Shared Assessments
EBA Consultation Paper 2025-12 Regulatory Response

Date: October 7, 2025

To: European Banking Authority

Submitted Through: Online Portal
https://www.eba.europa.eu/form/webform-consultation-18613?source_entity_type=node&source_entity_id=18613

From: Andrew Moyad, CEO, Shared Assessments LLC

Subject: EBA/CP/2025/12 Consultation Paper; Draft Guidelines on the sound management of third-party risk

The Shared Assessments Program appreciates the opportunity to submit comments to the European Banking Authority (EBA) Consultation Paper EBA/CP/2025/12 Draft Guidelines on the sound management of third-party risk.

Since 2005, Shared Assessments has been setting the standard in third-party risk assessments. Shared Assessments is a member-driven, industry-standard body that defines best practices, develops tools, and conducts pace-setting research. Program members cut across the full range of compliance, legal, operations, procurement, and risk roles work together in an inter-disciplinary manner to build and disseminate best practices and develop related resources that give all third-party risk management stakeholders a faster, more rigorous, more efficient, and less costly means of conducting security, privacy, and business resiliency control assessments. Additional information on Shared Assessments is available by visiting: http://www.sharedassessments.org.

On behalf of the Program and its diverse group of professional members and industry firms, thank you for accepting the following response regarding EBA/CP/2025/12 Consultation Paper: on the sound management of third-party risk.

1. Shared Assessments appreciates the opportunity to comment on the draft EBA Guidelines regarding the sound management of third-party risk. Overall, we believe the draft Guidelines represent a worthwhile update to the 2019 EBA Guidelines on outsourcing arrangements, though we recommend several modifications to achieve the same objectives while recognising the operational complexity of achieving those objectives.

2. The EU's Digital Operational Resilience Act (DORA), which the draft Guidelines emulate, presented a significant increase in regulatory expectations in pursuit of important goals. The draft Guidelines for non-ICT risk management services present a similar increase in expectations. Importantly, Shared Assessments agrees with the need for roughly parallel third-party risk management processes for both ICT and non-ICT outsourced services. These guidelines clearly recognise that third-party risk management today increasingly demands complete supply chain transparency. With that recognition, however, comes a set of challenges stemming from suppliers not recognising changes to long-term expectations between outsourcers and the partner organisations that anchor increasingly complex supply chains. These guidelines are an opportunity for the EBA to reset those expectations and to reduce inherent frictions that currently lie in the way of adequate transparency.

3. These important guidelines seem not to recognise enough that firms supporting almost any critical or important activity today commonly have an ICT component either within a third party or in a longer supply chain. The ubiquity of ICT components is an important reason why third-party risk management processes should be consistent across all outsourcing relationships, regardless of the degree that ICT elements inhere in their services. Accordingly, a more explicit expectation that these processes are expected for both ICT and non-ICT third parties is essential, particularly as the Guidelines recognise that "[d]ivergent regulatory approaches carry a risk of regulatory arbitrage" (Rationale, paragraph 16).

4. For all "critical or important" functions, the draft Guidelines require that competent authorities have unrestricted rights of entry and examination of the TPSP (paragraph 99), a parallel requirement to DORA. In a world where many organisations (both private and public) are expected to achieve more with fewer resources, competent authorities should ensure they have sufficient resources to address this requirement.

Question	Response
Question 1: Are subject matter, scope of application, definitions, and transitional arrangements appropriate and sufficiently clear?	**Response:** With a few exceptions noted in the discussion below, Shared Assessments believes that the Guidelines' subject matter, scope of application, definitions, and transitional arrangements are appropriate and sufficiently clear. The draft Guidelines apply the successful DORA framework to non-ICT risks. For US institutions such as affiliates of EU banks that may already adhere to US risk management regulations, the draft Guidelines will require more governance and centralisation. The Guidelines require more specific performance from the TPSP, but the outsourcer must also increase its efforts to manage the TPSP and its supply chain more tightly. This enhancement should greatly assist institutions in obtaining support from executive management and the necessary business units to identify and manage TPSPs more effectively. The proposed Guidelines provide exceptional depth in areas where there is no current US regulatory equivalent, notably supply chain risk management. These new requirements would affect both US institutions that utilise EU subcontractors and EU institutions that use US subcontractors. (Of course, it also would affect subcontractors around the world that work in any way with EU institutions.) Shared Assessments members have a general concern that real-world legal and commercial constraints will limit full supply chain transparency and directly interfere with their ability to achieve the goals of the draft Guidelines. Without additional regulatory assistance or guidance, financial institutions may be hobbled by the burden of incremental record-keeping, staffing, and other material expenses to comply fully with these updated requirements. **Alternative Regulatory Choices the EBA Should Consider**: One way for the EBA to address this overarching concern about the added resource burden is for EU authorities to include specific contractual requirements, similar to the EU Standard Contractual Clauses (SCCs) and extend those expectations to all subcontractors in supply chains. The GDPR SCCs are an illustrative precedent, as they have provided significant assistance to financial institutions in the negotiation of TPSP contracts. Importantly, SCCs reflect a more formal, unequivocal minimum standard of care expected from regulators, removing the uncertainty that legal, procurement, and risk professionals are otherwise expected to negotiate in otherwise standard, bespoke agreements that can extend weeks, months, even years in the worst cases. Shared Assessments' members have mentioned the unwillingness of third parties to detail subcontractors and outsourcers (regardless of criticality), among other points, in their standard terms. Some third parties lack visibility into their own supply chains beyond their direct subcontractors, which will lead to protracted and often unfruitful negotiations unless stipulated clearly and simply by regulators. Shared Assessments' members strongly suggest that the only way outsourcers are likely to have sufficient leverage to ensure visibility into the supply chain is for the outsourcer to include contract language that requires consistent hygiene from all providers in a supply chain. The EBA has an opportunity here to include supply chain contract language to achieve that outcome. That one action could materially reduce the cost of enabling the cascading levels of supply chain due diligence so important to achieving significantly improved risk management.

	As with DORA (see DORA Article 31(1a–1b) and Article 31(10))[1], whose designations of critical suppliers are expected this year, Shared Assessments recommends that the EU authorities also reference the DORA list of critical supply chain vendors (those directories of designated critical third parties will be updated annually, but a link to updated rosters can be provided in the guidelines). Of course, even a non-ICT third party service provider may utilise an ICT service provider that itself may or may not officially be designated as critical. Once a supplier in a third-party service provider's supply chain has been officially designated as critical under DORA, neither the outsourcer nor the subcontractor would have any discretion in its reporting transparency. The Guidelines may not discuss enough how critical suppliers might be part of any supply chain, even where the overt description of the supply chain might not suggest that. Rather than omitting discussion of how DORA-designated critical TPSPs fit into supply chains for seemingly non-ICT outsourcing relationships, the EBA should base its Guidelines on and acknowledge the everyday blurring of ICT and non-ICT relationships.[2] With regard to Definitions (paragraph 16), we believe "Concentration risk" is broader in scope and potential impact than the number of TPSPs performing any function. In fact, in our experience and that of our members, geographic or location concentration risk (whether service locations from a single TPSP or multiple TPSPs in a single country, province, territory, or metropolitan area reliant on the same transportation or energy infrastructure) is another material form of this risk essential to recognise and to manage. Accordingly, we recommend revising this definition in the final Guidelines to ensure regulated firms consider this broader perspective to manage those additional aspects of TPSP risk that have affected our members and the industry in many instances.
Question 2: Is Title II [Third-party arrangements] appropriate and sufficiently clear?	**Response:** With a few exceptions noted in the discussion below, Title II is appropriate and sufficiently clear. Section 4, paragraphs 33–37, describes the methodology for an institution to determine the criticality of subcontractors well, even as many of the stated risks in this part are not defined per se under paragraph 16. **Alternative Regulatory Choices the EBA Should Consider**: Per paragraph 30, the Guidelines helpfully note several situations where "consideration should be given" that include where TPSP support is "recurrent or ongoing" and whether such is "a mere purchase of a good." However, an additional and arguably more important consideration is whether TPSP support represents an Outsourcing arrangement, as

[1] DORA, Article 31(1a-1b): The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 32(1), shall:
(a) designate the ICT third-party service providers that are critical for financial entities, following an assessment that takes into account the criteria specified in paragraph 2;
(b) appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible, in accordance with Regulations (E.U.) No 1093/2010, (E.U.) No 1094/2010 or (E.U.) No 1095/2010, for the financial entities having together the largest share of total assets out of the value of total assets of all financial entities, using the services of the relevant critical ICT third-party service provider, as evidenced by the sum of the individual balance sheets of those financial entities.
DORA, Article 31(10): For the purposes of paragraph 1, point (a), competent authorities shall, on a yearly and aggregated basis… assess the ICT third-party dependencies of financial entities based on the information received from the competent authorities.

[2] DORA's definition of "critical ICT third-party service provider" is: "an ICT third-party service provider designated as critical in accordance with Article 31."

	defined by the Guidelines, and we recommend adding this point because of the potentially exceptional risk involved in that instance. Additional guidance may be needed in Section 3, paragraph 32 (functions excluded from Guideline scope), especially for points c (clearing) and e (correspondent banking services). Such functions may be ICT or FMI (financial market infrastructure); this may confuse readers. The Guidelines' explanation – that it is the responsibility of the financial institution to determine whether a subcontractor falls under ICT or DORA (with DORA prevailing) is made clear in footnote 42 on page 27 of the draft Guidelines. This citation is also important in the discussion of the Guidelines' Paragraph 50, below. We recommend elevating footnote 42 to the main body of the Guidelines and clearly stating this to eliminate this confusion. Shared Assessments strongly agrees with the EBA's approach in 32(f) and 32(g) without prejudice to the risks such TPSPs could still pose. One point that the EBA may wish to clarify is what threshold of ICT content places a subcontractor or function under DORA versus under the non-ICT Guidelines. This guidance would help financial entities that struggle to make the correct classification. An exclusion may also be needed for highly regulated functions that fail to qualify under (e) correspondent banks or (g) utilities (insurance carriers, for example).
Question 3: Are sections 5 to 10 (Title III [Governance framework]) of the Guidelines sufficiently clear and appropriate?	**Response**: With a few exceptions noted in the discussion further below, Title III is appropriate and sufficiently clear. Section 5: Overall, Section 5 aligns with industry best practices. Shared Assessments agrees with the approach in paragraphs 38 and 39 and especially appreciates the EBA's reference to a "holistic" institution-wide risk management framework. The decision to outsource by itself may create risk since not every potential outsourcer is equipped to oversee specific third-party relationships. Shared Assessments strongly endorses paragraphs 45(b) and (c) and the criticality of having sufficient internal resources in financial institutions to manage the outsourcing process. Section 6: Overall, much of Section 6 appears to be in line with general industry best practices, including at least annual reviews of "a written policy on third-party risk management" (paragraph 48) and inclusion of all phases of the lifecycle (paragraph 49). However, aspects of paragraphs 50 and 51 have problematic elements discussed further below. Paragraph 48 forces consideration of TPRM at the board level. Board-level oversight of third-party risk management programs is a critical component in any governance structure. Shared Assessments' research over the last decade has often found that board-level engagement in third party risk management activities has correlated with greater program maturity. While any board can delegate certain of its activities to management, paragraph 48 appropriately reinforces board responsibility. Paragraph 51 is an excellent reminder of the importance of considering the outsourcer's risk profile and potential business continuity issues as a critical component in outsourcing policies.

	Section 7: Shared Assessments agrees with the conflicts of interest language in paragraphs 52, 53, and 54. Section 9: Shared Assessments agrees with the EBA's language in Section 9. **Alternative Regulatory Choices the EBA Should Consider**: We urge the EBA to consider integrating the requirements of the entire paragraph 45 ("Financial entities should…") to the list of requirements under paragraph 43 (the direct duties of the "management body") to ensure the critical requirements of clear assignments, sufficient resource allocation, and the establishment of a designate are promoted with equal vigor and not left to the internal political uncertainties of budget and resource advocacy from lower levels in the organisation. Notably, per paragraph 43, if the management body already "is at all times fully responsible and accountable for at least…overseeing the day-to-day management…including the management of all risks associated with third-party arrangements" these other duties under paragraph 45 warrant direct inclusion here. Importantly, in our collective and often pained experience, this will reduce the organisational risk of expecting the second and third lines of defense to exercise sufficient internal power to ensure such assignments, resourcing, and other support are addressed, rather than negotiated with the management body and too often without sufficient success. An appropriate tone from the top is driven more forcefully when these other responsibilities (along with strategy and financial health) remain firmly with the management body, in our considered experience, including our varied individual experiences as leaders who have launched and matured such programs. Paragraph 50 calls on organisations to differentiate at the level of policy between ICT functions (where DORA prevails) and non-ICT functions (where the draft Guidelines prevail). We respectfully disagree with the value or need for such a distinction, particularly at the level of a policy. Frankly, we consider this inadvisable. Like organs in the human body, ICT and non-ICT functions at a financial entity are organically connected, and risks cascade across both, so policy language should not create any distinction between them, focusing instead on what are commonly shared risks. By forcing an artificial separation by service types often negligibly distinguished at the policy level, the essential, interconnected relationship between both could be disregarded or even missed. This is another instance where Shared Assessments strongly suggests the EBA elevate Footnote 42 on page 27 to the body of the Guidelines. The financial entity must determine whether the use of ICT somewhere in the supply chain is material and therefore triggers the use of the DORA framework rather than the Guidelines. The outsourcer must inform the TPSP that the relationship is now a DORA relationship. Importantly, the EBA should use the Guidelines to communicate its expectations when DORA is triggered in this way. What are the responsibilities of the outsourcer to the TPSP and to the remainder of the supply chain? By extension, the Guidelines should allow an enterprise risk management, operational, or resilience risk management policy or related group of policies to accomplish the same outcomes, not strictly a third-party risk management policy per se. In our experience, many organisations publish policy at highly granular levels by risk type or risk function, where others take a more consolidated approach and may address third-party risk management in other types of policies. In fact, their

	management structures and accountability may align better to those other types or combinations of policies without the need for an explicit or carved out third-party risk management policy. These same points apply to paragraph 51; allow financial entities to define their own appropriate mix of named policies, focus instead on their need to address all aspects of the EBA Guidelines in relation to their unique governance frameworks. Section 8 (business continuity plans) does not adequately stress that subcontracting parties anywhere along the supply chain should be considered when they represent a critical function in the TPSP's supply chain and may represent an industry concentration risk that may affect multiple TPSPs.[3] (This is also referred to in Paragraph 77.) The risk is that long and complex supply chains reduce the ability of competent authorities to oversee critical or important risks properly. Mitigating outsourcing risks requires supply-chain transparency, ensured by specific contract requirements, so that the outsourcer's mandated hygiene applies throughout the supply chain. The EBA should ensure that contract requirements clearly specify the importance of achieving transparency. Section 10 (documentation requirements). The draft Guidelines should explicitly state that an organisation may keep a local registry to satisfy local requirements. However, all local information must be passed on to the parent organisation for inclusion in a single registry. Section 10, paragraph 64: For critical or important functions of third-party arrangements, this part highlights the need to track key information about such TPSPs, all of which are vital in their management. However, from a risk management perspective, the notable gap in these expected requirements is the documentation of material deficiencies that may (and often will) exist in current agreements, such as obligations to maintain and test resilience plans, subcontractor notice, and incident response plans. Material contractual gaps are at least equally vital to record and to track to resolution as the other attributes these Guidelines stipulate in this paragraph. For example, the current Guidelines establish the need at this paragraph for "the existence of an exit plan" but an equally material set of considerations (and potential risks) is whether the related TPSP agreement allows for such, allows for termination, and even stipulates transition assistance during an exit. In the absence of such contractual terms, a mere exit plan may prove entirely academic and grossly insufficient in real-world situations. As a result, material contractual deficiencies should be recorded and made more transparent for the management body, the internal audit function and, as needed, any competent authority. Section 10, Paragraph 64(c) requires financial institutions to include the names of subcontractors in their register "to which material parts of a critical or important function are sub-contracted…" and to list detailed information about such subcontractors. As noted previously, Shared Assessments members often report difficulty having TPSPs provide any information about subcontractors, much less the identification of their own critical subcontractors and the additional details mentioned in the paragraph. However, the Guidelines emphasis on proportionality

[3] See, for example: https://www.riskrecon.com/report-risk-to-the-nth-party-degree

	and the qualification of "material" at paragraph 64(c) should reduce this burden if applied equally by financial entities and their competent authorities. The EBA can help financial institutions achieve the Guidelines' goals by specifying that third parties provide complete critical or important subcontractor identification to outsourcers. Ideally, that language would be included in all subcontractors' agreements (and so forth down the line).
Question 4: Is Title IV [third-party arrangement process] of the Guidelines appropriate and sufficiently clear?	**Response:** While many provisions in Title IV are appropriate and sufficiently clear, there are many others that are neither appropriate nor proportionate to the potential TPSP risks involved. Many provisions in this Title should be limited to outsourcing arrangements and/or critical or other important functions but not all TPSPs by default. In our view, applying many of these provisions to TPSPs more generally will create incredible resource burdens for financial entities and may prove extremely burdensome to implement with limited value for lower risk services. Section 12.2 (Access, information, and audit rights). This important paragraph specifies that outsourcers ensure contractual commitments to TPSP audit rights not just for the financial institution but also for competent authorities. Shared Assessments strongly supports extending critical or important TPSP audit rights to competent authorities. Section 13 (Monitoring), Paragraph 111 (financial entities should monitor…the performance of the TPSP…), Shared Assessments notes that no specification is made by the draft Guidelines for the scope, periodicity, technology, or tools utilised for ongoing monitoring. Our organisation believes this is wise. There is always residual risk, regardless of the level or intensity of monitoring. Scope, periodicity, and technology are all functions of the risk. **Alternative Regulatory Choices the EBA Should Consider**: Section 11, Paragraph 70: Shared Assessments notes that subcontractors (Nth parties) are not mentioned here. Good practice increasingly demands that financial entities consider supply chain characteristics beyond the TPSP for critical or important functions, and we recommend making this requirement explicit here, potentially as an added subpart f (after the conflicts of interest provisions in subpart e). Section 11.2 (Risk assessment of third-party arrangements) is appropriately broad and in-depth. Shared Assessments acknowledges that this section is broad, because different organisations must make their own assessments of inherent risk for areas material to the business. However, the Guidelines should consider requiring financial entities to document how they arrive at their assessment of criticality, absent authoritative designation. Further, we suggest that noting the DORA definition of "critical ICT third-party service provider" for the draft Guidelines will be helpful in setting the context for non-ICT institutions. EU-named Critical ICT Service Providers will be part of the regulatory landscape. The draft Guidelines do not explicitly address that reality. Paragraph 74: the proposed duties on financial entities are good practice for all TPSP engagements but only subparts a (risk management, compliance, and audits), b (potential impact on clients), and d (risk of service scale up without attendant contractual changes). However, the remaining provisions are more relevant and useful to apply to outsourcing arrangements, critical functions, or even important

	functions, including c (size and complexity of affected business area), e (TPSP substitutability), and f (ability to reintegrate the function). Indeed, subpart f implies an outsourcing arrangement and should be limited to such, while subparts c and e are not necessary considerations, in our experience, for the majority of lower risk, non-client-related services from TPSPs supporting financial entities. Finally, with respect to subpart g in this paragraph 74, these requirements represent a more granular expression of risks that are necessarily captured in subparts a and b of this paragraph. Accordingly, we recommend adding the details of subpart g to the appropriate parts of a and b where those may apply (e.g., outsourcing arrangements but not applicable in most TPSP engagements). Paragraph 75: Given the broad sweep of the recommended assessment practices here, we recommend the Guidelines here more directly stress the points "where appropriate" and "taking into account the principle of proportionality" by highlighting the need for this level of rigor only for outsourcing arrangements and critical or important functions. As the majority of TPSP engagements will be neither or none of these, the Guidelines risk imposing an excessive standard of care here on the great majority of less material TPSPs and potentially limiting the ability of a financial entity to perform these necessary assessments on their smaller minority of higher risk engagements that are outsourcings, critical, or important. Absent that refinement in these Guidelines, the resource burden on financial entities and their risk programs could prove overwhelming and undermine a suitable focus on proportionate risk management. Paragraph 76: As with our comments about paragraph 75 above, these additional considerations for a financial entity risk assessment should apply in a more proportionate manner to outsourcing arrangements, critical or important functions, or both, to ensure the management body is able to apply appropriate focus to its greatest risks, not all TPSPs by implication, whether intended or otherwise. Paragraph 77 (especially point b) refers to subcontracting critical functions by a TPSP, and acknowledges that "the risk that long and complex supply chains of subcontracting reduce the ability of financial entities to oversee the critical or important functions and the ability to effectively supervise them" highlights the need for outsourcers to know the critical suppliers named by DORA as well as the need to implement contract requirements for non-ICT services that are fully passed down the supply chain. In addition, as this paragraph 77 is usefully designed to anticipate "the possibility that the TPSP subcontracts critical or important functions to subcontractors," the presumption that the TPSP is performing such critical or important functions should be made explicit to prevent confusing financial entities with a regulatory presumption or expectation that a non-critical or non-important TPSP could possibly subcontract a higher risk service than their own. We recommend that this paragraph open with the more appropriate and limiting condition: "Where a critical or important third-party arrangement includes the possibility…" This will remove all doubt and maintain the proportionality principle so usefully highlighted by these Guidelines. Paragraph 78: As with our comments about paragraphs 75-77 above, these additional considerations for a financial entity risk assessment should apply in a

	more proportionate manner to outsourcing arrangements, critical or important functions, or both, to ensure the management body is able to apply appropriate focus to its greatest risks, not all TPSPs by implication, whether intended or otherwise. Paragraph 80 (due diligence considerations): In our experience, subparts a through c represent best practice for TPSP due diligence generally, but subpart d (supervision by competent authorities) is material and relevant for outsourcing arrangements, critical or important functions, or both, but not all TPSPs, the majority of which are not and will not be supervised or need such by competent authorities. Accordingly, we recommend striking subpart d from this paragraph, and we recommend moving this requirement to Paragraph 81, which importantly is focused on "critical and important functions." Section 12 (Contractual phase). Overall, this section is well-crafted, but several modifications are worth considering, as below. Paragraph 85: Per subpart k, the expectation that any TPSP should contractually agree "to fully cooperate with the competent authorities and resolution authorities" is too sweeping in its scope and will create substantial burdens and delays in contractual negotiations, most unnecessary. While right to audit provisions are commonly expected and accepted, such already grant a competent authority the indirect but real ability to work through a regulated financial entity generally. More important, the challenge this creates for financial entities in a negotiated contract is that the vast majority of their suppliers are lower risk and not subject to direct oversight by the financial entities competent authorities. By forcing thousands of legal, procurement, and risk professionals at financial entities and TPSPs to negotiate mostly moot provisions across an entire supplier base is not productive nor proportionate, in our considered experience. This provision expected by financial regulators on both sides of the Atlantic has created orders of magnitude more trouble and organisational difficulty than necessary. We urge the EBA to move this subpart to the more suitable place at paragraph 86 (critical or important functions, even more specifically to outsourced arrangements in which contractual terms should always stipulate expected cooperation with competent authorities). Paragraph 85(a): This paragraph should highlight the third-party service provider's obligation to include contract language that requires consistent hygiene from all of its providers in a supply chain. Paragraph 86(e): This paragraph involves the right to monitor performance with an unrestricted right to inspect and audit.[4] An important question for US-based suppliers is whether provisions of paragraph 86 exceed US regulations, in which case those suppliers may be unable to service EU-based companies. What does the EBA expect to happen in geographies where inspection and auditing of a TPSP and other potential critical or important suppliers is not an authorised practice? Is there a risk that the number of suppliers available to EU-based financial entities could significantly diminish?

[4] In the U.S., regulators are authorised to examine technology service providers on behalf of insured depository institutions under the Bank Service Company Act, 12 u.s.c. 1861-1867.

	Section 12.1 (Subcontracting of critical/important functions) should be reviewed and revised to recognise and resolve (through the contractual recommendations noted above) the practical difficulties institutions have when contracting with TPSPs. These practical difficulties may make the Guidelines difficult to test or validate. As noted, the ability of financial institutions to address many of the provisions, particularly those of Paragraph 90 (nature of written agreement with subcontractor of critical functions), is extremely limited at the present time. Today, as a practical matter, a financial institution's oversight of a TPSP's management of their subcontract relations is primarily satisfied by requiring a TPSP to have a complete and robust third-party risk management program, and then by assessing the TPSP's execution of that program. However, as noted previously, even this approach is severely limited by the failure of TPSPs to identify which subcontractors are critical to the services that they provide to the outsourcer. Additionally, often there is no contractual requirement that critical or important subcontractors adhere to outsourcer hygiene requirements. DORA ensures that due diligence should be adequate for any formally designated critical third party. However, any critical or important non-ICT third-party service provider that, by definition, does not rise to the level of official EU designation and is buried in supply chains may present a special challenge. The issue goes beyond simple transparency; it affects the adequacy of due diligence that must be ensured throughout the supply chain. Paragraph 90 specifies TPSP obligations for subcontracting critical or important functions, but this does not appear to require TPSPs explicitly to maintain a subcontractor register, without which TPSPs may be unable to fulfill requirements. Paragraph 95 is critical to due diligence in longer supply chains and can be assisted by specific contract requirements with model language. Paragraph 100. Shared Assessments notes that this paragraph recommends extending access and audit rights to non-critical and non-important functions in contracts. The EBA should modify this paragraph by moving and rephrasing the last sentence ("…that functions may become critical or important over time.") to an introductory position in the paragraph so that readers better understand the rationale for such a requirement. Shared Assessments recommends that the EBA modify the language in paragraph 100 to clarify that financial institutions should seek access and audit rights in cases only where they reasonably believe a non-critical or important relationship could become more significant over time. Those judgments should also be reassessed regularly. Paragraph 102 refers to pooled audits. Shared Assessments strongly supports pooled audits and recommends that the EBA take concrete steps to make it easier for CPA firms to engage more vigorously in this activity. In the United States, AICPA (American Institute of Certified Public Accountants) practices make pooled audits somewhat difficult in practice. Paragraph 114 (Financial entities should monitor internal concentrations) should be extended to include concentration risk in supply chains. This paragraph refers to Section 11.2, Paragraph 77, which does specify consideration of the subcontractor

	concentration, but Shared Assessments suggests this specification should be made more explicit in Paragraph 114. Section 14 (Exit strategies). Financial entities planning to disengage from a TPSP with a complex supply chain should consider the Nth party's impact on the friction of withdrawal. That point should be emphasised in paragraphs 119 and 75.
Question 5: Is Annex 1 [Guidelines on third-party risk arrangements addressed to competent authorities], provided as a list of non-exhaustive examples, appropriate and sufficiently clear?	**Response:** With the exception of a few items listed further below, Annex 1 is appropriate and reasonably clear. **Alternative Regulatory Choices the EBA Should Consider**: Annex I at times appears to conflict with the exclusion at Paragraph 32, page 27. Paragraph 32 states (in part): "…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); and…" However, Annex I, Level 2 for Admin services would seem to fit into "that do not have materials impact on the financial entities' risks exposure or on their operational resilience." While other example categories also fit the bill, these are the most obvious. **Administrative services** • Advertising & Marketing; • Document Management & Archiving; • Insurance Services; • Payroll Services; • Pensions & benefits; • Postal services & Mailing; • Procurement & purchasing of services; • Secretarial Services; • Talent acquisition & hiring; • Travel & Entertainment Services; Other The EBA should acknowledge that many of the services listed in Annex I may still have substantial ICT components, and that some of those ICT components might be supplied by DORA-named critical third parties. As with non-ICT services having an ICT component, the Annex I list does not appear to designate legal functions as potentially critical, which, of course, they are. The definition of "a function" can be broad enough (process, service, activity, etc.) to bring nearly anything into scope if not exempted. The non-exhaustive list is helpful, warrants greater clarity. An expansion of the list with more examples of "critical/important," "non-critical," and "excluded" may help harmonisation. Legal services should be named specifically. Any of the services mentioned might include legal services that are themselves critical. For example, the line item "Customer Services: Product Design" might involve patents, trade secrets, and marketing plans under legal advisement that may be critical to an institution's plans and to its ability to compete effectively. A compromise at a legal firm could materially affect the operation of non-ICT institutions. In addition, many of the functions listed in Annex I can have a legal component.