Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

# Comments

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

*Lobby Register No R001459*
*EU Transparency Register No 52646912360-95*

Contact:
Dr. Teo Geldner
Telephone: +49 30 1663-1757
E-Mail: teo.geldner@bdb.de

Berlin, 8 October 2025

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
https://die-dk.de
www.german-banking-industry.org

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

**General Comments**

The German Banking Industry Committee (Deutsche Kreditwirtschaft – DK) welcomes the objective of aligning the EBA Guidelines on Third-Party Risk Management with the existing DORA framework, as this would promote regulatory consistency, enhance legal clarity, and reduce implementation complexity for financial entities and supervisors alike. Consistency between the two regimes is essential to avoid duplication and fragmentation.

At the same time, these two frameworks create a distinction between ICT and non-ICT arrangements. This division is ultimately arbitrary and offers no value from a risk-management perspective – particularly given the broad alignment in regulatory expectations. In practice, this will create uncertainty for financial entities and will require them to assess and make subjective assessments to distinguish what is "predominantly" ICT. It would be helpful for the authorities to clarify that there is flexibility or overlap allowed in classification – this will enable financial entities to apply a consistent and risk-based approach to oversight, without needing to retrospectively reassess existing DORA-classified arrangements or justify their classifications to authorities.

Additionally, the draft Guidelines require significant revision to ensure a **more streamlined, principles-based, and risk-oriented approach**. Repetitive and overly granular requirements should be avoided, and a clearer proportionality framework is needed — particularly with regard to the materiality of third-party arrangements. Services with evidently low risk (e.g. marketing or staff training) should not trigger detailed risk assessments, due diligence requirements, or unrestricted supervisory access obligations. Applying the same regulatory burden to all arrangements, regardless of risk or function, may not operationally be feasible and may lead to disproportionate compliance costs.

This issue is further exacerbated by the Guidelines' shift away from the traditional outsourcing concept. The broad new definition of third-party arrangements (TPAs) significantly expands the scope to include a wide range of service relationships that were previously outside the regulatory perimeter. In practice, this means that financial institutions must apply the same level of control and documentation to non-critical, non-outsourcing arrangements — resulting in substantial additional administrative workload. Moreover, the interaction with existing regulatory provisions still based on the concept of outsourcing (e.g. Article 85(1) CRD, PSD) remains unclear and risks regulatory overlap.

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.

The same logic applies to contractual requirements. While we generally support alignment with Article 30 DORA, the Guidelines still retain elements from the 2019 Outsourcing Guidelines that are outdated or not appropriate for non-ICT services. For example, provisions on data processing locations, confidentiality, and audit rights should only apply where relevant, based

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

on the nature and risk of the service. Furthermore, the obligation to include extensive termination rights for all TPAs — regardless of criticality — goes beyond DORA and is likely to lead to difficult contractual negotiations, especially with smaller service providers.
A key area of concern is the proposed **register of third-party arrangements**, which — compared to the existing outsourcing framework — significantly increases the scope and depth of documentation obligations. Experience with the DORA information register has already shown the operational burden such detailed registers impose. Requiring the same level of documentation for all TPAs, including non-critical ones, will divert resources without offering clear risk management benefits.
We therefore recommend that:

- The Guidelines adopt a **risk-based, proportional register approach**, by ensuring flexibility in the application of data requirements to the broader population of third-party arrangements – i.e., certain data fields should not be necessary for lower risk arrangements, especially non-outsourcing arrangements;
- The register requirements be closely aligned with the DORA register, whilst allowing for optionality for data fields that are not applicable to all third-party arrangements – i.e., ensuring any data-related or ICT specific fields are optional where not applicable;
- Additional data fields beyond DORA register(e.g. service description, subcontractor location, data storage location for non-CIFs) should be avoided;
- The objective should be for a **streamlined register** be established for both ICT and non-ICT arrangements, rather than requiring parallel and overlapping systems.

To ensure the operational burden remains manageable, the Guidelines should clarify which services are clearly out of scope. Whilst we note the exclusions at paragraph 32.f. and the EBA's clarification at the recent public hearing that the prudential focus of the framework is on arrangements that meet that threshold, the reference to "risk exposures" may be too broad. If the EBA's intention is to set a fairly high bar for excluding services that are not material from a prudential risk management perspective this should be clarified in the language and through the recitals. For example, services that have a material impact to a firm's operational resilience would seem to reflect the prudential objectives.
Finally, to ensure the Guidelines achieve their objective of harmonization, NCAs should implement and supervise the Guidelines consistently and avoid national gold-plating or additional supervisory expectations (as seen with the 2019 Guidelines). This will be particularly important given the broader scope and such consistency would also be in line with the EU's broader objective of regulatory simplification and burden reduction.
Overall, we encourage the EBA to revise the draft Guidelines with greater focus on risk materiality, practical feasibility, and alignment with existing EU regulatory instruments — especially DORA.

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

**Comments on Questions:**

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

**General comments on Question 1:**

We generally welcome the aim of avoiding double regulation by applying DORA to ICT services and these Guidelines to non-ICT third-party arrangements. The proposed two-year transitional period seems very ambitious. Due to the burden of parallel regulatory changes, we would appreciate an extension of one year to allow for appropriate implementation. Furthermore, the implementation provisions in paras. 17–20 remain insufficient. In particular, the initial application date should not coincide with publication but be set at least six months after the availability of official translations, to give institutions sufficient time to adapt strategies, internal policies, and IT solutions (e.g. for the third-party register).

We further recommend that, in order to avoid overlapping regulation regarding ICT-services, the EBA Guidelines on Outsourcing of 25 February 2019 should already repeal those provisions which, due to the applicability of DORA, would otherwise result in duplication of work for financial entities. This is particularly the case where an arrangement qualifies as outsourcing and simultaneously involves an ICT service. Examples include: outsourcing register vs. information register, the obligation to conduct risk analyses and notification requirements under both regimes, as well as unaligned minimum contractual provisions.

**Specific comments on Question 1:**

**Para. 16: Definitions**

Third-party arrangements: The definition of a third-party arrangement should consider the aspect of a recurring or an ongoing basis for the services provided (according to the definition of an outsourcing arrangement). Please also refer to paras. 30 – 32 for further explanation.

In general, we strongly recommend the EBA aligns to consistent terminology with respect to DORA.

**Para.17**

We kindly recommend that financial entities be granted greater flexibility during the transitional period in determining when to address specific implementation aspects. In our view, a review and, where necessary, adjustment should only be required in the event of material contractual changes. Outsourcing arrangements are already monitored and governed under the EBA Guidelines on Outsourcing of 25 February 2019. Imposing significant additional effort for review and adjustment in the absence of material contractual changes would not be proportionate.

**Para. 19**

Due to the tight schedule of regulatory changes (especially the introduction of DORA), a longer transition period should be granted. Furthermore, non-ICT services which do not constitute outsourcing are generally associated with low risks. Otherwise, at least a risk-based approach should be applied (step-by-step concept). We therefore recommend extending the

implementation period by at least one year or applying a phased approach (e.g. non-ICT arrangements classified as critical within two years, non-critical within three years if necessary).

**Para. 20**

The transitional period should be extended by at least one year (to three years), taking into account typical contract durations or renewal cycles. In many cases, contracts are open-ended and not subject to explicit renewal, which makes strict cut-off dates impractical. Many firms are already substantially compliant and should not be expected to reopen and renegotiate contracts solely to align wording with the updated Guidelines. Therefore, institutions should be granted sufficient flexibility within the transitional period to implement the requirements in a risk-based and proportionate manner. Furthermore, in the event of harmonization of the registers, significant technical adjustments will be necessary.

**Title I: Proportionality: group application and institutional protection schemes**

**Para. 26**

We consider that the current wording "TPSPs within the group or the institutional protection scheme" does not fully reflect the range of typical constellations in this context. On the one hand, third-party service providers often include entities other than institutions that are directly part of the group or the IPS. On the other hand, indirect ownership structures or other forms of influence and control may also exist. For the sake of clarity, we therefore recommend that the following wording be used:
*"TPSPs within group- or institutional protection scheme (IPS)-related structures."*
Otherwise, certain intra-group service providers might not be able to benefit from this relief.

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

**Title II: Assessment of third-party arrangements**
**Question 2: Is Title II appropriate and sufficiently clear?**

**General comments on Title II:**
We recommend that, beyond the exceptions already defined, a more risk-based approach be incorporated into the EBA Guidelines. According to the current draft, the scope of application is significantly expanded to cover non-ICT third-party arrangements that were previously outside the outsourcing framework. Up to now, only services directly related to banking activities or other bank-specific functions were included. The planned expansion entails a substantial implementation burden for institutions. We do not consider this to be efficient and therefore advocate for a more risk-based approach, underpinned by sound internal risk management, together with appropriate documentation and oversight.
In the interest of the intended harmonization, the assessment of whether a function is critical or important should therefore be carried out in alignment with Article 3(22) DORA. This relates in particular to the impact on the financial performance of a financial entity, the soundness or continuity of its business operations, and the ongoing compliance with licensing conditions and obligations. In our view, the DORA definition is fully sufficient for assessing critical and important functions and should therefore also apply in the new EBA Guidelines, especially in light of the supervisory objective of harmonizing the two frameworks.

To avoid double regulation and in the interest of an effective and proportionate financial regulation regime within the European Union, we strongly urge the EBA to generally exempt regulated financial and ancillary services, or related services by financial entities that are themselves within the scope of these Guidelines. The relevant entities are already subject to stringent resilience and risk management requirements and applying the Guidelines to such arrangements would create a significant additional operational burden, without delivering meaningful risk reduction. This would be in line with the 2023 Final Report of the Financial Stability Board, as well as with the exemption granted under DORA by ESAs Q&A 2999 – DORA030.
A general exemption for these functions - similar to the one in para. 32(g) - would be the most effective in our view.

**Specific comments on Title II:**
**Section 3**: **Sound management of third-party risks**
We recommend that Section 3 be renamed for the sake of clarity to, for example, "Identification of (non-ICT) third-party arrangements."

**Para. 30**
We kindly recommend that a proportionality mechanism be introduced to exclude short-term and low-materiality contracts from the scope of third-party risk management requirements. The decisive point is that materiality is properly safeguarded so that requirements apply only where risks are significant to ensure that institutions can focus their resources on genuinely risk-relevant and long-term arrangements.

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

In addition, we recommend that the list of examples in the Guidelines be reviewed carefully to avoid overlaps with ICT-related services already covered by DORA. For instance, references to personal computers should be removed.

**Para. 31**
We kindly note that the reference to assessing *all aspects of the arrangement* may be more appropriately placed in the context of risk assessments. Irrespective of this, we assume that all other requirements, in cases involving multiple services, will only apply to those services that fall within the scope of the Guidelines.
We welcome **Footnote 42**, as it can help to avoid double regulation. However, we recommend that its content be integrated directly into the main text. In addition, we would appreciate clarifications to ensure that proportional relief can apply in multiple relevant directions, namely:

- Where an ICT service is only marginally or insignificantly supplemented or supported by other services, treatment under DORA alone should be sufficient.
- Where a non-ICT service is only marginally or insignificantly supplemented by an ICT service, treatment under the EBA-Guidelines alone should be sufficient.

**Para. 32**
To ensure efficiency, we propose clarifying that this assessment may be performed at service category level rather than individually for each arrangement, by making use of existing risk assessments.
We recommend that the illustrative list under para. 32 be changed:
(c) we kindly request clarification that the exemption applies both to payment services and to securities settlement services.
(f) Suggested footnote for para. 32(f):

- *The assessment does not need to be carried out for each arrangement individually, but may be performed at process or service category level, referring to existing risk assessments for related processes or similar services.*

We also note that the examples remain unchanged, except utilities, which now rely on a new exclusion rationale in para. 32 (g) ("subject to a regulated framework").
Furthermore, the non-exhaustive list should include the following services:

- Canteen as well as document destruction services.
- Consulting services and mandates
- Temporary staffing services and temporary staff
- Staff training
- HR-related services
- Administrative services
- Regulated financial services provided by another regulated financial entity and ancillary services (e.g. custody services, insurance services, depository tasks)
- Legal services in general

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

(g) We recommend that the wording be adjusted to include telephone services (rather than "telephone lines").

**Section 4: Critical or important functions**
We consider the formulations in Section 4 to be overly broad, particularly when compared with the definition of "critical or important functions" in Article 3(22) DORA. Paragraphs 33 to 37 leave significant room for interpretation and could ultimately result in financial institutions classifying almost all TPSP arrangements as "critical or important," given that some connection to a supervised activity or potential risk can almost always be identified.
In line with DORA, however, the focus should only be on those services where a failure or deficiency would significantly impair the financial institution, or lead to non-compliance with licensing conditions and obligations.

**Para. 34**
For the sake of clarity, we recommend the following rewording:
"*When relying on a TPSP for operating an internal control function of the financial entity or tasks thereof, …*"

**Para. 35**
The reference to section 12.1 appears to be incorrect and needs to be corrected or clarified.

**Para. 37**
In para. 37(b), the criteria for determining whether a function should be classified as critical or important under the new EBA-Guidelines are supplemented and expanded compared to DORA. The draft Guidelines additionally refer to market and credit risks, which in our view goes too far Such an expansion would effectively introduce a new system that applies only to third-party arrangements falling under the EBA-Guidelines, but not to those under DORA.
Furthermore, the provisions in para. 37(b)(ii), (iii) and (iiii) would mean that any non-ICT service which, in the event of failure, could have an impact on operational, legal, reputational or other relevant risks would automatically be deemed critical or important. This contradicts the principle of proportionality and a risk-based approach. A narrow interpretation would significantly broaden the scope, since almost every failure of a third-party provider could, in some way, affect such risks – even if only to a minimal extent. At a minimum, it should therefore be clarified that only relevant, i.e. material impacts are to be considered.
In addition, the introductory wording does not fully align with the subsequent content. The enumerations could be misinterpreted as implying that any direct link to supervised activities and/or any risk would already trigger classification as "critical or important." This would also contradict the principle of proportionality. A clarification that the assessment should focus exclusively on material risks and damage potential is therefore essential.

**Para. 37(b)(v):** We note that this provision refers to AML/CFT risks, although these are explicitly excluded from the scope of the Guidelines (see Rationale 11). We recommend clarifying that a regular assessment of risks by the financial institution itself – rather than by the management body, as currently foreseen – should be sufficient.

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

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

**General comments on Title III**
We consider the requirement to maintain all contracts with extensive information in a register to be overly broad and highly time-consuming. Experience with the DORA information register has already demonstrated these challenges.

We would consider it more effective to establish a streamlined register that is closely aligned with critical or important functions (both ICT and non-ICT), rather than collecting extensive data on all third parties. This could be designed as follows:

- A common reporting format to supervisory authorities to avoid media disruptions.
- A shared platform for risk classification of service providers (e.g. based on harmonised risk scores or traffic-light assessments).
- A common mapping of all subcontracting chains with a clear link to the main service and the responsible main service provider, irrespective of ICT or non-ICT classification, given the many hybrid forms.

**Specific comments on Title III:**
**Para. 38**
The wording appears to conflate two different documents – the strategy and the policy – which may be maintained under different responsibilities. We suggest the following rewording:
*"Such strategy should ~~include~~ refer to the policy on the sound management of third-party risks …"*
Looking at para. 50, we understand that financial institutions should have the discretion to decide whether to establish an integrated or separate strategy for ICT and non-ICT services.

**Para. 40**
The reference to para. 30 is unclear. Detailed individual risk assessments in accordance with Section 11.2 – also for arrangements or services that are not even covered by the Guidelines – would be wholly disproportionate. We kindly recommend clarifying that only arrangements not covered under Section 3 should be included in the financial institution's operational risk management on a general basis.

**Para. 41**
We consider para. 41 to be redundant. The GDPR already applies in any case, and this is reiterated under para. 47(g).

**Para. 43**
This paragraph contains general requirements that are already addressed under CRD and the EBA Guidelines on internal governance, but may create uncertainty if repeated here. For example, it is unrealistic to expect the management body of a financial institution to oversee

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

all (potential) conflicts of interest at TPSPs. We therefore recommend limiting this provision to the key points only.
In this context, we kindly suggest inserting a cross-reference to para. 45, which already requires the establishment of an appropriate role for this purpose.

**Para. 46**
We recommend clarifying the wording in point (c) as follows:
"*where internal control functions of the financial entity or tasks thereof are provided by TPSPs …"*
In addition, point (d) duplicates para. 44 and could therefore be deleted.

**Para. 48**
For the policy (unlike the strategy under para. 38), it should not be mandatory that the management body be directly responsible. A yearly review should also not be required; rather, reviews should take place regularly and on material occasions.

**Para. 49**
We would like to point out the following:

- Under (a), the cross-reference should be to para. 38 (instead of 43).
- Under (d), a footnote like Nr. 51 should be added: "*This role and the reporting-line can be combined with the one in charge of monitoring the arrangements concluded with ICT third-party service providers on the use of ICT services under Article 5(3) of DORA.*"
- Under (f)(iv), we kindly recommend inserting **"where applicable."**
- Point (h) should be replaced by a reference to Section 14.

**Para. 50**
We consider that institutions should have flexibility to decide whether the policy referred to here covers only the services within the scope of the draft EBA-Guidelines, or also ICT services subject to DORA. We therefore recommend deleting this provision and instead inserting, for example, a footnote noting that the policy may be combined with the policy required under DORA, provided that it differentiates accordingly.

If point (a) remains, we recommend the wording "where relevant": „The policy on third-party risk management should differentiate*, where relevant, between* the following."

**Para. 54**
We recommend deleting this provision. A similar requirement was originally proposed in a delegated act under DORA but was not retained in the final text. At that time, the DK commented as follows:
"*There should be no additional requirements for TPSPs that are part of a group or a member of an institutional protection scheme owned by the financial entity. A mandatory requirement to set intra-group conditions at arm's length within a regulation is legally questionable, as this would interfere with entrepreneurial freedom of decision. The term is also unclear and*

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

*compliance with this provision would be verifiable only to a limited extent. Verification can always be very complex and time-consuming, e.g. assessment of fair market price."*

**Para. 58**
The draft introduces an explicit requirement that business continuity plans (BCPs) related to third-party arrangements must align with the EBA Guidelines on internal governance. We recommend deleting this addition, as it deviates from the contractual expectations under DORA and undermines the objective of alignment.

**Section 10 – Documentation requirements**
**Para. 61**
The draft requires institutions to retain documentation of terminated third-party arrangements in the register and to keep supporting documentation for "an appropriate period of at least five years." This obligation goes **beyond the requirements of the DORA information register** and should not be reintroduced in the EBA Guidelines.
We kindly recommend deleting this provision. The five-year retention requirement was **deliberately removed from DORA** during the legislative process, including from the ITS on the information register. Reintroducing it here would therefore be inconsistent with DORA and constitute **gold-plating**. Instead, FAQ 52 on DORA should be applied: "In accordance with the final text of the ITS as published in the EU Official Journal, there is no requirement to include into the register terminated or expired contracts. "

**Para. 62**
We generally welcome the possibility of maintaining central registers for institutions belonging to the same group or institutional protection scheme. However, as long as DORA does not provide for such a possibility, this option does not represent a genuine relief for documentation purposes (see also para. 63).
Furthermore, para. 27(d) requires that an institution-specific register must be capable of being generated at short notice. This implies that the documentation must be maintained in such a way that the central unit, with the involvement of the institution, can update and reflect the institution's individual contracts at entity level. A real simplification could arise if reporting obligations could be fulfilled centrally (see also paras. 65 and 67). An example would be the central notification of planned arrangements with a group provider that support critical or important functions.

**Para. 63**
The draft Guidelines address the interaction between the EBA register and the DORA information register. While we welcome the approach not to apply DORA requirements one-to-one to all TPSP arrangements, the current wording raises a number of concerns.

**Concerns:**

- A complete merger of the two registers would not be feasible due to different structures and contents. The wording *"merged"* and *"avoid any discrepancies between those two registers"* creates unrealistic expectations.

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

- Clarity of contents: The draft partially requires more extensive information than DORA, including, for example:
    - Description of the service
    - Address/contact details of the service provider
    - Country of the subcontractor
- Overreach compared to DORA: Data which DORA requires only for critical functions (e.g. country of service provision, data storage/processing location) is here requested also for non-critical functions.
- Deviation from DORA categorisation (f): Under DORA, functions are mapped according to the institution's own categorisation of licensed activities (Annex I of Directive 2013/36/EU and Annex I Sections A and B of Directive 2014/65/EU). The draft introduces a different approach, which would undermine consistency.
- Unclear integration: Annex I of the Guidelines (*List of Functions*) deviates from the DORA information register model (two layers vs. one layer). This makes it unclear how the outsourcing register is expected to be aligned with the information register.

**Recommendations:**

- Replace the current wording with:

"*… 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.*"

- Present register contents in a separate paragraph for better clarity.
- No extra register requirements compared to DORA – ensuring identical structure, format, and attributes.
- No register requirements that are only relevant to ICT services and maintaining proportionality.
- Certain data fields should not be necessary for lower risk arrangements, especially non-outsourcing arrangements.
- Clarify that point (c) only applies to centralised register management; individual institutions cannot report data on other group members.
- In many places in the EBA-GL, the term 'functions provided by TPSPs' is used instead of the DORA term 'ICT services supporting a (critical or important) function' (for example in Para. 63 e and i). In some places, it therefore remains unclear whether, as with DORA, the initial focus is on assessing the support provided by the institution's processes (materiality assessment) or whether it is an assessment of the processes or services provided by the ICT service provider itself in the sense of an upstream risk analysis. We suggest harmonising the terminology.
- Delete point (k), as it is redundant to para. 64 (h).

In the event that institutions decide to merge their registers to the extent possible, the EBA should clarify that a merged register meets the requirements of DORA and the EBA-GL and that no separate registers need to be created.

**Para. 64**

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

Information that is already documented and maintained elsewhere should not have to be redundantly included in the register. This applies in particular to point (b) (dates of the most recent audits) as well as information related to BCM and exit strategies (points (d)–(g)).
In addition, the reference in point (g) to para. 63(g) is unclear and should be specified.
Moreover, the requirements for information to be stored in the register go beyond those in DORA – for example, by mandating the inclusion of the date of the most recent assessment of substitutability and reintegration.

Furthermore, it remains unclear whether 'function' refers to the (outsourced) function or service or to the function or (technical) process of the institution supported by the (outsourced) service. Reintegration (Para. 64 point (e)) can really only refer to the non-ICT service outsourced to third parties and not to the (specialist) function/process supported by the service, as only the non-ICT service itself can be 'reintegrated'. However, if 'function' refers to the actual service, then it is unclear which Recovery Time Objective (RTO) and Recovery Point Objective (RPO) should be calculated here, as these are not calculated for the service itself but for the entire process (within the framework of a BIA). It should therefore be clarified that the RPO and RTO refer to the supported process and not to the service purchased from the non-ICT service provider.

**Para. 65**
As noted under para. 63, the requirements should be consistent with DORA, where adequate and appropriate. In particular, the reference to a *"commonly used database format, comma separated values"* should directly follow from DORA. DORA itself provides for such options in the legislative text.

**Para. 67**
The obligation to submit the full set of extensive register information for planned services supporting critical or important functions is highly burdensome. For groups or institutions belonging to a institutional protection scheme, centralised submission by a central unit should in any case be permitted.
With a view to reducing unnecessary administrative burden, we kindly recommend deleting this provision altogether.

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

**Title IV: Third-party arrangement process**
**Question 4: Is Title IV of the Guidelines appropriate and sufficiently clear?**

**General comments on Title IV**
We consider that the title of Section IV would be more appropriately labelled "Third-party lifecycle."

**Specific comments on Title IV**
**Para. 71**
We kindly request the deletion of "investment services" from this section. The provisions of Section 2 of Delegated Regulation 2027/565 on outsourcing should be sufficient. This is an already highly regulated area of finance. In fact, we highly recommend excluding regulated financial services from the applicability of these Guidelines, as set out above.

We also point out, that the structure of the sentence in this clause should be revised, as the words "to a TPSP located in the same or another Member State takes place" appear to lack context.

**Para. 72**
We ask for moving the conditions for cooperation agreements under point (c) to Title V of the Guidelines. In addition, competent authorities should be required to provide adequate information on the agreements they themselves have concluded. Financial institutions are generally not in a position to assess whether all of the specified conditions are met. Further, as set out under Para. 71, we object to the inclusion of "investment services" in this regime.

**Paras. 74 and 75**
In the interest of proportionality, certain requirements should apply only to arrangements involving critical or important functions.
In para. 74, significant changes have been introduced that deviate from the DORA requirements. These include aspects such as data protection, the possibility of scale-ups, the impact on audits and the bank's control system, and an expanded assessment of replaceability, taking into account costs, time factors and reintegration. Alignment should be considered here to ensure equal treatment.

Furthermore, contractual aspects are dealt with in both Chapter 11.2 and Chapter 12, which leads to repetition (e.g. Para 74.e). Consolidating these passages would be desirable for the sake of clarity and comprehensibility.

**Para. 76**
We acknowledge the importance of identifying concentration risk at entity level as referenced in point (a), we note that third-party arrangements are often contracted at group level. As such, in certain contexts, entity level concentration risk assessments may not materially improve risk outcomes given those entities may have a limited ability to alter group-level

arrangements. We propose a proportionate approach that allows entities to rely on group-level assessments where appropriate.

The second part of point (b), concerning groups and institutional protection schemes, is too far-reaching. Such analyses can only be carried out at a central (group-wide) level. Individual institutions will not have access to all relevant information and can only provide their own perspective.
Moreover, a detailed weighing of mitigated risks against newly arising or intensified risks for every single third-party arrangement is not practicable, given the volume of such arrangements per institution. At most, such an exercise could be provided only for critical or important third-party arrangements within the meaning of paras. 34 and 35.

**Para. 78**
The requirements should, where appropriate, apply only to critical or important functions.

**Para 80a**
Instead of 'financial soundness' the term 'financial situation' should be used in line with DORA.

**Section 11.3 – Due diligence**
**Para. 81(f)**
The scope of criteria for assessing a third-party provider is disproportionately broad, particularly when relying on a critical or important function (e.g. regarding supply chain risks). This would lead to unmanageable additional workload. We therefore recommend reducing these requirements to a more appropriate level.

**Para. 83**
To avoid trickle-down effects, it should be clarified at least that the requirements are primarily directed at financial entities that fall within the scope of the CSDDD.
The extent of the due diligence obligations is disproportionate. The effort required to obtain the necessary information is not commensurate with the benefits of the provision. We therefore recommend deleting this requirement, or at least reducing it to a more appropriate level.

**Para. 84**
We kindly request textual harmonisation between DORA and these Guidelines with regard to the requirement for all contracts:
(DORA: *"be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format."*)
It should be clarified that this does not refer to the use of a document (in figures = 1), but rather to the written form of the contract as such, regardless of whether the overall contract may consist of various contractual components and annexes.

**Para. 85**

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

- The insufficient distinction between services supporting important functions and other services would result in a large number of contracts having to be amended, creating significant additional burden for institutions.
- Until now, minimum contractual clauses were only required for critical or important functions. The new Guidelines extend these minimum clauses to all outsourcing arrangements. This is not proportionate, creates significant implementation effort for financial institutions, and risks further concentration on a small number of large providers.
- We therefore recommend reversing this expansion; at least, the contractual requirements for non-critical or non-important non-ICT services should only be relevant if these services are necessary to support banking processes and they should apply only to new agreements. Existing contracts should be gradually converted as part of renegotiations, even if this would extend beyond the planned two years (principle of proportionality).
- In addition, the requirement to include a choice-of-law clause in all contracts – even where both parties are domiciled domestically – is unnecessary.
- It will be extremely difficult to renegotiate contracts with all TPSPs to include such clauses. Most TPSPs are not subject to prudential regulation and are not familiar with these requirements. DORA already demonstrated the challenges of negotiating minimum contractual content with ICT providers. Under the new Guidelines, the number of TPSPs covered could be far higher than under DORA, resulting in a multiple increase in workload, while many relevant TPSPs will have no reference to or awareness of these Guidelines.
- Under (d), (e) and (f): These contents are not required under DORA. These discrepancies risk undermining the objective of harmonized regulation across the EU and may result in unnecessary complexity and compliance burdens. In light of this, we respectfully request to remove the respective requirements.
- Under (j): DORA does not contain a corresponding provision for non-C/I services; For C/I services see para. 86 e). For C/I services it foresees reporting and monitoring obligations acc. to Art. 30 (3) lit. e). This would mean that the EBA requirements are stricter than those under the DORA regime in terms of monitoring obligations, in the sense that DORA does not foresee any obligation to monitor non-critical or non-important functions. This higher requirement for non-ICT services should be removed.
- Under (l): there is a wrong reference to Section 12.4, which does not exist. It should rather be 12.3.
- Under (m), the wording should be amended to include "where relevant."

**Para. 86**

- Under (a): It is not feasible to formulate meaningful quantitative targets for every type of service. We therefore recommend amending the wording to: "quantitative and/or qualitative performance targets."
- Under (c): These requirements are not required under DORA. These discrepancies risk undermining the objective of harmonized regulation across the EU and may result in

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

unnecessary complexity and compliance burdens. In light of this, we respectfully request to remove the respective requirements.
- Under (e)(i): We assume that this refers to Section 12.2.
- Under (f): The wording should be amended to "exit options". Strategies are internal determinations of the financial institution, not a contractual element.

**Para. 90(a)**
In contrast to DORA, the EBA-Guidelines require the written agreement to specify *"any types of activities that are excluded from subcontracting"*, while DORA (Art. 4(1) RTS Subcontracting) requires a provision defining which ICT services supporting critical or important functions, or material parts thereof, are **eligible** for subcontracting. This represents a different approach – exclusion of activities vs. inclusion of eligible services – and could result in broader subcontracting under the EBA-Guidelines than under DORA.
We kindly request clarification whether this deviation is intended. Alignment with DORA should be ensured.

**Para. 93**
A mandatory requirement for explicit approvals by the financial entity is not practicable, particularly for large multi-client service providers. Where conditions for subcontracting are clearly defined in advance and the financial institution raises no objections, silence should be deemed implicit consent.

**Para. 96**
- **Second bullet:** The wording is largely consistent with DORA, but it is unclear why the phrase *"or material parts thereof"* has been omitted. We kindly request clarification on whether this omission is intentional.
- **Third bullet:** The same concern applies. The omission of *"or material parts thereof"* should be explained.

In both cases, we recommend ensuring full alignment with DORA.

**Para. 104**
The extended requirements for financial institutions in connection with the use of *pool audits* create additional workload that reduces their usefulness. It should be permissible for organisation, execution, and reporting to be carried out by a central body.

**Para. 109**
- **Point a:** DORA requires a *"significant"* breach of laws, regulations or contractual terms, whereas the EBA Guidelines refer to *any* breach. We kindly request alignment with DORA.
- **Point c:** This provision should only apply to critical TPAs. Currently, para. 109(c) requires all TPSPs to report material changes. Material changes can only occur in the case of critical services. This is evident from the CIF inheritance logic in DORA and should be harmonized here.

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

Based on the reference in paragraph 85 l), para. 109 c) would also apply to noncritical TPAs.

- **Point d:** DORA requires *"evidenced"* weaknesses, while the EBA Guidelines only require *"weaknesses"*. This raises practical questions for contract negotiations, in particular who decides whether a weakness exists. We would appreciate further clarity and illustrative examples.
  Additionally, the EBA Guidelines refer only to "confidential, personal or otherwise sensitive data or information." In contrast, DORA refers to *"confidentiality of data, whether personal, otherwise sensitive, or non-personal."* Could the EBA clarify whether the same data categories are covered?
- **Point e:** The EBA Guidelines require a termination right triggered by an *"instruction of the competent authority."* This clarification is useful, given the discussions under DORA regarding when an authority may be unable to effectively supervise. However, the different wording compared to DORA risks divergent applications between the two frameworks. We kindly request clarification whether this deviation is intended.

Overall, harmonisation with DORA is recommended to ensure legal certainty and avoid divergent application.

**Para. 110**
As this point refers to exit strategies – which apply only to critical or important functions – it should also be clarified that this section is limited to critical or important functions.

**Section 14 Exit Strategies:**
We recommend including explicit derogations or exemptions for service agreements within group- and IPS-related structures. Such agreements are typically designed as permanent arrangements. Within groups and institutional protection schemes, sufficient control and influence mechanisms usually exist, such that the risk of provider failure or unexpected termination is very low.
Developing detailed exit strategies and plans for largely theoretical scenarios would create unnecessary administrative burden. Potential negative events (e.g. operational disruptions) and countermeasures are already addressed within BCM and risk assessments. The occurrence of such events does not necessarily imply the need to exit the arrangement. Even in cases of material underperformance, institutions generally retain influence over the TPSP. Depending on the nature of the arrangement, it may therefore be sufficient to focus on practical and reasonable response options.

**Para. 117**
Points (c) and (e) should be clarified or deleted. In our view, risks as such are not events or developments that should be directly addressed within an exit strategy.

**Para. 118**

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

It should be made clear at the very beginning of this paragraph that the requirements apply only to TPSPs supporting critical or important functions. Currently, this limitation appears only under subpoint (b) of para. 118; it should be brought upfront.

## Comments Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

**Annex I: Non exhaustive list of functions that could be provided by a third-party service provider**
**Question 5: Is Annex I, provided as a list of non-exhaustive examples, appropriate and sufficiently clear?**

**General comments on Annex I**
We are concerned that the list in Annex I, presented as a positive list of examples across a wide range of service categories, is overly extensive. If all of these examples were to be treated as TPSP arrangements within the meaning of these Guidelines, the resulting documentation, risk assessment and contractual requirements would be unmanageable in practice. This can be illustrated by the Level 2 categories of administrative services (e.g. marketing, document management, insurance, payroll, pension and social benefits, postal services, procurement, secretarial services, recruitment, travel and entertainment). It would not be proportionate to require risk analyses, register entries and monitoring for arrangements such as secretarial services or travel services.

In addition, we note several inconsistencies:

- Certain examples (e.g. secretarial services, postal services & mailing, travel services) are listed under para. 32 point (f). They contradict the overall purpose of Annex I and should be removed.
- Insurance services are to be deleted. On the part of the insurer, these are financial services regulated under a separate regime. The use of insurance services by a financial entity is not a normal contractual relationship (due to a lack of instruction rights) and should actually not fall under these guidelines.
- Institutions should retain the flexibility to define their own categories of services, as foreseen in DORA.
- The current drafting could be misread as implying that AML services cannot be outsourced, which is misleading. The special treatment of AML compared to data protection and ICT risk control creates confusion.
- Depositaries under AIFMD/UCITS are statutory control bodies whose duties – safekeeping, cash-flow monitoring and oversight of investment limits – are not to be regarded as outsourcable services.
  Outsourcing always presupposes that the outsourcing entity is legally permitted to perform the function itself, which is not the case for depositary activities.
  To avoid regulatory inconsistencies and duplication, the Guidelines should therefore clarify that depositaries are not to be considered "third-party risk vendors" within the meaning of the Guidelines, and Annex I should be amended or supplemented accordingly.

**General Recommendation:** The Annex I list should be reviewed to ensure consistency with paras. 30-32 and alignment with DORA in order to avoid overlapping. Clarity should be provided that support services of a purely administrative nature fall outside scope, and institutions must retain the discretion to classify their own arrangements.