subject to the Guidelines) versus entities that would not be.