POSITION PAPER

ESBG response to EBA consultation on draft Guidelines on the sound management of third-party risk

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

October 2025

ESBG

GENERAL INFORMATION

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions detailed below.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- are supported by a clear rationale;
- provide evidence to support the views expressed / rationale proposed, and;
- provide alternative regulatory options for consideration by the EBA.

GENERAL INFORMATION

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

We appreciate that the draft Guidelines are built upon the 2019 Guidelines on outsourcing arrangements and aligned with the framework introduced by the DORA Regulation. This will help financial entities to operate in a more consistent, solid and predictable framework. Nonetheless, we believe some adjustments are needed in order to improve the clarity of the text.

Ad definitions:
Regarding the definitions, we suggest including the concept of services on an "ongoing basis" in the definition of "third-party arrangements", as it would enhance consistency with DORA ("ICT services" definition) and reduce interpretative uncertainty. Additionally, we see merit on clarifying the interplay between the definitions of "outsourcing arrangements" and "third-party arrangements". We would also appreciate an extension of the definition of "third-party arrangements" to include a reference to the criteria set out in Section 3 (paragraphs 30-32). The proposed definition of third-party arrangement in para. 16: "an arrangement of **any** form […] for the provision of one or more [of **any** process, service or activity or part of it]", otherwise might not leave room to exclude anything, even though para. 32 then goes on to exclude certain functions from the definition. This leads paragraphs 30-32 to conflict with the definition in para. 16.

In monistic and dualistic systems, the definition of "management body includes different responsibilities. We, therefore, in line with the governance guidelines (EBA/GL/2021/05), ask for clarification that the requirements do not interfere with the structures and responsibilities under national company law.

Section 3, Background and rationale states in para. 17 that the "definition of 'critical or important function' is in line with the definition of Article 3(22) of DORA. Not disputing this statement, the usage of the term throughout the document is not consistent with the approach in DORA, where an arrangement with a third-party provider will "support" or "concern" a critical / important function of the financial entity, but will not establish a function by itself.

Moreover, we strongly recommend that the Guidelines adopt the definition of critical or important functions (CIFs) as laid out in Article 3(22) of DORA. This definition is sufficiently precise and has already been implemented across ICT-related regulatory processes. By contrast, paragraphs 33–37 of the draft Guidelines introduce additional and vague criteria, which could lead to nearly all TPAs being classified as critical or important, given that some level of operational or reputational risk can almost always be identified. In line with DORA, only those services whose failure would materially impair a financial institution's performance, continuity, or regulatory compliance should qualify as

CIFs. Using a single, consistent definition across both frameworks would be more effective and promote supervisory convergence.

Paragraph 20 of section 3 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.

Our proposal would be to further harmonise with the DORA approach and categorise third-party arrangements as "supporting critical and important functions" with the according level of reliance - and keep the term "functions" for the financial entities, which remain accountable for its correct execution, even if they have parts of it executed through third party services.

Ad Transitional arrangements (see section 3. – Implementation, paragraphs 19 and 20):
While para. 19 refers to "third-party arrangements of critical or important functions" with regard to the proposed 2-year transitional period, para. 20 refers to "all existing third-party arrangements". Experience from DORA and the BRRD related changes of documentation show that negotiations with service providers 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).

Additionally, we suggest establishing a phase-in period between the publication date and the date of entry into force. Financial entities need adequate time to implement the new requirements, particularly as a review, as mentioned in para. 17, does not immediately result in compliance will all the guidelines' provisions and many contracts are open-ended and not explicitly renewed.

We welcome the clarity of the draft Guidelines regarding the application of the proportionality principle. However, we would like to suggest a few targeted clarifications to ensure that proportionality is explicitly applied to smaller financial entities, in line with the Digital Operational Resilience Act (DORA):

Ad para. 22:
We suggest the following addition: *"For smaller financial entities, and in the supervision thereof, the principle of proportionality allows governance arrangements and ICT risk management controls to be adapted to the organisational nature of the entity, recognising that reliance on ICT third-party service providers is often inherent to their business model. Competent*

authorities should apply supervisory expectations in a manner proportionate to the size, complexity, and ICT risk profile of the institution, reducing unnecessary administrative burdens while maintaining effective operational resilience oversight."

Ad para. 23:
We propose adding: *"For smaller institutions, the principle of proportionality should recognise that extensive reliance on ICT third-party service providers is often inherent to their business model, and that oversight, monitoring, and documentation obligations should be adapted to allow such institutions to rely more directly on the governance, controls, and reporting mechanisms of their ICT third-party service providers, without being subject to the same operational and administrative requirements as larger institutions. Competent authorities should consider this proportional approach when conducting ICT operational resilience supervision."*

Ad para. 24:
We recommend the inclusion of a clarifying sentence: *"Smaller entities are not expected to implement all measures with the same depth or formality as larger entities; they may rely on the governance, internal controls, and reporting mechanisms of ICT third-party service providers in accordance with their outsourcing arrangements, provided that such reliance is consistent with the institution's ICT risk management framework and with the supervisory expectations under DORA. Competent authorities should adopt a proportionate approach when assessing compliance."*

These clarifications would improve the practical applicability of the Guidelines, ensuring that requirements are proportionate to the size, complexity, and ICT risk profile of different financial entities, while preserving alignment with the objectives of DORA and regulatory operational resilience requirements.

Ad subpoint 2.26.a:
Since TPSPs are not always directly part of the group or ISP, which is suggested by the wording "TPSPs within the group or the institutional protection scheme", this subpoint does not cover all the usual situations in this context. For clarification, we suggest "TPSPs within group or institutional protection scheme (IPS)-related structures".

***Question 2**: Is Title II appropriate and sufficiently clear?*

Although we support Title II, to avoid over-scoping and consistent with para. 3.32 exclusion and the existing CIF criteria, we suggest adding a couple of borderline examples (e.g., general support functions such as PMO or market data info providers) to Annex I or the main text, clarifying they are not critical/important unless they directly affect service continuity.

For clarification purposes, we recommend that section 3 under Title II be renamed, e.g. "Identification of (non-ICT) third-party arrangements".

Ad para. 3.32 – listed exemptions:
While it is shortly mentioned at para. 3.30 immediately above 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 para. 3.32. Since the guideline as we read it clearly is intended to apply to recurrent/ongoing "run-the-bank"-services only and not to one-time/project like "change-the-bank"-services (like, e.g., business or strategic consultancy during a project), we would appreciate to have also included an express exemption for "change-the-bank"-services in para. 3.32. We also believe that under para. 3.30, "personal computers" should be omitted as these are covered by DORA.

In addition, the list includes various services that do not have material impact on the financial entities, mailrooms, post-room services, etc. In this context, we suggest clarifying whether print activities as well as canteen operations also fall under these exemptions. If so, it would be helpful to explicitly mention them within the guidelines. Under point 3.32.g, we also suggest that telephone line be replaced by telephone services.

As the draft Guidelines propose to assess third-party arrangements (excluding the exceptions mentioned in paragraph 32 (a) to (g) and "a mere purchase of a good" described in paragraph 30), we see merit on clarifying the expectations about the assessment of "recurrent or ongoing basis" mentioned in paragraph 30: "(…) Within this assessment, 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". We believe this clarification would be useful because we understand that the draft guidelines aim to include any third-party arrangement irrespectively of its recurrency.

Furthermore, while we welcome footnote 42, as it can help reduce double regulation and compliance costs, we believe that the content should not only be included in the text but also extended, to include:

- If an ICT service is only marginally/insignificantly supplemented or supported by other services, treatment under DORA alone is sufficient.
- If another service is only marginally/insignificantly supplemented by an ICT service, treatment in accordance with the EBA guidelines alone is sufficient.
- Similarly, treatment under the EBA guidelines is sufficient in all constellations in accordance with ESA Q&A 2999 - DORA030 regarding the provision of ICT services in connection with supervised transactions/services by another financial entity.

Overall, we consider the wording in **section 4** to be too broad, especially in comparison to the definition of "critical or important functions" in Article 3(22) of DORA. Paragraphs 4.33 to 4.37 leave a lot of room for interpretation and could ultimately result in financial entities having to classify almost all TPSP arrangements as "critical or important". As with DORA, however, this classification should only apply to services where a failure or malfunction would

significantly impair the financial entity or lead to a breach of its authorisation conditions and obligations.

Ad para. 4.34
For clarification, we recommend the following change: "When relying on a TPSP for operating an internal control function of the financial entity or tasks thereof,".

Ad para. 4.35
We assume that the reference should be to section 11.1 instead of section 12.1

Ad para. 4.37 – "…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:

I.) create a new function for the financial entity
II.) change an already existing, non-critical function into critical function when it is not executed by the bank, but by a third-party
III.) 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 kindly ask for clarification whether this is really the intention of this section. Underlying issue may be the point mentioned above related to definitions.

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

Ad para. 5.38:
For clarity reason: the strategy and the policy are different documents, for which different responsibilities may be entailed. We therefore recommend a modification of the wording of para. 5.38 to "Such strategy should ~~include~~ reference the policy on the sound management of third-party risks ...". Furthermore, as financial entities should have the freedom to develop integrated or separate strategies for non-ICT and ICT services, clarification of this matter in the text would be welcome. Finally, we would value if the guidelines made it more clear what the other components of the overarching third party risk strategy, especially considering that some translated versions of EBA guidelines use the same word for both "policy" and "strategy" (e.g. the Swedish version of EBA/GL/2014/15 uses the Swedish word "strategi" for both the English words "policy" and "strategy".

Ad para. 5.40:

We believe that detailed individual risk assessments, in accordance with section 11.2 (also for arrangements/services not covered by the guidelines) would be completely disproportionate, implicating superfluous time and resources. We therefore suggest clarification. Arrangements not covered by the scope (criteria in section 3) should be included in the financial entity's overall operational risk management.

Ad para. 5.41:
As clarified again in subpoint 5.47.g, GDRP applies here and therefore, para. 5.41 seems superfluous.

Ad para. 5.43:
Taking into account the efforts of simplification and reducing regulatory complexity, para. 5.43 contains overarching requirements, which overlap with CRD. We therefore suggest removing points a; b; c; d and f and maintaining only the points essential to TPRM.

Ad point 5.45.b:
Even though it would be prudent to allocate sufficient resources for ensuring compliance with all legal and regulatory requirements we suggest that the requirements in these guidelines should be limited to the allocation of sufficient resources regarding the requirements relevant to TPRM.

Ad point 5.45.c:
It is unclear if the responsibilities are the same for a person with an "established role" as for a "designated member of senior management". The "established role" should monitor TP arrangements, whereas the "member of senior management", if designated, seems to have further reaching responsibilities. We assume that the responsibilities should be the same, which, if so, could be clarified.

Ad points 5.45.a and b
We believe that, in order to reduce regulatory overlap, the guidelines should focus on the management of third-party risk and not on general requirements on internal governance, and that points 5.45.a and b should be amended accordingly.

Ad points 5.46.c and d:
For clarity reasons, we suggest that the wording in 5.46.c be modified to: "where internal control functions of the financial entity or tasks thereof are provided by TPSPs ..."; We also suggest that the given examples on outsourcing of control function tasks (i.e., that only intragroup and intra scheme outsourcing is mentioned) is rephrased since it is otherwise implied that extra group outsourcing of such tasks is not allowed. 5.46.d seems to be a repetition of para. 5.44 and could therefore be omitted.

Ad subpoint 5.47.f:
Under the subjective restriction of "appropriate timeframe", the requirements under point 5.47.f become unrealistic, while not taking into account the possibility of remedial measures in case of issues with the TPSP. We would

appreciate some clarification in the wording or replacement with a more general reference to appropriate business continuity management and exit strategy.

Ad para. 6.48:
We believe that an annual review should not be mandatory; regular reviews and (where necessary) event-related reviews would be sufficient. Also, we believe that the requirement on the management body for reviewing the policy on third-party risk management should be aligned with CRD6, where it is established that Member States shall ensure that the management body reviews the policies for the management of risks at least every two years.

Ad points 6.48.a and f.iv
Since the responsibilities of the management body are described in para. 5.38, under point 6.48.a, reference should be made to this point, instead of para. 5.43. Regarding point 6.48.f.iv, since some contracts are open ended and not renewable, we suggest inserting "where applicable" at the start of the sentence.

Ad point 6.49.b
Since the financial entities are responsible for ensuring compliance with all applicable legal and regulatory requirements when using third-party arrangements regardless of what is stated in a policy, we believe that point 49.b could be omitted.

Ad para. 6.50:
While recognizing that a common policy covering DORA and the EBA-GL on TPRM will usually be sensible, this should only be formulated as a recommendation within the guidelines. As such, we suggest modifying this point by inserting "where relevant" in para. 6.50.

Ad para. 6.51
It could be clarified what the policies of the financial entities are expected to cover. According to the proposed text, financial entities should ensure that the policy covers the identification of "the following potential effects" but the listed items under a. through d. aren't "effects". We propose that guideline replaces "following potential effects of …" with "potential impact on the following areas resulting from …".

Ad para. 7.54:
Taking into account financial entities, groups and IPSs' freedom of commercial making decision, the requirement to set condition at "arms lengths" questionably interferes with this. Furthermore, a corresponding requirement was also omitted from DORA (it was still included in the draft RTS on Article 28(2) DORA), and we therefore suggest removing this requirement.

Ad para. 8.55:
Business continuity management typically not only takes into account the importance of the function but also time-sensitivity in the matter, prioritising functions encompassing both of these characteristics. As such, we suggest that

the requirements set out in this point should therefore focus on processes that are both time-critical and important.

Ad para. 9.60
Paragraph 224 of the draft revised guidelines on internal governance states that all internal audit recommendations (i.e., including those regarding 3P) should be subject to a formal follow-up procedure. To avoid regulatory overlap, we believe para. 9.60 could be omitted.

Ad para. 10.1.63, Register of arrangements
Considering that subpoint c is only relevant in the case of centralised register management in accordance with para. 10.1.62, we ask that clarification be provided, taking into account individual institutions, for whom this would not be possible.

Subpoint g. requires 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 a position to negotiate with a supplier outside of the European Union to get a LEI and also an EU-ID does not exist.
We therefore suggest being less restrictive with this information and allow the company name – or at least a more general identifier like the company register number.

Due to their different structural levels and content, a merger of the two registers is not even possible, therefore raising unrealistic expectations under para. 10.1.63 due to the terms "merged" and "avoid any discrepancies between those two registers". We propose that the wording be modified to reflect this issue: "... the register shall be consistent to the extent possible and may be combined with relevant parts of the register of information under Article 28(3) DORA.".

Subpoint k. overlaps with point 10.1.64.h and we therefore suggest its removal, simplifying the guidelines and focussing on critical or important functions.

We believe more clarity is needed regarding paragraph 63 (f). Considering the mention in page 59 "Financial entities are encouraged to maintain their own classification rather than using those examples set out in the Annex, if more relevant or appropriate", it would be helpful to understand if the Annex must be applied to identify the functions or if it should complement the internal list of functions developed by each financial entity. Furthermore, the documentation requirements should differentiate much more between critical/important and non-critical/non-important to avoid burdening smaller financial entities with far-reaching administrative tasks.

Ad para. 10.1.64:
As part of the effort of simplification and reducing regulatory complexity, information or documentation that is already required elsewhere should not be maintained redundantly in the register, notably points b, d, e, f, g.

Ad para. 10.1.67:

Overall, under paragraphs 10.1.61-67, while welcoming the cost-benefit options that allow consistency with the DORA register, we suggest that the EBA publish an optional common data dictionary to allow firms to maintain one integrated dataset across ICT and non-ICT registers.

Finally, we would also appreciate having more clarity on the level of detail required in the reporting of the proposed Annex I to understand if it would need to be at the "function" level (level 1 category of Annex I) or at the "service" level (level 2 category of Annex I).

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

For clarification, we believe that Title IV should be renamed to "Third-party lifecycle"

Ad paragraphs 11.1.71 and 72:
Ad authorization/registration of TPSPs:
From a documentation perspective, we include in our contract's respective representations and warranties by the TPSPs, which apply for the whole duration of the contractual relationship (therefore also covering potential later changes).

Ad cooperation agreement between supervisory authorities as listed in points 72. b. and 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. Furthermore, without sufficient information from competent authorities on the agreements, financial entities would hardly be able to assess for themselves whether such bilateral agreements meet all the conditions set out. Since these are thus requirements that will not be fulfillable in all circumstances, we would appreciate, if they were either taken out or if at least it is clarified how financial entities may proceed without strict compliance with such requirements.

Ad para. 11.2.74:
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 section 11.3), we would appreciate a differentiation also at such stage to avoid disproportionate requirements.

Ad point 11.2.76.b

The second part of point 11.2.76.b. regarding groups and IPS seems too broad. Such analyses could only be carried out at a central (higher) level. The individual institutions belonging to the group or IPS will not have all the necessary information and can only take into account their own perspective, so we suggest removing the end of the subpoint.

Ad point 11.2.78.c.:
From a documentation perspective, respective representations and warranties are included in contracts and the TPSPs are required to comply with certain contractual clauses ensuring utmost compliance irrespective of the local laws and regulations applicable to the TPSPs. Enforceability is usually ensured by agreeing on respective applicable law and jurisdiction clauses, whereas arbitration is the preferred way of dispute resolution given the wide-spread applicability of respective enforcement treaties.

Ad point 11.3.81.c.:
The reference to geographic dependencies seems like an outlier in this context since the remaining sub-points of para. 81 stipulate "positive" requirements that can be checked whereas point 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 separating this sub-point and making it a separate point.

Ad points 11.3.81.e. and f and para. 11.3.83:
Again, from a documentation perspective, respective representations and warranties are included in contracts. With regard to para. 83 we also 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 be premeditated by too widely formulated requirements within the context of general third-party management rules. A revision against this background would be appreciated.

Ad para. 12.84:
Just for the sake of clarity, the documentation of respective contracts can be rather complex and thus while we absolutely agree that the documentation has to be in a written form, it may not be in "one" single agreement but in a conglomerate of several related agreements.

Ad para. 12.85
The requirement of DORA inspired key contractual provisions for all third-party agreements, regardless of criticality, in our view, not a proportionate approach and will introduce a great regulatory burden for financial entities and bring only questionable value. Such requirements should be limited to agreements relating to critical or important functions.

Ad point 12.85.j
The provision to reference the resolution authority's power should only be relevant for agreements with TPSP in third countries. The powers of the resolution authorities are not, regarding intra EU agreements, dependent on the contractual terms between a financial entity and a TPSP.

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 point 85.j seems to be doubled and further clarified in point 86.e and since the parallel requirement under DORA also is stated for critical functions only, we recommend deleting point 85.j.

Ad para. 12.86:
Point 86.a:
Since it is not possible to formulate meaningful quantitative targets for every type of service, the wording should be modified to "with precise quantitative and/or qualitative performance targets"
Point 86.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).
Point 86.e:
We estimate that point 86.e.i probably refers to section 12.2 instead of section 12.1. Also, it would be valuable if point 86.e.ii could be expanded so that the intended purpose is clarified.
Point 86.f:
As strategies are specific decisions made by the financial entity and are not part of the contract, the wording should be modified to "exit options".

Ad para. 12.1.88:
The article refers to subcontracting 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 bank's 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 para. 12.2.98:
This point seems to partly overlap with the resolution resilience requirements under the BRRD and related legislation. From a documentation perspective, we 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 paragraphs 12.2.103-105:
We welcome paras. 12.2.103 to 105 on pooled/joint audits and reliance on third-party certifications/reports. However, to reduce duplication, we propose clarifying:

i. Recognised standards (e.g., ISAE 3402, SOC 2 Type 2, ISO/IEC 27001)
ii. Safe-harbour conditions for reliance and
iii. Acceptance of multi-client/group reliance in the subcontracting chain.

Ad point 12.3.109.b:
The formulation seems too generic and will be difficult to agree with TPSPs – TPSPs are usually rather concerned when termination rights allowing for immediate termination are formulated too vaguely so that they could allow for a "disguised" termination for convenience. We therefore propose to at least change to "capable of materially negatively altering". Alternatively, point b, could be taken out since it seems anyway covered in point c.

Ad section 14:
This section should be supplemented by opening clauses or exceptions for service arrangements within group and IPS-related structures. In most cases, such arrangements are designed as permanent divisions of labour. Within groups and IPS-related financial associations, there are usually sufficient control and influence mechanisms in place so that the risk of a TPSP failure or unexpected termination of the arrangement is very low.
Developing and maintaining detailed exit strategies and plans for what are therefore largely theoretical events would entail redundant bureaucratic costs. Furthermore, the occurrence of such events does not necessarily mean withdrawal from the arrangement, even in the event of material non-performance as the problems can potentially be fixed by the TPSP.

Ad points 14.117.c and e:
In our understanding, risks as mentioned are not events or developments that are taken into account directly in the context of an exit strategy and we would therefore appreciate it if they were either taken out or if at least clarified.

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

Annex I is indeed useful as a reference tool, but its non-binding nature may lead to uncertainty. In this regard, we propose that the EBA defines a minimum mandatory taxonomy of functions and services, allowing financial institutions to expand it based on their business models. We believe this would support data collection and reduce interpretative discrepancies.

Nonetheless, we would appreciate having more clarity on the concepts of "level 1" and "level 2" categories. More specifically, it would be helpful to know if "level 1" would correspond to a "function" and "level 2" would correspond to a "service".

Regarding the list of activities included in Annex I, such as "Depositary tasks & administration for UCIs" and, in particular, those identified as "Depositary tasks for UCIs", it is important to emphasise that depositary activities are a regulated financial service provided by depositary entities in compliance with the obligations established in the regulations, for the ultimate benefit of the unit-holders. We understand that the inclusion of these activities in Annex is to contemplate, if applicable and within the limitations established for this purpose in the regulations, that depositary entities could rely on third-party providers to provide their services to UCIs.
Therefore, we recommend that the provision of depositary services to UCIs is removed and left outside the scope of the Guidelines especially as their Asset Management Companies would not be considered obligated subjects.

Furthermore, the examples should also be checked again for consistency with Section 3 of the TPRM Guidelines and DORA, to ensure that there is no overlap. For example, "postal services & Mailing" does not fall within the scope of the EBA Guidelines.

We would also like to point out that "Marketing" is mentioned twice.

Finally, we also believe that the TPRM should be added to the control functions (this may, at least partially, be transferred to a service provider).

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.

About ESBG (European Savings and Retail Banking Group)

ESBG represents the locally focused European banking sector, helping 32 savings and retail banks in 27 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. Advocating for a proportionate approach to banking rules, ESBG unites at EU level some 859 banks, which together employ 619,000 people driven to innovate at 37,000 branches. ESBG members have total assets of € 6,35 trillion, provide € 372 billion in loans to customers, and serve 163 million Europeans seeking retail banking services. ESBG members commit to further unleash the promise of sustainable and responsible 21st century banking. Learn more at www.wsbi-esbg.org.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. October 2025.