Brussels, 8 October 2025

MR/MM

EACB comments on
EBA draft Guidelines on the sound management of third-party risk
(regarding non-ICT risks)

General comments

The EACB welcomes the opportunity to comment on the EBA draft Guidelines on the sound management of third-party risk, with focus on non-ICT risks. We appreciate the initiative to foster harmonisation for the sound management of third-party risk and value the effort to build on existing regulatory products, such as the EBA Guidelines on internal governance, outsourcing, and ICT/ security risk management. This approach shall aim to avoid fragmentation and ensure consistency across supervisory expectations.

In particular, it is essential to ensure consistency between the DORA and the EBA Draft Guidelines on sound third-party risk management. Indeed, we commend that the Guidelines seek to align terminology and definitions with DORA and other relevant legislative acts. We support applying the classification of critical or important functions in line with DORA. Consistent with this approach, **the degree of dependency should be the determining factor** for distinguishing between "non-critical or important" non-ICT services and "critical or important" non-ICT services. Similarly, **requirements regarding the register and minimum contractual provisions should not diverge** concretely in substance or scope. We believe indeed that the final version of the Guidelines should ensure that identical circumstances are addressed by uniform terminology and definitions.

However, we see that the proposed classification of non-critical or important non-ICT services is not limited to banking-specific or institution-specific services. This raises the question of **whether banks would be required to apply comprehensive outsourcing management to all external procurements** and record them in the register. Such an interpretation would mean that **services previously assessed as non-ICT services under DORA would now also have to be included, thereby removing any intended regulatory relief**.

If a third-party arrangement does not qualify as outsourcing, it is difficult to see which prudential risks related to the core banking business the draft Guidelines would aim to address. **ICT-related risks are already comprehensively covered by DORA, outsourcing and in general critical or important functions are addressed under the EBA Guidelines.** The remaining contracts are typically ancillary in nature and should therefore fall outside the scope of the Guidelines, being left to institutions' contractual freedom — a fundamental legal principle that cannot be restricted without a clear legal basis. **Expanding the scope beyond these boundaries would impose disproportionate and unjustified burdens without achieving tangible supervisory benefits. It would indeed be useful if the EBA clarified whether the assessment of criticality would be meant to differ in any way from the methodology relevant for DORA and the Outsourcing GLs.**

The EACB shares the view that the EBA Guidelines on third-party risk management should not impose additional, disproportionate, or unnecessary operational burdens on institutions.

Implementation in the SREP exercise

As a follow-up to the EBA publication of the final text, we encourage competent authorities to provide clear and consistent guidance to ensure that the implementation of the new EBA Guidelines remains coherent with existing regulatory frameworks, proportionate in scope, and operationally feasible for institutions. It would be important to clarify how, for instance, the ECB intends to coordinate the rules applicable to non-ICT third

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail: secretariat@eacb.coop

parties under the Guidelines with the DORA regime for ICT providers, in order to avoid duplication of obligations – we encourage the EBA to include language in this direction. This is particularly relevant with regard to registers, reporting, and governance structures. The treatment of hybrid contracts, which combine ICT and non-ICT services, also requires clarification. Institutions need to know whether they will be required to apply the contractual clauses stemming from both frameworks cumulatively.

A second area of concern relates to **the register of third parties and the associated reporting obligations**. The new Guidelines appear to leave some flexibility as to whether non-ICT providers should be included in the register required under DORA. At the same time, the ECB has communicated its intention, in the medium term, to extend the information register to cover contractual agreements not currently subject to DORA, with a view to centralising all third-party dependencies. It would therefore be important that the ECB confirms whether it expects the establishment of a single consolidated register encompassing both ICT and non-ICT arrangements, and specifies the level of granularity, the frequency of updates, and the modalities of supervisory reporting.

Another key issue is the **feasibility of contractual requirements and audit rights**. Institutions need to understand to what extent they are expected to impose standardised contractual clauses – covering rights of access, audit, and cascading sub-outsourcing – on all providers, including non-financial firms and extra-European suppliers. Given the practical challenges of negotiating such provisions, it is essential to determine the degree of flexibility that will be allowed by the supervisor when strict implementation proves impossible.

Finally, **further guidance is needed on the transition period and the retrofitting of existing contracts**. The Guidelines foresee a two-year period, but clarification is required as to the starting date, and whether institutions will be permitted to implement a progressive remediation plan prioritising contracts based on criticality and feasibility of renegotiation. For complex or long-standing contracts, a phased approach may be necessary, and additional time may be justified once the relevant services have been identified and their criticality assessed.

Answers to selected questions

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

The consultation paper substantially broadens the scope compared to the previous guidelines. While in the past the focus was mainly on outsourcing contracts, the new guidelines now include all agreements with third parties, excluding those related to ICT services. This **extension entails a significant increase in both the complexity and the number of relationships to be monitored**, especially for small and non-complex banks, which until now have managed only a limited number of external relationships. It is therefore essential that the EBA defines clear and proportionate criteria, in order to avoid an excessive administrative burden and to ensure that efforts are focused on the relationships that are truly relevant.

Indeed, further work would be necessary to clearly distinguish what kind of agreements fall under these EBA Draft Guidelines. We think the Guidelines should **clarify how non-ICT services that meet the definition of a third-party agreement but do not constitute outsourcing agreements are treated**. Indeed, the provisions just regulated “third-party arrangement” and “critical and important function", ignoring the “outsourcing arrangement” terminology when assigning requirements. In fact, it remains unclear potential consequences and implication of classifying a non-ICT service in "outsourcing arrangement".

Furthermore, we ask for clarification that the requirements may be interpreted in line with the structures and responsibilities under national company law, in line with the governance guidelines (EBA/GL/2021/05). This would be critical given that management bodies may allocate and distribute competences in a different way, based on the monistic or dualistic system and national provisions. We also notice that the Guidelines address the various concepts of “management function”, “senior management” and “key function holder". In the

glossary, only the "management body" term is defined, we recommend to clearly establish the link with the definitions under CRD6 (and other EBA products) for the sake of clarity and legal certainty.

With the implementation of the Guidelines, **institutions should keep a register for information on all third-party arrangements, excluding any ICT-relevant third-party agreements**. The Guideline also introduces the **possibility to keep only one register to report information in accordance with these Guidelines and DORA. However, the two registers are not identical in terms of requirements**. This distinction is currently supported by established processes and would lead to legal ambiguities and uncertainties due to the new requirements of the draft Guidelines.

Moreover, it should be clarified that there's 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. Otherwise, certain intra-group service providers might not be able to benefit from this relief.

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 register. This ensures that administrative costs are reduced, and joint outsourcing arrangements are only recorded once. These adjustments would simplify organisational and administrative procedures. In addition, the default risk for intra-group service providers is minimal due to consolidation with their parent companies.

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."*

Finally, **the proposed two-year transitional period is highly appreciated. However, we consider a further extension of one year to be necessary**. In fact, many small banks have long-term contracts that require time to be amended and brought into compliance with the new guidelines, and a longer period would ensure a gradual and realistic implementation of the Guidelines. **During the transition period, financial institutions should be granted greater flexibility in determining when to address specific implementation aspects. Review and 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.

Regarding the provisions in Para. 17-20, 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).

Q2. Is Title II appropriate and sufficiently clear?

Several provisions of the draft Guidelines require clarification and refinement to ensure proportionality, consistency with the DORA, and avoidance of unnecessary administrative burden. In fact, the consultation paper substantially extends the scope of application from outsourcing contracts to all third-party arrangements (TPAs), including non-ICT services previously excluded from the outsourcing framework. While we acknowledge the objective of enhanced oversight, this expansion entails a significant implementation burden, particularly for small and non-complex institutions. We therefore strongly recommend embedding a risk-based approach, underpinned by sound internal risk management and adequate documentation, so that supervisory expectations focus on genuinely risk-relevant and long-term arrangements. **Short-term or low-materiality contracts should be expressly excluded from the requirements**

Critical or Important Functions

The draft Guidelines define "critical or important functions" (CIFs) in a manner that goes beyond Article 3(22) DORA. Chapter 4 introduces additional conditions that effectively broaden the scope by qualifying functions as critical or important, irrespective of the institution's own assessment. Para. 37(b) refers broadly to operational, legal, reputational and other risks, which could lead to classifying almost all TPAs as critical or important. This approach undermines the principle-based approach embedded in DORA, impacting the financial performance of an institution, the soundness and continuity of its business operations, and the ongoing compliance with licensing conditions and obligations. **It would be useful indeed to clarify whether the assessment of criticality is intended to differ in any way from the methodology relevant to DORA and the Outsourcing Guidelines.**

In addition, Para. 37(b)(v) introduces AML/CFT risks despite their exclusion from the Guidelines' scope (Rationale 11). This inconsistency should be corrected. Finally, Para. 35 contains a reference to section 12.1, which appears to be incorrect and requires clarification.

To ensure consistency and legal certainty, the determination of CIFs should be fully aligned with DORA. Institutions should not be required to maintain parallel systems of classification for different regulatory purposes.

Finally, with regard to recovery and resolution aspects, we believe it would be useful to also clarify the articulation between these GLs and the existing GLs on outsourcing, for the critical or important functions in relation to the recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation, as discussed in Para. 37.

Treatment of Non-ICT Services and Annex I

We believe that point f) on Para. 32 (t*he acquisition of services that do not have material impact on the financial entities' risks exposures or on their operational resilience (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators)* partly contradicts Annex I. Examples such as secretarial services and travel services illustrate the risk of overlap and regulatory uncertainty. Experience from the DORA consultation has shown that even illustrative examples may generate binding supervisory expectations. Accordingly, we recommend that the list in para. 32(f) be clearly framed as **non-exhaustive** and that regulated services in general (including utilities) be excluded.

In addition, **we propose clarifying the treatment of exemptions under paragraph 32**. The Guidelines should clarify whether the exemption applies equally to payment services and to securities settlement services. Furthermore, the rationale for excluding the service categories listed in paragraph 32(f) has shifted compared to the EBA Outsourcing Guidelines (2019). We are concerned about the removal of explicit references to market information services (e.g. data provided by Bloomberg, Moody's, Standard & Poor's, Fitch), as well as to goods (such as payment cards, card readers, office supplies, computers, furniture) and utilities (electricity, gas, water, telephone lines). Indeed, all regulated services should be excluded as a matter of principle, and the overall list should be expressly presented as non-exhaustive.

Previously, exclusions were defined on a functional basis ("would otherwise not be undertaken by the institution"), whereas now they are framed in risk-based terms ("no material impact on risk exposure or operational resilience"). This shift may lead to the **misunderstanding that an assessment is required for almost all service arrangements unless explicitly whitelisted.** To **avoid unnecessary bureaucracy, we suggest clarifying that such assessments can be carried out at the level of service category or process, rather than individually for each arrangement, by leveraging existing risk assessments.** This would allow institutions to

establish an entity-specific whitelist, effectively extending the EBA's general list. In this regard, we recommend that additional categories of immaterial services be explicitly recognised, including canteen services, document destruction, consulting mandates, temporary staffing, and administrative support. For consistency, the assessment of immaterial services should be permitted at the **service category level**, making use of existing risk assessments, rather than requiring case-by-case analysis. Additional categories such as canteen services, document destruction, consulting mandates, temporary staffing, and administrative support should be explicitly recognised as non-material.

Finally, we emphasise that the definition of financial institutions is already outlined in Article 2(2) in conjunction with Article 2(1) of DORA. To avoid double regulation and reduce administrative burden, regulated services provided by financial institutions should not be considered non-ICT services under the EBA Guidelines, but rather as financial services. Currently, only a subset is included in the whitelist, which creates the risk of potential inconsistencies.

Proportionality

Limitations still remain in the application of the principle of proportionality. In small and non-complex banks, many operational activities are outsourced to another entity within the group or to external providers. In such cases, it is essential to clarify which organisational safeguards must remain within the outsourcing bank.

Specifically, the EBA should clarify whether the management of control functions (compliance, risk management, internal audit) must mandatorily remain within the outsourcing bank; and whether such management may be entrusted to a member of the management body. If, instead, the management of these functions does not necessarily have to remain internal, it should be clarified which concrete measures are required to ensure effective supervision in line with the guidelines. In addition, it should be clearly stated whether a single professional might be responsible for overseeing all third-party contracts, encompassing both operational outsourcing related to the first line of defence, and the oversight of agreements concerning the second and third lines of defence (compliance, risk management, internal audit).

On IPS, we welcome the provision in paragraph 27, which allows for the centralisation of certain monitoring and supervisory activities. This is a key element for small and non-complex banks, which often rely on central structures for the management of relationships with external providers. Indeed, the EBA should clarify:

- which activities may effectively be carried out at central level (e.g. risk assessment, monitoring, audit);
- which controls and responsibilities must remain with individual banks;
- how to ensure a clear allocation of responsibilities to avoid overlaps and duplications.

In some jurisdictions, centralised monitoring and supervisory tasks are entrusted not to groups or IPS entities, but to dedicated companies that operate exclusively for the banks concerned, while not formally being part of the group or IPS. It would be useful if the guidelines could specify whether such entities may assume the role of centralised structures, under which conditions (for example, regarding independence, governance, and contractual arrangements), and how information flows and responsibilities should be defined to ensure regulatory compliance and operational continuity.

We welcome the content of Footnote 42, as it can help to avoid double regulation, and we recommend to include it 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.

Treatment under the EBA-Guidelines alone should also be sufficient in all constellations referred to in ESA Q&A 2999 – DORA030 concerning the provision of ICT services related to supervised activities/services by another financial institution. Finally, in case of multiple services, the text should clarify that the requirements of the Guidelines will only apply to those services that fall within its scope.

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

The draft Guidelines foresee a significant extension of the outsourcing register, aligning it with the ICT register required under DORA. This expansion entails the inclusion of a much wider range of data and contractual arrangements, including non-ICT services that were not previously subject to detailed registration. While we acknowledge the objective of harmonisation, this approach will considerably increase the administrative and operational burden, especially for small and non-complex institutions, and risks being disproportionate to the benefits.

Proportionality and Risk Analysis

The requirement for comprehensive risk analysis should apply only to services supporting critical or important functions. **For non-critical or non-ICT services, simplified, category-based assessments—analogous to the proportional approach under DORA—should be explicitly permitted.**

Some requirements included in the draft Guidelines, such as maintaining historic data on terminated contracts for up to five years or applying arm's-length conditions to intra-group arrangements, had originally been considered in the DORA legislative process but were deliberately omitted from the final text. **Reintroducing such obligations under the Guidelines would create legal uncertainty, additional complexity, and questionable enforceability. We therefore recommend deleting these provisions.**

Centralised Registers and Reporting

Centralised maintenance of registers at group or IPS level can bring efficiency gains, provided that institutions remain able to generate institution-specific registers at short notice. This presupposes close cooperation between the central unit and individual institutions and would be facilitated by centralised reporting mechanisms.

At the same time, reporting obligations should be limited to contracts supporting critical or important functions, as extending them further would impose unnecessary burdens. Reporting complete, comprehensive register information for planned services involving critical or important functions is already highly resource-intensive; adding non-material contracts would further complicate the process without clear benefit.

Alignment with DORA and Implementing Regulation

It should be clarified whether only non-ICT-relevant contracts will be listed in the outsourcing register in the future, or whether both ICT and non-ICT services must be included. The draft appears to suggest the continued coexistence of two registers—one for ICT services under DORA and one for third-party arrangement under the EBA Guidelines—while also requiring compatibility and alignment between them.

We agree with the EBA approach of having the two registers separate but compatible, and institutions should have the option to maintain them in an integrated format if this is operationally more efficient. The **introduction of new mandatory fields should be avoided**, as this would significantly increase costs without necessarily improving third-party risk management.

To ensure consistency, the requirements of the outsourcing register should be fully aligned with DORA and its Implementing Regulation (EU) 2024/2956 on the information register. This includes the use of harmonised structures, data models, formats, and submission channels. Any divergence in terminology or categorisation between the two frameworks risks creating confusion and duplication.

In particular, we support applying the same functional categorisation of activities as foreseen under DORA, rather than introducing new levels of classification that cannot easily be reconciled between ICT and non-ICT services. Furthermore, any requirements for formatting (e.g. "comma separated values") should follow DORA's approach and remain flexible, avoiding prescriptive and ineffective technical rules.

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

The requirement for a specific weighing of mitigated risks against newly arising or intensified risks for each third-party procurement is not practicable given the volume of such arrangements within institutions. At most, such an exercise could be envisaged for critical or important functions, as defined in Para. 34 and 35 of the Guidelines. Even then, clear guidance would be needed on the methodology: should risks merely be compared and documented, should a netting be performed, or should procurement be permitted only where the overall risk is lower? If the result is positive, should risk values then be integrated into the institution's broader risk assessment? Without clarification, institutions will face uncertainty in implementation.

It also remains unclear whether the queries listed in this section apply to all third-party services or only to those supporting critical or important functions. This ambiguity risks extending requirements far beyond proportionate levels.

Alignment with DORA

Textual harmonisation between DORA and the Guidelines is essential. For instance, DORA requires that contracts be documented in a written form accessible in a durable medium. Equivalent wording should be used here to avoid discrepancies. Similarly, requirements concerning subcontractors should be clarified. Paragraph 64 already obliges institutions to record subcontractors providing essential parts. Requiring all sub-services to be included risks conflicting obligations and excessive burdens.

The Guidelines should also ensure consistency with Regulation (EU) 2022/2554 and Delegated Regulation (EU) 2024/1173, particularly regarding reporting obligations. Clarification is needed on which reports are expected, and confirmation that reporting is not envisaged for every third-party purchase but rather for those supporting critical or important functions.

Business Impact Analyses and Exit Strategies

Exit strategies should be applied only to third-party arrangements that support critical or important functions. The draft requires separate BIAs for exit strategies, which would add significant administrative workload. As BIAs are already integral to business continuity management, their results could be used as a scalable basis for determining resources in exit planning. This would highlight the link between contingency measures and exit strategies, and avoid duplication. Furthermore, references to "objectives" and "success criteria" in this context are ambiguous and should be clarified with examples.

Exit Strategies and Group/IPS Considerations

Within groups and IPS structures, service agreements are typically permanent and accompanied by strong control mechanisms. Risks of failure or termination are therefore minimal. In such cases, it is sufficient to consider practical response options within existing Business continuity frameworks rather than developing detailed exit plans for hypothetical scenarios.

Requirements in Para. 117–119 should be clarified accordingly, with "risks" distinguished from "events," and success criteria illustrated by examples.

Proportionality in Specific Provisions

Several paragraphs introduce requirements that should, in the interest of proportionality, be limited to critical or important functions:

- Para. 74–75: The expanded requirements (data protection, scale-up potential, audit impacts, extended replaceability assessments) go beyond DORA. Alignment is recommended.
- Para. 76: Analyses should be conducted centrally at group level, as individual institutions lack access to all relevant information.
- Para. 78: Requirements should apply only where critical or important functions are involved.
- Para. 81(f): The criteria for assessing providers are overly broad, creating unmanageable workloads. Narrowing their scope is necessary.
- Para. 83: Due diligence obligations risk extending beyond financial resilience towards broader political objectives. **At minimum, they should be limited to entities within the scope of CSDDD**.
- Para. 85: Minimum contractual clauses should continue to apply only to critical or important functions. Extending them to all outsourcing arrangements would create disproportionate implementation costs and negotiation difficulties, especially with non-financial or extra-EU providers. For non-critical arrangements, requirements should apply only to new agreements, while existing contracts should be adjusted progressively during renegotiations.
- Para. 86: Quantitative targets are not always feasible; wording should be amended to permit "quantitative and/or qualitative" targets. Exit options should be distinguished from internal strategies.

Contractual and Subcontracting Provisions

The Guidelines diverge from DORA in several areas:

- Para. 90(a): DORA defines eligible subcontracting for ICT critical/important services, whereas the Guidelines focus on excluded activities. This approach should be harmonised.
- Para. 93: Requiring explicit approval for each subcontracting change is impracticable; pre-defined conditions with deemed consent should suffice.
- Para. 96: The omission of the phrase "or material parts thereof" compared to DORA should be clarified.
- Para. 100: Audit rights should not extend to non-critical or non-important functions, in line with DORA.
- Para. 104: Pool audits should be centralised to avoid unnecessary duplication.
- Para. 109: Terminology diverges from DORA regarding "significant breaches" vs. "any breaches" and "evidenced weaknesses" vs. "weaknesses." Harmonisation and illustrative examples are needed. Differences in the categorisation of confidential data should also be clarified.
- Para. 110–118: Exit strategies must apply only to critical or important functions. Requirements referring to general services should be deleted or narrowed accordingly.

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

The scope of Annex I should be carefully reviewed to ensure coherence with paragraphs 30–32 and proper alignment with DORA, thereby avoiding overlaps or inconsistencies. It should be clarified that purely administrative support services are outside the remit of the Guidelines, and institutions should retain sufficient discretion to classify their own third-party arrangements. Further practical guidance would also be helpful, notably on the criteria for identifying critical or important functions, on simplified approaches to concentration risk assessments, and on the effective application of proportionality.

At the same time, we are concerned that Annex I, as currently drafted, sets out an overly broad prescriptive list of service categories. Were all these examples to fall automatically within the definition of third-party

service provider arrangements, the resulting documentation, risk assessments, and contractual requirements would be disproportionate and difficult to manage. This is particularly evident in the Level 2 categories of administrative services, which include functions such as marketing, document management, payroll, pensions, postal services, procurement, secretarial support, recruitment, and travel. It would not be reasonable to impose full outsourcing requirements—including risk analyses, register entries, and monitoring—on arrangements such as secretarial or travel services.

There are also inconsistencies that should be addressed. Certain examples—such as secretarial services, postal services, and travel—are already listed under paragraph 32(f), and their duplication in Annex I undermines the overall clarity of the framework. Insurance services should likewise be excluded: these are regulated financial services in their own right, governed by a separate prudential regime, and the contractual relationship between an insurer and a financial institution does not provide for instruction rights in the same way as outsourcing. The current drafting could also be misinterpreted as prohibiting the outsourcing of AML functions, which would be misleading. Treating AML differently from data protection or ICT risk controls risks creating unnecessary confusion.

In conclusion, institutions should be free to structure and categorise services in line with DORA, without being constrained by an exhaustive list.