Wise response

EBA Consultation Paper - Draft Guidelines on the sound management of third-party risk with regard to non-ICT related services

Contact details: policy.emea@wise.com

Consultation questions & responses:

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

Wise response:

Yes, our institution finds the proposed subject matter, scope of application, definitions, and transitional arrangements to be both appropriate and sufficiently clear.

As a payment institution that has fully integrated the existing EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) into our third-party risk management and compliance frameworks, the proposed revisions represent a logical and coherent evolution of the current requirements, particularly in the context of the application of the DORA (EU 2022/2554).

The revised guidelines effectively delineate the supervisory expectations for outsourcing arrangements involving functions that are not ICT services, thus clarifying the regulatory perimeter for arrangements that fall outside the direct scope of DORA.

2. **Is Title II appropriate and sufficiently clear?**

Wise response:

No, while Title II, "Assessment of outsourcing arrangements," provides a clearer framework, certain areas require further clarification and refinement to be considered fully appropriate and clear.

We acknowledge the improved clarity brought by defining "outsourcing" as a specific subset of the broader "third-party arrangement" category. The explicit exclusion of global network infrastructures (e.g., Visa, MasterCard) and correspondent banking services is a welcome and logical development that reflects the unique nature of these arrangements.

However, we believe the logic underpinning these exclusions should be extended. We propose that services provided between regulated financial institutions should also be explicitly excluded from the definition of outsourcing. These arrangements are fundamentally different from typical outsourcing, as the service provider is itself a supervised entity subject to prudential requirements. Applying the full scope of outsourcing guidelines to such relationships

creates a duplicative supervisory burden without a commensurate increase in risk mitigation. Some examples include:

- A payment facilitator processing transactions through a commercial acquirer;
- A payment institution using a credit institution for the safeguarding of client funds as required under PSD2;
- An E-Money Institution (EMI) partnering with a bank for the issuance of IBANs linked to their e-money accounts.

Additionally, while we agree with the principle of Paragraph 27[1] (that arrangements with multiple functions require a holistic assessment) it introduces significant ambiguity when dealing with hybrid services.

The paragraph and its accompanying footnote state that it is the financial entity's responsibility to determine if an ICT service within a broader third-party arrangement is "material" enough to trigger the DORA framework. This guidance is insufficient and could lead to inconsistent application.

We request more granular guidance or specific criteria on how to assess the materiality of embedded ICT "microservices" within a predominantly non-ICT service arrangement. For example, if a non-ICT service like physical document archiving includes a minor cloud-based portal for tracking, it's unclear how an institution should determine if this component makes the entire arrangement subject to DORA. Further clarity is essential to ensure a proportionate and consistent application of the DORA framework without placing an undue burden on the assessment of non-critical ICT components.

Additional Concerns

34. When relying on a TPSP for operational tasks of internal control functions, financial entities should always consider such tasks as critical or important functions, unless the assessment establishes that a failure to provide the tasks or the inappropriate provision of the tasks would not have an adverse impact on the effectiveness of the internal control functions.

Concerns:
Does the definition of "reliance" in this context align with its interpretation in DORA/RTSs, given that "reliance" is a broad concept open to various interpretations?

To what extent can reliance on third parties for operational tasks satisfy the initial requirement?

Ask:
Clearly define 'reliance' and its constituent components within the 'Definition' section.

---

35. When financial entities intend to use TPSPs for the provision of functions of banking activities or payment services or issuance of ARTs as defined in Article 3(1), point (6), of

[1] Where an arrangement with a service provider covers multiple functions, institutions and payment institutions should consider all aspects of the arrangement within their assessment, e.g. if the service provided includes the provision of data storage hardware and the backup of data, both aspects should be considered together.

Regulation (EU) 2023/1114 to an extent that would require authorisation by a competent authority, they should automatically consider such function as critical or important.

Concern:
The current binary criteria applied to banking activities and payment services disproportionately impact providers. For instance, a small banking service provider, despite handling low volumes and posing minimal risk in the event of failure, may be subjected to overly extensive controls.

This approach would be disproportionate and excessive in terms of requirements implementation and it can not be considered as aligning which key principle of the Regulation.

Ask:
Re-consider updated version with the potential removal scenario of: '*they should automatically consider such functions as critical or important*' and keep this in the version of 2019 Guidelines.

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

Wise response:

Paragraphs 67-68 of Section 10 in Title III of the draft Guidelines provide guidance on the preliminary notification of third-party arrangements to the competent authority. This guidance makes a specific reference to Article 19(6) of Directive (EU) 2015/2366, which requires payment institutions to communicate their **upcoming outsourcing agreements to the competent authorities.** The guidance, however, omits a reference to the similar obligation under Article 28(3) of Regulation (EU) 2022/2554 which requires financial entities to inform the competent authority about any **planned contractual arrangement on the use of ICT services supporting critical or important functions.** Given this omission, it is unclear if a financial entity subject to both regulations should treat these as two separate notification obligations required to be fulfilled independently, or if a single, merged notification process is foreseen pursuant to the current draft guidance?

Regarding paragraph 67, preliminary notification requirements also apply to sub-contractors supporting critical or important functions, in the case where a financial entity that is part of a group to which the entity outsources support of critical or important functions and the group further sub-contracts support of critical or important functions to TPSPs. Does the requirement apply only to the direct outsourcing arrangements of the financial entity, or does it extend to the sub-contracting of critical or important functions of the parent company?

Do the governance requirements included under Title III (due diligence, exit plan, etc) also apply to sub-contractors of TPSPs supporting critical or important functions, in the case where a financial entity that is part of a group to which the entity outsources support of critical or important functions and the group further sub-contracts support of critical or important functions to TSPs. Does the requirement apply only to the direct outsourcing arrangements of the financial entity, or does it extend to the sub-contracting of critical or important functions of the parent company?

On a separate topic, while the prospect of maintaining a single, unified register for both ICT and non-ICT third-party arrangements is a positive development that could streamline reporting, significant clarification is needed on the operational and technical expectations.

The introduction of a potentially unified register presents a critical opportunity to reassess and simplify the associated reporting obligations. We strongly advocate for a material reduction in the volume and granularity of the information to be provided in the register. The focus should be on essential data points that are proportionate to the objective of supervisory oversight, thereby reducing the administrative burden on financial institutions, as alluded to in the EBA's own communications.

Furthermore, a clear implementation roadmap is essential to ensure a smooth and effective transition. Drawing from the industry's experiences with the DORA ROI, we formally request that the EBA provides an adequate transitional period, publishes any final Regulatory Technical Standards well in advance of the application date, and makes a dedicated testing environment available. Proactively providing these elements is crucial for preventing ambiguity and ensuring a successful, efficient rollout across the financial sector, especially in consideration that this would implicate in plausible changes to already-existing controls created for DORA compliance.

Additional Concerns

42. The use of TPSPs for the provision of functions cannot result in the delegation of the management body's responsibilities. Financial entities remain fully responsible and accountable for complying with all of their regulatory obligations, including the ability to oversee the use of TPSPs for the provision of critical or important functions.

44. The use of TPSPs should not lower the suitability requirements applied to the members of the management body of financial entities, senior management including key function holders, and persons responsible for the management of the payment institution.

Concern:
If a financial institution is fully responsible for managing responsibilities and not allowed in delegation of the responsibilities (42), how can the use of TPs potentially lower suitability requirements?

These two points partially contradict each other. Hence, theoretically, these responsibilities can be delegated to a third party, provided they adhere to the same internal standards.

Ask:
This can create confusion and need better clarity over what 'The use of TPSPs should not lower the suitability requirements' actually means, the wording on this might be simplified to avoid 'grey areas' creation.

---

63. d. the outcome and date of the last assessment performed of the TPSP's substitutability (as easy, medium, highly complex or impossible to substitute);

Concern:

Not clear what criteria is used to differentiate ‘easy, medium, highly complex or impossible to substitute’ and may result in unclarity.

Ask:
Provide definition of ‘substitutability’ within the 'Definition' section.

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

Wise response:

No, while we agree with the objective of strengthening the governance framework, the guidance in Title IV is not sufficiently clear or appropriate regarding its practical implementation, particularly concerning the new contractual provisions.

The guidelines substantially elevate the requirements for minimum contractual provisions in outsourcing/TP agreements. While this strengthens oversight, it simultaneously creates significant practical challenges for institutions in contract negotiation and lifecycle management.

The process of renegotiating contracts to meet new regulatory standards is a complex, resource-intensive task (as the industry recently experienced with the implementation of DORA). This challenge is magnified by the significant negotiation asymmetry that exists when dealing with large, international service providers who often present non-negotiable, standardized terms, largely delaying remediation processes and compliance with the new regulation.

To address this, we strongly recommend that the EBA develop and issue guidance on standard contractual clauses. This would not infringe upon the contractual freedom of parties. Instead, it would be a proactive measure to facilitate compliance by establishing a clear, authoritative baseline for what is expected. Such clauses would empower financial institutions to negotiate from a more equitable position and ensure that the EBA's own strengthened requirements are met consistently across the market.

A single, fixed transitional period for all existing contracts is insufficient. We propose a more pragmatic approach to implementation. Specifically, we request a longer, dedicated transitional period for contracts that have been recently signed or are due for renewal within the first year after the guidelines' publication. This flexibility would allow for a more orderly negotiation process, reduce the immediate compliance burden, and acknowledge the practical realities of managing extensive contract portfolios.

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

Wise response:

Yes, our institution finds Annex I to be appropriate and sufficiently clear.

The format of a non-exhaustive list of examples is a practical and well-understood approach for providing guidance. As this structure is consistent with the framework of the previous 2019 guidelines, it ensures continuity and allows for a straightforward interpretation.

We believe the Annex provides adequate direction for institutions to determine which services fall within the scope of the guidelines.