3.10.2025

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

**Comments of the Austrian Banking Industry**

**Q1: Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?**

It should be clarified:

* Which agreements fall under the EBA Draft Guidelines on the sound management of third-party risk (EBA GL)?
* How are non-ICT services treated that meet the definition of a third-party agreement but do not constitute outsourcing agreements?
* What consequences will the classification "outsourcing" have in the future and what are the associated implications?

Our understanding is that the new EBA GL will separate ICT and non-ICT services in future. The EBA GL therefore only cover permanent/recurring services that

* are not qualified as ICT services under DORA ("these Guidelines only cover the use of TPSPs providing or supporting functions that are not qualified as ICT services under DORA" (recital 7) and
* are not covered by the exemptions under recital 32.

As a result, the outsourcing register should no longer contain any ICT-relevant, outsourcing-relevant third-party agreements in future. In our opinion, the outsourcing register and the information register are not identical in terms of requirements.

This distinction is currently supported by established processes and would lead to legal ambiguities and uncertainties because of the new requirements of the draft guidelines.

In future, outsourcing should also be recorded in the outsourcing register, regardless of whether it is ICT-relevant or not. This is subject to the two registers being compatible and matching. The scope of application should be clarified to exclude Austrian leasing companies, as this is not always clear from the draft.

According to our understanding, the application of the guidelines is limited to “run-the-Bank”-services. However, this is not entirely clear from the current wording. We therefore propose the following amendment (see also below under Title II) to include an explicit exemption for “change-the-bank” services in Recital 32.

Further it should be clarified

* that the introduction of a **centralised outsourcing register between members of the same IPS is possible**, thus eliminating the need for each bank to maintain its own outsourcing register. This ensures that administrative costs are reduced and joint outsourcing arrangements are only recorded once.
* that **group-wide exit plans between members of the same IPS are possible**, thus eliminating the need for each banking institution to have its own exit plan. This ensures that administrative costs are reduced.

The above points would simplify organisational and administrative procedures. In addition, the default risk for intra-group service providers is minimal due to consolidation with the parent companies.

Finally, the questions remains if there will still be a distinction between significant and non-significant outsourcing?

Moreover, it should be clarified that there’s a still a distinction to be made between critical and non-critical outsourcing, regardless of whether ICT relevance is involved or not. This distinction should be kept.

Ad definitions:

In Section 3 (Background and rationale), Recital 17 states that the “definition of ‘critical or important function’ is in line with the definition in Article 3(22) of DORA.” While we do not dispute this statement, the use of the term throughout the document is not consistent with the approach under DORA. Accoarding the DORA, an arrangement with a third-party provider may “*support”t* or “*concern”* a critical or important function of the financial entity, but it does not establish such a function by itself.

Section 3, Recital 20 requires financial entities to determine “whether the function to be provided by a TPSP is considered critical or important”.  In our understanding, the term “function” is used here as a synonym to “service”. This broader function definition, covering third-party services and financial entities processes will not be manageable in the context of the register of information (RoI) under DORA and the register of third-party arrangements in Section 10 – as DORA requires in the RoI a full list of functions and information how these functions are supported by third party (ICT-)Services, whereas this guideline would classify the Third-Party engagements being critical and important functions.

We propose a closer alignment with the DORA framework by categorising third-party arrangements as “supporting critical and important functions,”. The classification of “functions” should remain reserved to financial entities, which retain full accountability for their proper execution, even where certain elements are performed by third-party service providers.

Ad Transitional arrangements (see Recital 19 and 20):

While Recital 19 refers to “third-party arrangements of critical or important functions” with regard to the proposed 2 year transitional period, recital 20 refers to “all existing third-party arrangements”. Experience from DORA and the BRRD related changes of documentation show that negotiations with vendors can be rather tedious, especially with regard to (pre-)existing documentation. We therefore would appreciate an alignment of these two provisions with a fixed transitional period applying only to third-party arrangements of critical or important functions while stipulating a “best-efforts”-clause with regard to the remaining services (based on a respective prioritization/adaption plan).

**Q2: Is Title II appropriate and sufficiently clear?**

Ad Recital 32 – listed exemptions:

While it is shortly mentioned in Recital 30 that “consideration should be given to whether the function is provided or planned to be provided by a TPSP at least on a recurrent or ongoing basis”, this aspect is then not expressly mentioned in recital 32. As we understand it, the guideline is clearly intended to apply to recurrent or ongoing “run-the-bank” services only, and not to one-time, project-based “change-the-bank” services (such as business or strategic consultancy provided during a specific project). For the sake of legal clarity and consistency, we would therefore welcome the inclusion of an explicit exemption for “change-the-bank” services in Recital 32.

In addition, the list includes various office services and mailrooms, post-room services etc. In this context, we suggest clarifying whether print activities also fall under these exemptions. If so, it would be helpful to explicitly mention them within the guidelines.

Ad Recital 37 – “…function performed by financial entities…”

The term “function performed by financial entity” in the first sentence in combination with a) and b) would indicate that a new arrangement with a third-party could:

1. create a new function for the financial entity
2. change an already existing, non-critical function into critical function when it is not executed by the bank, but by a third-party
3. require a splitting of an existing function - or creation of a “sub-function” if only a part of an existing function is subject to a service provided by a third party
(e.g. the function of the bank is “Ensuring Anti Money Laundering for transactions” and only some scanning is received through a third-party service)

We therefore ask for a clarification whether this is really the intention of this section. Underlying issue maybe the point mentioned above related to definitions.

**Q3: Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?**

It should be clarified if only non-ICT-relevant contracts be listed in the outsourcing register in future.

In addition, clarification is needed that non-ICT services and ICT services will be listed in the register in accordance with the new EBA GL.

In future, the outsourcing register will continue to be based on outsourcing, regardless of whether it is relevant to ICT or not. This is subject to the two registers being compatible and matching each other.

The scope of application should be changed in such a way that there will continue to be two registers in future, in which the relevant contracts are to be maintained separately in the register.

The established processes would be complicated by the separation into ICT and non-ICT. If there is a focus on ICT-relevant third-party agreements, there is a risk that outsourcing-relevant agreements will no longer be adequately monitored.

If information is removed from the outsourcing register because it is transferred to the information register, information will be lost for third-party risk management for non-ICT-related outsourcing contracts.

Additionally, the questions remain what does it mean that the outsourcing register should be compatible with the DORA information register and which information/data points does the reference in the draft EBA GL regarding discrepancies refer?

In our view, it should be explicitly laid down that two separate registers are to be maintained.

No new mandatory fields should be introduced, as this would lead to increased administrative costs and make third-party management more complex and expensive overall, without any apparent improvement in the management of third-party risk.

It should be clearly explained how the discrepancy between the two different registers is to be understood, as the information register contains much more extensive ICT obligations and more mandatory fields.

The question remains if the reference to the discrepancy does relate to the information that must be included in the register according to the draft EBA guidelines or does the reference relate to the information that DORA provides for the information register.

In our view, the two registers should remain in their current form.

Ad Recital 63 lit g, Register of arrangements

It required to provide the LEI Code or EU-ID of an identified Alternative Service Provider. Taking into account that there might not be an existing business relationship with the potential alternative supplier, the financial entity might not be in the position to negotiate a supplier outside of the European Union to get a LEI and also an EU-ID does not exist.
We therefore suggest to be less restrictive with this information and allow the company name – or at least a more general identifier like the company register number.

**Q4: Is Title IV of the Guidelines appropriate and sufficiently clear?**

Ad Recital 72 lit b and lit c:

With regard to TPSPs that are situated outside of the European Union (which are targeted by such provision), it seems unlikely that respective cooperation agreements are in place between all respective supervisory authorities. Further, it seems unlikely that even if such agreements are in place, that details of such agreements will be disclosed upon a mere request of a customer of a TPSP or that supervisory authorities will be prepared to amend such agreements on a respective request. Since these are thus requirements that will not be fulfillable in all circumstances, we would appreciate if they are either taken out or if at least it is clarified how financial entities may proceed absent strict compliance with such requirements.

Ad Recital 74:

The assessment seems not to differentiate between critical/important functions and others (compare in this context section 11.3 which clearly distinguishes between the respective functions). Since certain requirements only apply to critical/important functions (e.g., enhanced business continuity and exit plan requirements – again see also in section 11.3), we would appreciate a differentiation also at such stage.

Ad Recital 81 lit c:

The reference to geographic dependencies seems like an outlier in this context since the remaining lits of recital 81 stipulate “positive” requirements that can be checked whereas lit c seems to be a reference to a “negative” requirement (i.e. these should not be present or if they are they should be mitigated). We would therefore recommend to separate lit c and make it a separate recital.

Ad Recital 83:

We want to refer to the ongoing discussions about supply chains, which will be regulated separately and which are currently under review as to their extent and thus should in our view not premeditated by too widely formulated requirements within the context of general third-party management rules. Against this background a revision would be appreciated.

Ad Recital 84:

Contracts can be rather complex, so in our understanding, it should be possible that the documentation of respective contracts may not be in “one” single agreement but in a conglomerate of several related agreements.

Ad Recital 85 lit j:

The requirements listed for all third-party agreements respectively for those that relate to critical/important functions should in our view be aligned with the respective parallel requirements under DORA and the BRRD. Since recital 85 lit j seems to be doubled and further clarified in recital 86 lit e and since the parallel requirement under DORA also is stated for critical functions only, we recommend to delete recital 85 lit j.

Ad Recital 86 lit c:

This seems to be a new requirement when compared to DORA/BRRD. Since insurance is rather a mitigating factor which might be required following certain risks identified during a respective TPSP due diligence, we would recommend to make this an optional point and to link it to respective risks (i.e., to include respective insurance requirements in the contract in case respective risks have been identified and risk mitigation matters are required as a consequence).

Ad Recital 88:

The article refers to subcontracting of critical or important functions or material parts thereof. This might be difficult to execute in praxis, as the criteria that led to the definition of a service to be critical or important might not always be transparent to the rank 1 supplier of the service and it might not be possible to provide the rank 1 supplier enough information to be able to execute a proper assessment whether its sub-supplier (rank 2 supplier) would be a critical or important function from the banks perspective.
An alternative approach would be to define the level of reliance of the service (rank 1) on the sub-provider (rank 2), assessing the potential impact of a non-availability or poor execution of the sub-service on the main service.

Ad Recital 98:

This recital seems to partly overlap with the resolution resilience requirements under the BRRD and related legislation. From a documentation perspective, institutions include references to resolution authorities in addition to supervisory authorities in our agreements when regulating audit and access rights and we include our standard resolution resilience clauses in contracts that are relevant from a resolution resilience perspective. Thus, it is ensured that the same access and monitoring rights will be granted to all relevant authorities and by avoiding too specific references, the respective rights are future-proof in case of future changes/additional requirements.

Ad Recital 109 lit b:

The current wording appears too broad and may be difficult to agree with TPSPs. In practice, TPSPs are often concerned when termination rights are drafted in vague terms, as this may be perceived as a potential ‘disguised’ termination for convenience. We therefore suggest, at least, to change to “capable of materially negatively altering”. Alternatively, lit b could be removed since it seems to be already covered by lit c.

**Q5: Is Annex I, provided as a list of non-exhaustive examples, appropriate and sufficiently clear?**

See also our comment as to the scope: We would appreciate and recommend a clarification that only “run-the-bank”-services are in scope, maybe also with some examples of out-of-scope services.