European Payment Institutions Federation aisbl

EBA Draft Guidelines on the Sound Management of Third-Party Risk (Non-ICT) – EPIF Position

Executive summary

EPIF welcomes the EBA's objective to enhance supervisory transparency and convergence for non-ICT third-party arrangements. However, we recommend four refinements to improve proportionality and efficiency for both supervisors and in-scope entities:

- **Registry vs. notification obligations:** Maintain the Section 10 documentation principle and rely on periodic registry submissions (plus targeted supervisory engagement) and suggesting the avoidance of systematic ad-hoc notifications for relevant arrangements.
- **Section 4 clarity:** Make the criteria for "material impairment" more explicit and provide illustrative consequences, together with examples of critical functions to promote harmonized classification.
- **Scope delineation:** Include an illustrative list of out-of-scope services and lead a supervisor-led consultation to publish a non-binding taxonomy of typically non-critical, non-ICT categories.
- **Additional guidance on subcontracting and ICT dependencies:** We recommend the EBA clarify what in-scope entities can reasonably require from third-party providers regarding subcontractor oversight. Also, guidance is needed in relation to the management of cases where a non-ICT vendor relies on an ICT subcontractor. Considering the possible convergence between the non-ICT framework and DORA, there is a need to seek proportionate solutions.

1) Registry vs. Notification Obligations

Position

We support the Section 10 documentation requirement whereby firms maintain comprehensive records of non-ICT third-party arrangements in scope of the guidelines. However, the guidelines could clarify whether it is recommended that Member States avoid introducing systematic notification duties for CIF-supporting arrangements and instead rely on (i) maintenance and periodic submission of the registry and (ii) targeted supervisory engagement (e.g., a request for a meeting or deep-dive where needed).

Why does this improve supervision and industry practice?

- Supervisors can monitor all changes efficiently using a single, high-quality registry and trigger focused reviews when warranted.
- In-scope entities can concentrate resources on (a) sound management of critical relationships, (b) accurate registry upkeep, and (c) clear, transparent delivery of information—rather than duplicative notifications.
- Avoids administrative burden with no loss of risk visibility.

Implementation suggestion.

The EBA should consider issuing detailed guidance to supervisory authorities regarding the appropriate methodologies for overseeing the registries maintained and periodically updated by in-scope entities.

2) Section 4 — Clarifying "Material Impairment" & Examples of Critical Functions

Position.

Section 4 should more explicitly define when a third-party failure would materially impair: a) continuing compliance with authorization conditions or other financial-services obligations; b) financial performance; or c) the soundness or continuity of services and activities.

What to add?

- Criteria & consequences: The EBA could provide guidance and examples of when it is considered that there is a material impairment, with non-exhaustive examples such as: a significant regulatory infringement (e.g., leading to supervisory measures or sanctions); a demonstrable impact on financial performance (e.g., a defined turnover or cost threshold over a set period); service continuity events (e.g., an outage or backlog that prevents delivery of regulated or core services). These are illustrative, not prescriptive, and would calibrate risk assessments across markets.
- Examples of CIFs: The EBA could include non-exhaustive examples of functions that should commonly be treated as critical. Additionally, the EBA could collect information from supervisors to identify the most common CIFs reported under the current EBA Outsourcing framework and include such CIFs as examples. This will help to codify common practice and foster convergence between Member States and supervisors.

Benefits.

- Clear materiality signals reduce interpretative variance, guide contracting/monitoring intensity, and support predictable supervisory outcomes.

3) Scope Delineation — Out-of-Scope Examples & Supervisor-Led Taxonomy

Position.

Given the scale of non-ICT services, the EBA should provide an illustrative (non-exhaustive) list of arrangements that are ordinarily out of scope, beyond those covering the limited set of functions that are currently provided for in paragraph 30 and 32 of the Consultation Paper —i.e., services unrelated to regulatory/management-compliance or core business activities, and which cannot reasonably affect an in-scope entity. This prevents over-capture of low-risk vendors and sharpens focus where it matters.

Supervisor-led taxonomy.

We propose the EBA convene competent authorities to compile a non-binding, living taxonomy of commonly encountered non-ICT functions, which can remain out of the scope, considering the principle of proportionality. Publishing this guidance would harmonize expectations and reduce interpretative gaps across Member States, while preserving proportionality.

Benefits

This would enhance clarity on what is ordinarily out of scope, reducing interpretative divergence across supervisors. Consequently, it would avoid the overcapturing of low-risk vendors and sharpen attention on concentration risks. This allows supervisors to maintain the focus on targeted activities, and reduces the administrative burden for firms and supervisors, while preserving transparency and accountability.

4) Guidance on Managing Subcontractors and ICT Dependencies in Non-ICT Chains

Position.

We urge the EBA to provide specific and practical guidance on how in-scope entities should oversee their third-party providers, especially regarding the due diligence and monitoring of subcontractors. This guidance would help Member States apply consistent standards for subcontractor oversight. In most cases, oversight of subcontractors is carried out through the direct vendors, since in-scope entities typically do not have a direct contractual relationship with fourth parties. It is important to recognize that obligations applying to critical third-party providers also extend to critical subcontractors, and that in-scope entities remain accountable for these functions. However, there is a clear need for further direction on how these oversight responsibilities should be managed in practice. For example, Member States would benefit from explicit expectations on how in-scope

entities can fulfill their due diligence obligations, such as the types of evidence they should collect to confirm compliance by subcontractors.

Furthermore, situations may arise where a non-ICT third-party contracts an ICT subcontractor, which could create overlap between the non-ICT framework and DORA. Guidance on managing these cases would help in-scope entities determine the appropriate actions.

What to add?

- Guidance on how in-scope entities should exercise the oversight of subcontractors through their direct third-parties to ensure subcontractor compliance.
- Provide guidance on how to address ICT subcontractors within non-ICT chains (e.g., a non-ICT vendor supporting AML obligations that uses a cloud provider for data storage), including whether DORA-equivalent controls should apply and how to reflect this in registries and contracts.

Benefits.

- Legal and operational clarity: Defines what is enforceable and proportionate for in-scope entities, considering the operational aspects, without requiring direct control over 4th parties.
- Framework convergence: Ensures consistent treatment where non-ICT arrangements involve ICT components, reducing regulatory overlap and uncertainty.