Response to EBA consultation paper on EBA Draft Guidelines on the sound management of third-party risk

Question n. 1

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

Subject Matter

- Subcontracting due diligence:

The guidelines appear to require financial entities not only to assess whether a TPSP is delivering a critical or important function, but also to assess whether any subcontractors engaged by that TPSP are performing such functions. While we understand the importance of managing subcontracting risks, this requirement could place a significant operational burden on financial entities—especially when dealing with large or layered third-party ecosystems. Taking into consideration the principle of proportionality and the context of regulatory simplification considerations we suggest that the GL do not apply to TPSP's subcontractors. Or, at a minimum, that further guidance is provided or a risk-based approach is introduced to support eventual implementation.

- Audit rights for future criticality:

The current wording—"T*he right to audit is key for providing the appropriate assurance that at least critical or important functions provided by TPSPs, as well as functions that may become critical or important in the future…*"—raises concerns about clarity. It is not always straightforward to determine whether a function may become critical or important in the future. Assessment of criticality should be performed taking into consideration the information available at the time and the present criticality or importance of the function during the assessment, we therefore suggest this wording should be deleted.

Scope

- Overly broad TPSP definition:

The current definition of TPSPs is overly broad and does not allow institutions to exclude providers that are irrelevant for supervisory purposes. Unlike outsourcing or ICT definitions, it lacks flexibility for institutions to apply judgment based on risk and relevance. We suggest narrowing the scope to suppliers delivering services directly linked to financial services, enabling institutions to focus on material risks. The expansion of scope to all third-party arrangements will substantially increase the volume of contracts subject to oversight, many of which are low-risk. This creates a significant operational burden and may divert resources from managing truly material risks. This scope expansion may also lead to regulatory divergence, placing EU financial entities at a competitive disadvantage compared to institutions in jurisdictions with more targeted third-party risk frameworks. A clearer categorization of services—potentially through a whitelist or exclusion criteria—would help institutions focus on arrangements that genuinely warrant supervisory attention.

Clarification of Exemptions:

The GLs could provide clearer and more consistent exemptions. For instance, it is unclear why only correspondent banking services are explicitly exempted, while other banking services are not. This selective approach raises questions and may lead to inconsistent application across institutions. A more transparent exemption framework would help entities better understand the scope of the Guidelines and avoid unnecessary compliance efforts for low-risk or well-established service categories.

- Intragroup arrangements:

Applying the same framework to intragroup arrangements is disproportionate. While point 24 acknowledges that financial entities may have a higher level of control over intragroup TPSPs and can factor this into their risk assessment, this recognition is not sufficient. Simply allowing institutions to "take it into account" still places the full burden of assessment and compliance on each entity, regardless of the nature or structure of the group. We believe the Guidelines should go further by allowing a risk-based approach and exclude intra group arrangements from the GL's application. Intragroup TPSPs often operate under shared governance, policies, and compliance structures, which should allow entities to rely on group-level assessments and controls rather than duplicating efforts.

A comment regarding the EBA conclusions set out in S*ection 5.1, E. Cost-benefit analysis - Table 1. Costs and benefits*:

While credit institutions and investment firms subject to the CRD may already fall within scope, the assertion that the additional costs are negligible does not hold in practice. The updated guidelines significantly broaden the scope by explicitly including third-party arrangements (TPAs) that were previously out of scope or not subject to the same level of scrutiny. As a result, existing contracts will need to be reassessed and, in many cases, renegotiated to meet the new requirements. This process involves legal review, operational alignment, and potentially complex discussions with suppliers—who are likely to reflect these compliance efforts in their pricing. These costs will not only arise at the time of entering new agreements but also when reopening or amending existing arrangements to ensure compliance with the updated deadlines and expectations.

Definitions

- Definition of "Third Party Arrangements"

We propose limiting the definition of third-party arrangements to services performed "on a recurrent or ongoing basis." This would help avoid disproportionate obligations for short-term or one-off arrangements that pose minimal risk, ensuring a more proportionate and practical application of the Guidelines.

We also propose including in the definition of Third-party arrangements the exclusion of "services that do not have a material impact on the financial entity's risk exposures or operational resilience.

To support consistent application, the Guidelines could:

1. Introduce a time-based threshold (e.g. contracts shorter than 12 months) below which third-party risk management requirements would not apply, unless the service is critical or high-risk. This would ensure a more proportionate and risk-based approach.

2. Introduce a materiality threshold to help Financial Entities focus their risk management efforts on arrangements that genuinely warrant supervisory attention. However, defining a fixed, one-size-fits-all threshold is inherently challenging, as materiality can vary significantly depending on an entity's size, structure, and business model. Conversely, leaving the threshold entirely open to interpretation—based solely on proportionality or internal judgment—could introduce additional complexity and inconsistency in implementation. A more balanced approach could involve setting out guiding criteria or reference points (e.g. contract value, duration, or strategic relevance), while allowing institutions the flexibility to calibrate thresholds based on their specific context.

- ICT services:
It will be important for Authorities to provide a clear and consistent definition of what constitutes ICT services. As it stands, different interpretations of ICT are still co-existing across entities and regulatory texts, which creates uncertainty in implementation and compliance. A harmonized definition would help ensure that institutions correctly identify which services fall under ICT-related requirements—particularly in distinguishing between those governed by DORA and those subject to other supervisory frameworks. Additionally, for multidisciplinary setups, the taxonomy provided may feel forced and inefficient, offering limited practical benefit for managing risk.

- CIF Definition and Test:

While the GLs adopt DORA's definition, they retain the 2019 EBA test and criteria, which are more prescriptive and diverge from DORA's streamlined approach. Full alignment is needed to ensure consistency in CIF assessments across ICT and non-ICT services.

- Hybrid entities:

It would be important for the guidelines to clarify the treatment of "hybrid entities"—that is, third-party service providers offering operational services with embedded IT components, such as platforms or technology-enabled business services. These entities may not fall neatly into either ICT or non-ICT categories, which creates uncertainty regarding which regulatory framework applies (e.g. DORA vs. EBA/ESMA guidelines). A clearer definition or guidance on how to assess and classify such hybrid services would support more consistent implementation and oversight.

- Closely connected TPSPs:
The term "*closely connected Third-Party Service Providers (TPSPs)*" is used in the guidelines but lacks a clear definition. To ensure consistent interpretation and application, it would be helpful for the guidelines to provide a precise definition or illustrative examples of what constitutes a closely connected TPSP. Clarifying this term would support institutions in correctly identifying which arrangements fall under this category and applying the appropriate level of oversight and risk management.

Transitional Arrangements

2-year review for TPA involving CIFs:

We would like to raise concerns regarding the proposed two-year review period for third-party arrangements involving critical or important function (paragraph 19). This timeline poses significant challenges, particularly for newly in-scope entities, where the review process may require substantial changes to internal policies, governance structures, and operational workflows. The short implementation window risks operational disruption and increased compliance costs, especially considering the experience with DORA. We therefore recommend extending the deadline for reviewing and remediating existing third-party arrangements to ensure a more feasible and proportionate transition.

Transitional provisions for non-outsourcing TPA:

We also suggest that the transitional provisions be layered and distinguish between outsourcing arrangements and other types of third-party arrangements. For non-outsourcing arrangements, the transitional period could be aligned with the average duration of existing contracts (e.g. x years), allowing institutions to integrate the new requirements more naturally into their renewal cycles and avoid unnecessary renegotiations. Alternatively, for non-CIF third-party arrangements, amendments could be required only upon contract renewal, depending on their relevance and risk profile. This would support a more proportionate and operationally feasible implementation approach.

Question n. 2

Is Title II appropriate and sufficiently clear?

Assessment of third-party arrangements

Paragraph 30. Include the exclusion of low-risk services

While we agree with the exclusion of certain types of services under Section 32(f), we note that the current wording excludes them only "as a general principle." This phrasing introduces a rebuttable presumption, which may lead to interpretative uncertainty and inconsistent application across institutions. We suggest that the Guidelines consider explicitly excluding services that are clearly not relevant for supervisory purposes—such as routine cleaning, catering, or minor maintenance—rather than relying on a general principle. This would enhance clarity and reduce the compliance burden associated with assessing low-risk service arrangements that do not materially impact the institution's risk profile or regulatory obligations.

Paragraph 32. Deletion of Market Information Services:

We would like to express our concern regarding the removal of the exclusion for Market Information Services from the scope of application. In the 2019 EBA Guidelines on Outsourcing, Market Information Services were explicitly excluded from scope, with the following example provided: *"Market information services (e.g. provision of data by Bloomberg, Moody's, Standard*

& Poor's, Fitch)". The rationale for excluding these services was clear: they typically do not involve critical or important functions, nor do they materially impact the institution's risk profile or operational resilience.

The current draft Guidelines removed this exclusion without providing sufficient justification. Even if most TPA with data vendors will classify as ICT and therefore be under scope of DORA, this is not true for all suppliers and for all the services they provide. In this sense, these providers might operate outside the scope of DORA and they are unlikely to show flexibility in what concerns contract negotiation. It is also unclear for us the treatment that shall be given to hybrid contracts were both ICT and non-ICT components are present in equal measure. For this reason, we believe that the inclusion of Market Information Services within scope risks diluting the focus of the Guidelines and overburdening institutions with low-risk third-party arrangements. We would therefore recommend that the EBA reintroduce the exclusion for Market Information Services in the final version of the Guidelines. This would ensure consistency with past practice, maintain proportionality, and align with the broader regulatory framework.

Paragraph 32. c) Extension of Oversight-Based Exclusion to Additional Functions of Regulated Entities

We welcome the inclusion of the current exclusion for "*clearing and settlement arrangements between clearing houses, central counterparties, and settlement institutions and their members*". However, we urge the EBA to extend this exclusion to include other functions provided by these entities, which are already subject to regulatory oversight. For example, Euroclear (a regulated FMI) provides a range of services beyond clearing and settlement, all of which are already supervised by competent authorities. Requiring such entities to monitor a provider that is already under regulatory supervision does not offer additional value. Expanding the exclusion to include other functions would help avoid unnecessary administrative burden and redundancy.

Extending the exclusion ensures greater consistency with DORA. As clarified in the DORA FAQ (Q74, published on 31 May 2024), when a financial entity provides a service that requires it to be authorised/licensed/registered as a financial entity, such services are deemed regulated financial services and not ICT services under the meaning of Article 3(31) of DORA. Aligning the exclusion with DORA would help avoid regulatory overlap and ensure a coherent supervisory approach.

Paragraph 32. d) Extension of Oversight-Based Exclusion to Additional Functions of Regulated Entities

The current exclusion for "global financial messaging infrastructures that are subject to oversight by relevant authorities (e.g. SWIFT)" is clear and appropriate. However, we suggest considering whether this exclusion could be extended to cover other functions provided by the same entities that are already under regulatory oversight. These entities often offer a broader range of services—such as compliance tools, reference data utilities, or risk mitigation platforms—that, while not strictly messaging infrastructures, are integral to the financial system

and operate under similar regulatory scrutiny. Including these under the same exclusion could ensure consistency and avoid unintended regulatory fragmentation.

Other exclusions to be considered:

-Regulated financial services performed by financial entities subject to compulsory or voluntary supervision, in line with DORA;

-ICT TPA that are explicitly out of scope of DORA;

-Arrangements falling below a certain materiality threshold (which could not be based in a pre-determined fixed amount, it should be determined by the entity taking into considerations relevant criteria provided by the EBA but adapted to the reality of each financial entity)

-Temporary contracts (which threshold should be determined by the entity taking into considerations relevant criteria provided by the EBA but adapted to the reality of each financial entity)

-Services provided by public authorities in the strict sense, and functions legally required to be performed by the service provider;

Inclusion of "de minis" provision:

We also recommend an inclusion of a "de minis" provision to exclude arrangements of negligible impact, which would reduce administrative burden and focus oversight on material risks.

Critical or Important Functions

Paragraph 33. Risk-based differentiation of TPA:

There is a rightly distinction between CIF and other functions in this paragraph, which is a logical and necessary step. However, under the proposed framework, third-party arrangements previously considered “other services” and not covered by the EBA Guidelines on outsourcing will now fall into the same risk category as non-material outsourcing arrangements—i.e., those not involving CIFs. The consultation paper currently outlines only two risk buckets: CIFs and non-CIFs. To ensure proportionality and operational efficiency, we recommend further differentiation within the non-CIF category. Specifically, a risk-based approach could allow for fewer provisions to apply to low-risk third-party arrangements, reducing unnecessary compliance burdens while maintaining resilience. This would better reflect the diversity of third-party relationships and support more targeted oversight.

Paragraph 34. Clarifying the criticality assessment of internal control functions:

To ensure maximum consistency and harmonization with the DORA Regulation, we recommend revising the wording in Paragraph 34 to more explicitly link the identification of criticality of operational tasks within internal control functions to the established criteria for critical or important functions (CIFs). Specifically, the assessment should be clearly tied to whether a disruption would result in material impairment of:

-Compliance with authorisation conditions;

-Financial performance;

-The soundness and continuity of core business services and activities.

This alignment would enhance clarity for financial entities when determining which internal control functions fall within the scope of CIFs and ensure a consistent application of risk-based oversight across all relevant functions.

Question n. 3

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

TITLE III.

Paragraph 47. f) clarify "appropriate time frame" (Section 5):

The reference to an “appropriate time frame” is vague and may not reflect the operational realities of such transitions. What is considered an appropriate time frame? In practice, transferring a function to an alternative TPSP or reintegrating it internally can be complex and time-consuming, especially for highly integrated or bespoke services. We recommend that the regulation include further safeguards and clarifications, such as:

-Taking into account the type of TPA, including its complexity and integration level;

-Considering the risk exposure associated with the function;

-Allowing for flexibility in timelines based on the nature of the function and the financial entity’s contingency planning;

-Encouraging the use of pre-assessed fallback options or exit strategies as part of contractual and risk management frameworks.

-This would ensure that the requirement remains proportionate and operationally feasible, while still supporting resilience and continuity objectives.

Policy on Third Party Risk Management

Integration of ICT and Non-ICT Risks in Third-Party Risk Management Policies:

The Guidelines explicitly state that they do not provide guidance on third-party arrangements in the context of ICT, as this is covered by DORA. Given that DORA serves as the main framework for digital operational resilience in the financial sector, we recommend that the Guidelines more clearly emphasize that a financial entity’s third-party risk management policy must recognize and prioritize the DORA framework for all ICT-related third-party risks. To promote regulatory consistency and streamline internal governance, it would be beneficial to encourage financial entities to adopt a unified third-party risk management policy that addresses both ICT risks (under DORA) and non-ICT risks (under these Guidelines), instead of having a clear differentiation which would be a duplication of efforts. Such a policy should clearly delineate responsibilities, processes, and oversight mechanisms for each category, while operating under a common governance structure. In our view, this approach would avoid the perception of

fragmented or siloed frameworks and better reflect the integrated nature of DORA, which consolidates and modernizes rules on ICT-related risk.

Overlap between EBA Draft GLs & CSDR:

We urge the EBA to ensure stronger coordination between the Guidelines and the CSDR framework to eliminate unnecessary duplication and regulatory fragmentation. The definitions and obligations linked to outsourcing and Critical Service Providers (CSPs) under CSDR diverge from those under DORA and the draft Guidelines, despite targeting similar risk domains. This misalignment results in a proliferation of supplier classifications at group level—outsourcing, ICT, non-ICT, CIF, non-CIF, CSP, BRRD-critical—creating operational inefficiencies and compliance complexity.

For Euroclear entities, CSDR requirements remain applicable, including mandatory approval processes for certain outsourced services and notification obligations for dependencies on critical service providers and utilities. If non-ICT risks are to remain within CSDR's scope, we strongly recommend aligning terminology and conceptual frameworks with DORA. Requirements such as subcontracting must be harmonized to avoid conflicting interpretations and implementation burdens.

Furthermore, we call for a clear regulatory distinction between intra-group subcontracting involving regulated entities and third-party subcontracting. Recognizing the operational and governance efficiencies of group arrangements would significantly reduce redundant compliance efforts and support proportionality in supervisory expectations.

Paragraph 48. Frequency to review and update the Third-Party Risk Management Policy:

While we acknowledge the importance of regular oversight of third-party risk management policies by the management body of financial entities, the requirement to review and update such policies at least once a year is too stringent, particularly for complex group structures such as Euroclear. In practice, updating and implementing these policies across multiple entities and jurisdictions involves significant coordination, resource allocation, and internal governance processes. A rigid annual review cycle may not be operationally feasible.

We recommend that the regulation allow for greater flexibility that would ensure that the policy remains effective and proportionate, without imposing unnecessary administrative burdens. For example:

-Risk-based review cycles, where frequency is aligned with the materiality and complexity of third-party arrangements;

-Event-driven updates, triggered by significant changes in the risk landscape, regulatory requirements, or service provider performance;

-Group-level discretion, enabling entities to align review timelines with their internal governance and oversight frameworks.

Business Continuity Plans (Section 8)

Paragraph 55. Proportionality in business continuity planning for CIF:

Not all functions deemed Critical or Important, for various reasons, may necessarily require BCP. We would suggest clarifying that not all CIFs may require a dedicated BCP, depending on the nature of the function and the associated risk exposure, for example.

In particular, we recommend that the regulation allow for a risk-based assessment to determine whether a BCP is necessary for a given CIF. This would ensure that resources are focused on high-risk functions where disruption would have a material impact on operational resilience.

Additionally, the involvement of TPSPs in BCP testing should be proportionate and feasible, taking into account the type of service, contractual arrangements, and the financial entity's ability to simulate disruptions without direct TPSP participation. This approach would enhance proportionality and practicality, while still supporting the overarching goal of operational resilience.

In the interest of building a consistent and coherent framework for both ICT and non-ICT third-party arrangements, we recommend removing the requirement outlined in Paragraph 58. As currently drafted, it introduces expectations that deviate from DORA's contractual requirements, potentially creating confusion and misalignment with existing regulatory standards. Maintaining alignment with the EBA Guidelines on internal governance and the DORA Regulation is essential to ensure clarity, avoid duplication, and support effective implementation across financial entities. A harmonised approach would also reduce the risk of regulatory fragmentation and unnecessary compliance burdens.

Documentation requirements (section 10)

Impracticability of having a single RoI for ICT/Non-ICT:

The requirements outlined in the draft Guidelines are currently insufficient and lack clarity regarding the format and technical specifications for the Register of Information (RoI) concerning non-ICT services. This creates uncertainty for financial entities attempting to implement a unified and compliant RoI. Moreover, there are notable discrepancies between the draft Guidelines and the DORA framework, particularly in terms of data structure, reporting expectations, and alignment with ICT-related RoI obligations. These omissions will not allow for the goal of a single, integrated RoI across ICT and non-ICT third-party arrangements. We recommend that Section 10 be revised to:

-Clearly define the format and technical specifications for non-ICT RoI entries;

-Ensure full alignment with DORA to support a unified and streamlined approach;

-Avoid introducing parallel or conflicting requirements that would hinder the creation of a single RoI.

-Remove the obligation to retain expired/terminated TPA for periods of at least 5 years, which is not aligned with DORA.

-Draft GLs require both end date and next renewal date, while DORA only requires the renewal date if extensions are possible.

- Last assessment date and reasons for criticality are required, but the expected dropdown format may not reflect internal criteria.

-Intra-group vs. non-intra-group distinction is included.

Additional Provider Info: Contact details and tax ID are requested, which may be excessive.

-Description, category, and subcategory are required.

-Only for critical functions but may be difficult to standardize.

-Type and country of subcontracted service are required for critical functions.

- Dates of last assessments are required for critical functions.

- Detailed data including LEI/EUID, contact info, and parent company—may be burdensome.

- Notice periods and service location are required for all arrangements, though DORA limits this to critical functions.

-Required if applicable, but scope should be clarified.

Proportionality and Technical Clarity in RoI Requirements:

The expanded scope of the Register of Information (RoI) introduces a significant increase in reporting obligations compared to previous frameworks. Without clearer alignment to DORA's RoI ITS, these risks becoming an administrative burden rather than a tool for effective risk management or supervision. To avoid this, we recommend:

-Applying proportionality: low-risk, non-ICT arrangements should not be subject to the same level of detail as CIFs.

-Ensuring alignment with DORA: the fields, input formats, and mandatory nature of data should reflect the DORA RoI ITS.

-At a minimum, the EBA should provide a structured template detailing required data points, input types, descriptions, and whether each field is mandatory or not.

Paragraph 63 g) and 64 c) RoI of CIF:

We recommend removing the requirement to include personal data (such as passport numbers and national identity numbers) in the Register of Information (RoI). These data points are not necessary for effective third-party risk management and raise significant concerns under the GDPR, particularly regarding data minimisation and lawful processing. Their inclusion could expose financial entities to unnecessary compliance risks and should be excluded from the mandatory fields in our view.

Paragraph 64 b) Audits of CIF

The draft Guidelines require the inclusion of audit dates related to critical or important functions in the Register of Information. To ensure clarity and consistency, we recommend specifying:

1.Type of audit: Whether this refers to internal audits, external audits, supervisory examinations, or audits conducted by the TPSP's own audit function.

2.Timing reference: Whether the field should capture the last audit date, the next scheduled audit, or both—given the plural use of "dates."

Paragraph 67. Prior Approval/Notification Regarding Planned Contractual Arrangements of Critical or Important Functions

We urge the EBA to remove in its entirety *Paragraph 67*, namely, the requirement to inform competent authorities regarding planned contractual arrangement on the provision of CIF by TPSPs and when a function performed by a TPSP has become critical or important. This requirement imposes a significant administrative burden upon Financial Entities, and it is inconsistent with the DORA framework.

Question n. 4

Is Title IV of the Guidelines appropriate and sufficiently clear?

Title IV

Section 12

Clarification of Risk Assessment Methodology for Third-Party Arrangements

This section deviates from the 2019's approach by imposing the assessment of the potential impact of TPA across relevant risk categories, including: operational, reputational, legal and concentration risks. In this regard we would recommend that the Guidelines provide clearer direction on how these assessments should be calibrated. Without further guidance, there is a risk that institutions may approach these assessments as checklist exercises, rather than conducting meaningful, risk-based evaluations. To ensure consistency and effectiveness, we suggest, e.g:

-Introducing criteria or examples to help entities determine the depth and scope of assessment based on the nature and materiality of the arrangement;

-Encouraging a proportional approach, where low-risk or non-critical arrangements are subject to lighter assessments;

-Clarifying that assessments should be qualitative and contextual, not just procedural or template-driven.

Paragraph 85 - Proportional Application of Contractual Requirement:

We note that Paragraph 85 introduces a requirement for TPA to include a set of contractual elements, without distinguishing between critical or important functions (CIFs) and other types of third-party arrangements. This marks a departure from the 2019 EBA Guidelines on outsourcing, which applied such requirements specifically to outsourcing arrangements involving CIFs. By removing the CIF qualifier, the current draft implies that all non-ICT third-party arrangements—including non-outsourcing and non-CIF contracts—must now meet the same

contractual standards. This creates a disproportionate burden, particularly for non-CIF outsourcing arrangements that were previously out of scope. Moreover, it would require financial institutions to reopen and renegotiate existing contracts that were updated in line with the 2019 Guidelines, resulting in significant operational and legal costs with limited added value from a risk management perspective. We would recommend the following suggestions:

Option A - optimal alternative:

Retain the wording of the 2919 GLs and limit these contractual requirements to CIF.

Option B - Granular Scope Adjustment:

Exclude non-CIF outsourcing arrangements that were previously out of scope under the 2019 EBA Guidelines from the obligation to include the full set of contractual elements outlined in Paragraph 85.

Option C - Deferred Compliance for Existing Contracts:

Allow financial entities to update non-CIF TPA to comply with the new requirements only at the time of renewal, rather than requiring immediate renegotiation. This would balance regulatory objectives with operational feasibility.

Additionally, given the significantly broadened scope of third-party arrangements now captured under the GLs—including non-outsourcing and non-ICT services—some of the contractual requirements outlined are not universally applicable and may result in unnecessary complexity. Paragraph 85 c) information on data processing and storage location, g) Data confidentiality obligations and h) Data access rights, for example, are not relevant in all third-party contexts, particularly where there is only an inbound flow of data or where the service does not involve any data processing at all.

We would recommend that the GLs adopt a risk-based and context-sensitive approach, ensuring that such requirements are tailored to the nature of the service, on an "if applicable" basis instead of a mandatory basis. This would avoid imposing disproportionate obligations on low-risk, non-ICT arrangements and support more practical implementation across diverse third-party relationships.

Paragraph 86 - Monitoring Rights over TPSPs

We appreciate the EBA's efforts to harmonize third-party risk management (TPRM) across financial entities and align non-ICT service oversight with the principles of DORA. However, we would like to raise concerns regarding the proposed expansion of monitoring and audit rights over TPSPs, particularly as outlined in Section 12.1 of the draft guidelines. The new provisions—such as the unrestricted right of inspection and audit, the obligation to cooperate during onsite inspections, and the requirement to define scope and frequency of audits—represent a significant departure from the 2019 Guidelines, which only required institutions to retain the right to monitor service provider performance on an ongoing basis. While we understand the intent to strengthen oversight, we believe these additions may result in disproportionate implementation costs for financial entities, especially where existing arrangements are already compliant with the 2019 EBA Outsourcing Guidelines. The proposed changes would necessitate

contractual amendments across a wide population of legacy agreements. We would respectfully suggest that the EBA either retained the 2019 wording or, at least:

-Clarify that these enhanced monitoring rights apply only to new third-party arrangements entered into after the guidelines come into force, and not retroactively to existing contracts.

-Allow for proportional implementation based on the materiality and risk profile of the arrangement, especially where the TPSP supports non-critical functions.

-Recognize existing contractual frameworks, avoiding the need for further amendments unless a material gap is identified.

In this Section, the Guidelines refer to implementing changes "*in a timely manner and as soon as possible*." We would appreciate clarification on what is considered an appropriate time period for such implementation. It is currently unclear whether this timeframe is to be defined by the financial entity based on its internal policies and risk assessments, or whether the EBA intends to establish specific expectations or benchmarks for timeliness.

Section 12.2 Audit rights

Paragraphs 97 and 97 - Discrepancy with DORA on Audit Rights for Non-Critical Service Providers:

We note a misalignment between the current Guidelines and the DORA Regulation regarding the mandatory inclusion of audit and access rights in third-party contracts. While DORA limits this requirement to critical ICT third-party service providers, the Guidelines appear to extend it to all third-party arrangements, including those not supporting critical or important functions.

This broader scope introduces uncertainty and implementation challenges, particularly when negotiating audit rights with providers of non-critical services. It also risks diluting the risk-based approach that underpins both DORA and the EBA Outsourcing Guidelines.

Paragraph 100 Clarification Needed on Forward-Looking Assessment of Criticality:

The current wording in this paragraph "Financial entities should take into account that functions may become critical or important over time" as well as in the background section of the GLs "The right to audit is key for providing the appropriate assurance that at least critical or important functions provided by TPSPs, as well as functions that may become critical or important in the future…", raises concerns about clarity. It is not always straightforward to determine whether a function may become critical or important in the future. This introduces uncertainty for institutions when deciding whether to include audit rights in contracts for non-critical functions. It may be helpful to provide additional criteria or examples to support this forward-looking assessment, or to clarify whether audit rights should be included as a precautionary standard in all third-party arrangements, regardless of current criticality.

Introduction "Lead overseer" role similarly to DORA:

DORA introduced the notion of "Lead Overseer" to be appointed to conduct inspections on systemic ICT-TPSP benefiting to all related European financial institutions. This notion is very

useful as often individual companies do not have the weight to perform audit versus global industry giants. We are recommending the same concept to be applied in the EBA guidelines.

Section 12.3 Termination Rights

Paragraph 109 b) - Termination Rights:

We acknowledge the importance of ensuring financial entities retain the ability to terminate third-party arrangements when necessary. However, we would like to raise concerns regarding the proposed termination right under this paragraph, which allows termination in case of "impediments capable of altering the performance of the function."

This provision is vague and broad, and in practice, it may be interpreted by third-party service providers as a termination right for convenience. Such clauses are often difficult to negotiate, especially with strategic or large-scale providers, and may lead to contractual resistance or increased costs for financial entities.We would recommend that the EBA:

-Clarify the scope of what constitutes "impediments" and ensure it is tied to material impact on the performance of critical or important functions.

-Allow for proportionality in the application of this termination right, based on the nature and risk profile of the outsourced service.

-Recognize existing contractual safeguards (e.g. service level agreements, remediation periods) as sufficient mechanisms to address performance issues before triggering termination.

Section 13. Monitoring

Paragraph 115 c) - Performance and Quality Monitoring Requirements:

We support the principle of ongoing oversight of third-party arrangements, especially those supporting critical or important functions. However, we would like to highlight that the proposed requirements—particularly the expectation to receive business continuity documentation and conduct testing cycles—will have a similar operational impact to DORA, even for non-ICT critical service providers. This introduces a significant compliance burden for financial entities, as many non-ICT providers do not currently operate with the same level of resilience documentation or testing maturity as ICT providers. Requiring all such providers to implement and test business continuity plans (BCPs) may lead to contractual friction, increased costs, and limited added value in terms of risk mitigation. We recommend that the EBA:

-Clarify the scope of these requirements, particularly whether they apply to non-ICT TPSPs supporting critical functions.

-Allow for proportional implementation based on the nature of the service and the provider's operational context.

-Recognize alternative assurance mechanisms, such as self-certification or existing internal controls, where full BCP testing may not be feasible or is disproportionate.

Section 14. Exit Strategies

Paragraph 118 a) - Clarification on Applicability of Exit Strategy Requirements:

We would appreciate clarification on whether this requirement applies to all third-party arrangements or only those supporting critical or important functions (CIFs). Applying this requirement universally may be disproportionate, especially for non-critical arrangements where exit planning is less relevant from a risk perspective. If the intent is to focus on CIFs, we suggest that the guidelines explicitly state this scope to avoid unnecessary implementation efforts and contractual complexity for low-risk services.

Question n. 5

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

Inconsistency with Paragraph 32(f) Regarding Excluded Services:

Annex I includes "Secretarial services" and "Travel and entertainment services" as examples of functions that could be provided by third-party service providers. However, these services are explicitly excluded from the scope of the Guidelines under Paragraph 32(f), which states that "support functions such as cleaning, catering, secretarial services and travel arrangements" are out of scope.

This creates a contradiction within the Guidelines and may lead to confusion during implementation, particularly when determining which third-party arrangements require compliance with the Guidelines. Therefore, these services should be removed from Annex I.

Clarification Needed on Definition and Scope of "Service":

Annex I includes a wide range of functions that could be provided by third-party service providers, including "Insurance services" and "Talent acquisition & hiring." These types of services typically do not fall under a risk-based approach for third-party risk management and are often considered low-risk or support functions. This raises questions about the intended scope of the Guidelines and what is considered a "service" subject to compliance. Greater alignment and clarity are needed to help financial entities determine which third-party arrangements fall within scope, particularly in light of exclusions listed in Paragraph 32(f).

Exclusion of Insurance Services and Proposal for Whitelisting Low-Risk Arrangements:

"Insurance services" are included in Annex I as examples of functions that may fall under the scope of the Guidelines. However, we believe this inclusion is not aligned with the nature of insurance contracts, which are legal agreements designed to transfer or mitigate risk, rather than operational services requiring ongoing oversight. Insurance policies do not involve continuous service delivery and do not pose a threat to the continuity of financial entities' operations. Their inclusion in the scope of third-party risk management appears inconsistent with the spirit of the Guidelines, which aim to ensure resilience and oversight of outsourced functions that could impact service continuity or regulatory compliance. To support a more proportionate and risk-based approach, we propose the introduction of a whitelist of low-risk or excluded services, which could include:

-Engagement of law firms

-Regulatory-related services

-Office premises and infrastructure

-Memberships and subscriptions

-Office supplies and administrative support

-Energy and utilities

-HR-related services (e.g. payroll, recruitment platforms) -Etc.

Clarification and Exclusion for Regulated Financial Entities

Annex I includes “securities services” as an example of functions that may be provided by third-party service providers. These financial Institutions are already highly regulated financial market infrastructures, subject to extensive oversight under EU and national frameworks. Applying the full scope of these Guidelines to such entities would be disproportionate and could lead to duplicative regulatory obligations without a corresponding benefit in terms of risk mitigation.

We recommend that the EBA adopt a similar approach to the one taken under DORA, where regulated financial services provided by regulated financial entities are excluded from the definition of ICT services. While this exclusion was clarified via the ESAs’ Q&A (DORA030 – 2999 – EIOPA), we believe a formal clarification or carve-out in these Guidelines would be appropriate to ensure consistency and avoid unintended regulatory overlap. Additionally, the service “Clearing, settlement & reconciliation;” is in contradiction with paragraph 32 and should be removed.