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

BNY welcomes the opportunity to respond to the EBA draft Guidelines on the sound management of third-party risk, published 8th July (EBA/CP/2025/12). We would note that we are broadly aligned with the AFME consultation response and have focused our response in here on the most relevant aspects from a BNY perspective.

BNY is a global financial services platforms company at the heart of the world's capital markets. We service clients across the end-to-end investment lifecycle, acting as a single, integrated global financial services platforms company for clients looking to create, administer, manage, transact, distribute or optimize investments.

In the European Union (EU), we primarily operate through our European bank headquartered in Belgium, with branches in nine EU member states.

BNY key messages

- BNY supports the EBA objective to establish a more harmonised framework regarding the sound management of third-party risks, and to take into account the entry into force of Regulation (EU) 2022/2554 (DORA).
- We recommend the EBA take a proportionate and risk-based approach, consistent with DORA, to the implementation of the Guidelines. We see opportunities to strengthen proportionality in the Guidelines, as outlined in our response.
- It is critical that there is consistent interpretation and application of the Guidelines by National Competent Authorities (NCAs).
- We believe the Guidelines have potential for significant duplication and overlap with other EU regulations which is not in line with broader EU regulatory simplification objectives.
- Regulated financial services should be excluded from the scope of the Guidelines, as these are already subject to direct regulatory oversight and supervision.
- We highlight depositary and custody arrangements as a prime example since they already fall under comprehensive regulatory requirements. The Guidelines could create duplicative and potentially conflicting requirements for custodians, depositaries and their clients.
- BNY suggests the deletion of Annex 1 to streamline the Guidelines and improve clarity.

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

Proportionate and Risk Based

- BNY notes the extension of scope from outsourcing to all third-party arrangements outlined in the Guidelines. While this is consistent with broader trends, it is critical to ensure the approach remains proportionate and risk based. We see opportunities to strengthen proportionality in the Guidelines, as outlined in our response under Title IV of the Guidelines.

Duplication of Regulations and Exclusion of Regulated Activities

- We believe the Guidelines have potential for significant duplication and overlap with other EU regulations. Regulated financial services should be expressly excluded from the scope of the Guidelines, as these are already subject to direct regulatory oversight and supervision. The imposition of transversal requirements where sectoral requirements already apply creates confusion and conflict and is not in line with broader EU regulatory simplification objectives.

- We would like to emphasise that a clear example of this is in custody arrangements. These are already subject to a range of regulatory requirements designed to ensure a safe and efficient framework for the holding, disposal and other exercise of rights relating to intermediated securities, including provisions going to selection and appointment of a custodian/sub-custodian (in MiFID) or a delegate (under AIFMD and UCITS) and to appropriately mitigate risks.

- We would stress that it is therefore not necessary to apply additional outsourcing type requirements to these relationships (albeit in the context of third-party risks). Depositary relationships under AIFMD and UCITS are explicitly and directly regulated functions. It would create duplicative and potentially conflicting requirements for custodians, depositaries and their clients. The application of these Guidelines to those arrangements, will bring about significant operational burden, including remediation of existing contracts.

- We believe that uplifts to contractual provisions with key Third Party Service Providers (TPSP) have already been required under the EBA Outsourcing Guidelines and DORA, and therefore any further uplift should be effected on a rolling basis, as contracts are updated during the normal course of business. This would be a commercial and pragmatic approach and would avoid another wholesale repapering exercise for the industry. In order to achieve this, we suggest that the Transitional Arrangements set out in paragraph 20 be modified so that the documentation requirements should be completed no later than three years from the date of application.

- We believe a consistent interpretation and application of the EBA Guidelines by National Competent Authorities (NCAs) is needed. We see opportunities to

strengthen proportionality further in clarifying that NCAs should not expect firms to apply all requirements to all their third-party arrangements, particularly where existing regulatory regimes already address contracting, due diligence and periodic review requirements or where supplier firms are themselves regulated for the service provided.

Alignment with DORA

- We believe the Guidelines should be limited in scope to third parties not already covered by DORA. This is the case for the exclusion of TPSPs providing ICT services already covered in DORA from the scope of application of the Guidelines (paragraph 7). This approach would align with DORA FAQ guidance and ensure consistency after extensive industry dialogue.

- We would stress the need for greater flexibility for non-critical TPSPs (if in scope), allowing firms to determine appropriate contractual safeguards. We believe the prescriptive contractual requirements go beyond the EBA Outsourcing Guidelines and DORA, potentially creating unnecessary compliance challenges for non-critical TPSP arrangements. This was the approach adopted by the Prudential Regulation Authority in the UK in their approach to Outsourcing and Third-Party Risk Management (see paragraph 6.3 of SS2/21)[1]. Prescriptive requirements should be reserved for critical engagements.

- We recommend further guidance on how to integrate the draft EBA Guidelines with the ICT risk framework under DORA.

General matter / scope

- We recommend clarity on whether a TPSP is deemed "critical" only when they provide a critical and important function (CIF), or also when merely supporting one. We believe that the Guidelines should specify that only those TPSPs underpinning a critical or important function are covered. Section 4 and related provisions should be amended to resolve this ambiguity, which has previously caused confusion under DORA.

- Finally on scope, we would emphasise that the consultation paper does not include any explicit provisions regarding the distinction between ICT third-party services and non-ICT third-party services. We recommend the EBA provides clarification regarding the relationship between the regulation of ICT third-party service arrangements under DORA and those involving non-ICT services.

Question 2: Is Title II appropriate and sufficiently clear?

Sound management of third-party risks

[1] https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss

- We agree with the explanation given in paragraph 30 that when assessing whether an arrangement with a TPSP falls within the scope of these Guidelines, consideration should be given as to whether the function is provided or planned to be provided by a TPSP at least on a recurrent or ongoing basis. Our interpretation is that if the function will not be provided on a recurrent or ongoing basis then the arrangement will fall out of scope of the Guidelines. We suggest that the paragraph 30 be amended so that it explicitly makes this point.

Exclusions

- We support the exclusions in paragraph 32 but request an explicit exclusion for regulated financial services, in line with the exemption under DORA. Since these services already operate under direct regulatory oversight and supervision, explicit exclusion will avoid duplication, minimize confusion, and ensure consistent application of the Guidelines.

- If there is not an exclusion for regulated financial services, we strongly recommend specific exclusions are included for custody arrangements. Indeed, these arrangements already fall under comprehensive regulatory requirements, which ensure a secure and efficient framework for holding, disposing of and exercising rights in intermediated securities. These rules impose rigorous criteria for selecting and appointing custodians and sub-custodians (MiFID) or delegates (AIFMD/UCITS) to mitigate risks. In addition, AIFMD and UCITS mandate an independent depositary for funds, explicitly barring the fund or manager from performing or outsourcing this role themselves.

- In particular, we believe that if custody arrangements are considered within the scope of the Guidelines, then the conditions currently set out in paragraph 72 would seriously limit the service offering of European custodians. Custodians depend on sub-custodians to access global markets and treating sub-custodians as third-party service providers would cut off access to several global markets in which, for example, competent authorities do not have cooperation agreements with the supervisors of the sub-custodian.

- We recommend that entities appointing depositaries and custodians using sub-custodians and CSDs be explicitly excluded from the scope of the Guidelines. Our specific suggestion is for the Guidelines to be amended as follows:

> "As a general principle, the following functions are excluded from the scope of these Guidelines:
> a. a function that is legally required to be performed by a TPSP (e.g. statutory audit, **appointment of fund depositaries under UCITS and AIFMD), appointment of a fund accounting agent or transfer agent;**
> b. global network infrastructures (e.g. Visa, MasterCard);

c. clearing**, and** settlement **and custody** arrangements **between provided by** clearing houses, central counterparties**, CSDs as well as by custodians** and settlement **agents institutions and their members;"**

Critical and Important Functions

- We welcome the EBA's intention of aligning these Guidelines with DORA. However, paragraphs 33 – 37 from the Guidelines set out a list of specific functions which must be considered as critical or important, as well as a separate list of factors for consideration that diverge from DORA. Therefore, we urge the EBA to remove these provisions and rely solely on DORA's definition.

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

- We support aligning the register under these Guidelines with the register of information under DORA wherever possible, as this will enhance comparability and improve third-party monitoring. However, we believe that firms should retain the flexibility to merge the Guidelines' and DORA's registers or keep them separate, based on their own systems and processes.

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

Proportionate and Risk Based Approach

- We recommend a proportional and risk-based approach, consistent with DORA, is taken to ensure that expectations remain operationally feasible. We also see opportunities to strengthen proportionality under Title IV of the Guidelines which include:

I. We note additional risk criteria have been introduced in paragraphs 73 and 74 in the pre-contractual risk assessment phase, applying to all third-party arrangements (TPAs). It is important that any additional considerations, such as reputational, legal, and concentration risks, be addressed through a proportionate and risk-based approach.

II. We note that under the contractual phase, paragraph 85 (j) and (k) requires financial entities to monitor the performance of TPSPs and to cooperate with competent and resolution authorities in relation to all TPSPs, not solely those supporting CIFs. We recommend a proportional and risk-based approach is adapted in line with DORA and the 2019 EBA Outsourcing Guidelines.

III. We also note that the contractual framework with TPSPs is expected to be strengthened. In this context, financial entities should adopt a proportionate and risk-based approach when determining appropriate contractual provisions for

TPAs that do not support critical or important functions (non-CIF TPAs). Under the access, information, and audit rights provisions, paragraph 98 requires that, regardless of the criticality or importance of the function performed by TPSPs, the TPA must include reference to the information-gathering and investigatory powers of competent and resolution authorities. In this context, we expect a more proportionate and risk-based approach, consistent with DORA.

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

- We do not agree with the inclusion of Annex 1, which is currently confusing, lengthy and overlaps with regulated activities. Therefore, we suggest the deletion of Annex 1 to streamline the Guidelines and improve their clarity.

- We believe that Annex 1 currently includes activities that are excluded from the scope of TPSP arrangements. We believe it is contradictory to have an exclusion in Paragraph 32 and Annex 1 (e.g. secretarial services, depositary tasks and administration for UCI, safekeeping and custodianship, Trustee and Depositary services).

- We note that under depositary tasks for investment funds, cash flow monitoring and oversight duties are listed. According to AIFMD and UCITS regulations, it is mandatory to appoint a depositary for AIFs and UCITS. This appointment is not considered a delegation or outsourcing by the fund or fund manager as the regulations explicitly prohibit these entities from performing the function themselves. We believe that the broad drafting of Annex I may inadvertently capture the acquisition of depositary services per regulatory requirements.

- We strongly recommend that if Annex 1 is not deleted, the EBA should make clear that this Annex should be seen as a tool, providing examples of activities that could, under certain circumstances, be provided by TPSPs, and not in any way as a definition of scope.

About BNY

BNY is a global financial services company that helps make money work for the world – managing it, moving it and keeping it safe. For 240 years BNY has partnered alongside clients, putting its expertise and platforms to work to help them achieve their ambitions. Today BNY helps over 90% of Fortune 100 companies and nearly all the top 100 banks globally to access the money they need. BNY supports governments in funding local projects and works with over 90% of the top 100 pension plans to safeguard investments for millions of individuals, and so much more. As of December 31, 2024, BNY

oversees $52.1 trillion in assets under custody and/or administration and $2.0 trillion in assets under management.

BNY is a global financial services firm operating in the European Union (EU) primarily through a European bank headquartered in Belgium with branches in nine EU member states. BNY is the corporate brand of The Bank of New York Mellon Corporation (NYSE: BK). Headquartered in New York City, BNY employs over 50,000 people globally and has been named among Fortune's World's Most Admired Companies and Fast Company's Best Workplaces for Innovators. Additional information is available on www.bny.com. Follow on LinkedIn or visit the BNY Newsroom for the latest company news.
