CONSULTATION RESPONSE

EBA Draft Guidelines on the sound management of third-party risk

7 October 2025

HVG LAW B.V. & EY ADVISEURS B.V.

1. INTRODUCTION

1.1 HVG Law B.V. (**HVG Law**) and EY Adviseurs B.V. (**EY**) (hereinafter: we, us) welcome the development of a harmonised and robust framework for third-party risk management within the financial sector. We recognize that the EBA Guidelines on the sound management of third-party risk (**Guidelines**) are of central importance in ensuring resilience and clarity across the supply and value chain for financial entities.

1.2 We have carefully reviewed the consultation draft of the Guidelines and, on that basis, would like to share a number of observations and recommendations for further consideration. Our comments focus on the following key areas: (i) definitions (prepared by EY); (ii) classification of critical or important functions (prepared by EY); (iii) register of information (prepared by EY); (iv) scope of services (prepared by HVG Law) and (v) scope of critical or important functions (prepared by HVG Law).

2. EY: DEFINITIONS

2.1 The published Guidelines are a step towards further standardizing the supervisory landscape for financial organisations, which is important for a consistent and effective approach to managing third-party risks across the European Union (**EU**).

2.2 In line with Regulation (EU) 2022/2554 (**DORA**), the Guidelines move away from outsourcing as the sole focus and instead encompasses a broader scope of Third-Party Service Providers (**TPSP**) arrangements. We understand that outsourcing is considered as a subset of TPSP arrangements. While the Guidelines expand its scope beyond outsourcing to include all TPSP arrangements, outsourcing arrangements are still explicitly defined in the Guidelines and the term continues to be referenced throughout. The definition of outsourcing remains challenging and open to multiple interpretations.

2.3 Furthermore, the current definition of a TPSP lacks clarity. While the version in the definitions section appears broad, the Guidelines later introduce additional specifics (such as requiring that services be provided regularly or on an ongoing basis). This means that financial entities must assess whether an arrangement with a TPSP qualifies as an arrangement under the scope of the Guidelines, considering its recurrence and ongoing nature. These assessments may require legal and operational interpretation that can be challenging across diverse service categories and jurisdictions.

2.4 The Guidelines acknowledge the challenge of clearly distinguishing between outsourcing and (other) TPSP arrangements. Greater clarity on this distinction would help financial entities understand when specific requirements apply. In addition, introducing precise definitions along with concrete examples and criteria, would enable more consistent and accurate classification of TPSP arrangements.

3. EY: CLASSIFICATION OF CRITICAL OR IMPORTANT FUNCTIONS

3.1 In line with DORA, the Guidelines require that TPSPs must be assessed to determine if they support critical or important functions. If so, stricter requirements are triggered. We understand that critical or important functions (**CIFs**) are categorized based on impact, compliance, continuity and financial performance. We note a difference compared to DORA, in which CIFs are categorized based on severity, compliance and systemic impact. Although it concerns a minor change, such inconsistencies can result in legal uncertainty and operational unclarity for financial entities

3.2 Maximum alignment with existing frameworks and a clear rationale for deviations is recommended to avoid the risk of creating confusion, regulatory arbitrage, and increased compliance costs.

4. EY: REGISTER OF INFORMATION

4.1 The Guidelines introduce a significant change by requiring financial entities to record all non-ICT TPSPs in the Register of Information, regardless of the criticality or importance of the function provided. While the intention to enhance transparency and supervisory oversight is understandable, this requirement can raise concerns regarding proportionality and operational burden.

4.2 Without distinguishing between TPSPs that support a CIF and those that do not, the requirement places a significant administrative burden on financial entities, particularly smaller institutions. They are obliged to document and maintain information on a broad range of minor and low-risk TPSPs, potentially diverting resources from effectively managing genuinely material risks.

4.3 We advise to reconsider limiting the mandatory registration to non-ICT TPSPs that support CIFs, as it would ensure that the Register of Information remains a practical and effective tool for both financial entities and supervisors, in line with the principle of proportionality and risk-based supervision.

5. HVG LAW: SCOPE OF SERVICES

5.1 A central aspect of the Guidelines is the boundary it seeks to draw between arrangements covered by DORA, those relating to ICT services, and those which fall under the Guidelines. This demarcation is of importance: it determines not only applicable risk management requirements but also impacts further market harmonization and supervisory expectations across the EU. The following analysis describes the relevant provisions, and related challenges in applying the different scopes.

5.2 The Guidelines clearly include that, following DORA, ICT services provided by TPSPs to financial entities fall within the scope of DORA. Only non-ICT related services are governed by the Guidelines, with an explicit ambition of close alignment between DORA and the Guidelines "*to ensure a level playing field and foster supervisory convergence*", as mentioned in the executive summary of the Guidelines.

5.3 More specifically, the Guidelines state: "*The management of information and communication technology (ICT) risk and the use of TPSPs to provide ICT services as defined in Article 3(21) of Regulation EU 2022/2554 are not under the scope of application of these Guidelines as they fall under the scope of DORA. In this regard, these Guidelines only cover the use of TPSPs providing or supporting functions that are not qualified as ICT services under DORA. Consistency has been ensured, to the extent possible, with DORA and its relevant mandates; while DORA provides for the framework on the management of third-party risks with regard to ICT services, those Guidelines apply for non-ICT related services provided by TPSPs*".

5.4 However, the practical application is quickly complicated by contractual arrangements that integrate both ICT and non-ICT functions. The Guidelines require financial entities to holistically assess such arrangements, as mentioned in paragraph 31: "*Where an arrangement with a TPSP covers multiple functions, financial entities should consider all aspects of the arrangement within their assessment, e.g. if the third-party service provided includes the provision of operational task of risk management and prudential reporting, both aspects should be considered together*".

5.5 An additional complication is introduced by the related footnote nr. 42 to said paragraph 31: *"In case where for the provision of a non-ICT service, the arrangement with a third-party service provider also implies the use of ICT services as defined under Article 3(21) of DORA, it belongs to the financial entity to determine whether the use of ICT service is material for the provision of the services under the third-party arrangement and therefore triggers the application of DORA framework in lieu of the present Guidelines*". Footnote 42 underscores the importance of the entity-level assessment and refers to ESAs Q&A DORA030 for further guidance.

5.6 Where a third-party arrangement covers multiple intertwined functions (e.g., risk management with embedded ICT tools, or regulatory reporting delivered via an ICT platform), the Guidelines require the entity to holistically assess all components. In practice, these functions are rarely separable, making the scoping decision extremely complex, especially as DORA has the objective of a very broad scope and application level. The aforementioned footnote solidifies that, for such arrangements, the financial entity must perform a "materiality" determination regarding the ICT element before deciding which framework applies, being either DORA or the Guidelines.

5.7 Practical example: If a financial entity engages a TPSP for prudential reporting who provides business advice (non-ICT service) and a real-time reporting analytics platform (ICT service, e.g. via cloud dashboard), the financial entity must assess the materiality of the ICT element with respect to the totality of the service involved. This can easily result in different regulatory scoping by different financial entities in similar cases.

5.8 To meaningfully achieve harmonization when implementing the Guidelines, it is recommended to:

(a) Supplement materiality assessment with concrete, objective criteria, including scenario-based decision trees or minimum "materiality" thresholds.

(b) Provide additional worked examples that specifically address modern digital, cloud, and multi-function outsourcing contexts.

(c) Facilitate early engagement for financial entities with supervisors for ambiguous arrangements to mitigate the risk of adverse supervisory findings.

6. HVG LAW: CRITICAL OR IMPORTANT FUNCTIONS

6.1 There appears to be an ambiguity between critical or important functions (**CIF**) and the excluded non-material functions in the Guidelines, which is further stipulated in this section.

6.2 The Guidelines mention the following definition of excluded functions in paragraph 32(f): "*the acquisition of services that do not have material impact on the financial entities' risks exposures or on their operational resilience (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators)"*

6.3 In addition, the Guidelines provide the following definition of CIF in paragraph 16: "*means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law*."

6.4 The Guidelines rely on a negative definition for excluded functions (those with no material impact) and a positive definition for CIFs (functions where a disruption would "materially impair" key aspects of the entity). This creates a structural grey area.

6.5 This grey area is the following. There are functions that are neither automatically CIF but also not clearly, categorically excluded as they might not have zero material impact. Many support, logistics, or back-office services may not have an obvious material impact but could, under certain conditions or at certain scales, become somewhat significant but non-material for risk or compliance. This combined approach means that there is a set of functions that are neither expressly excluded nor clearly captured by the definition for CIF. For example, a function that is not "material" enough to

automatically be considered CIF, but not so insignificant as to fit the exclusion examples, sits in a classification "no man's land". Therefore, the Guidelines' approach leaves uncertainty in how to classify such functions under a risk-based policy framework.

6.6 This lack of clarity can cause financial entities to face challenges in both directions. On one hand, they may include too many minor functions in their third-party risk frameworks under the Guidelines, resulting in unnecessary compliance work. On the other hand, they might overlook functions that could become significant and should therefore be treated as CIF. To address this, it would help to limit the list of excluded functions to those that are truly and permanently insignificant, and to avoid using "no material impact" as the sole exclusion criterion. This change would make clear that not all non-critical functions are automatically excluded and would leave space for financial entities to use their own risk-based judgment when assessing each function.

6.7 Practical Example: Consider accounting support, payroll administration, or document archiving services. In certain situations, these support or back-office functions may not obviously qualify as "critical or important functions" (**CIF**), since disruptions might not immediately jeopardize the financial entity's operations or regulatory obligations. However, nor are they as operationally insignificant as catering or other functions explicitly excluded by the Guidelines (see paragraph 32(f)). The Guidelines offer no clear guidance for handling such "in-between" cases.

6.8 The identified contradiction is of legal and compliance relevance, especially as financial entities often already encounter challenges when identifying CIF under DORA with respect to their own organization. Adding another slight ambiguous framework to that existing challenge might not contribute to harmonized third-party risk management. When implementing the Guidelines, it is recommended to:

(a) Confine the explicit carve-out for excluded functions to examples that will never reasonably present material risk to the entity's compliance or operational continuity,

(b) Recognize and address the spectrum between permanently non-material and non-critical as excluded functions but also contextually relevant functions, allowing for risk-based categorization by the financial entity.