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

Consultation Response

October 2025

Executive Summary

Northern Trust welcomes the opportunity to respond to the EBA draft guidelines on the sound management of third party risk[1] (e.g., "revised guidelines"), published 8 July 2025.

The revised guidelines stem from the original EBA Outsourcing Guidelines, finalised in 2019 and the implementation of the Digital Operational Resilience Act (DORA), which went live in January 2025. As such the EBA has thought to apply enhanced resiliency practices, as implemented under the DORA framework, to address any gaps in risk management practices for non-Information and Communication Technology (ICT) services, which have been outsourced.

Northern Trust is a provider of wealth management, asset servicing, asset management and banking solutions to corporations, institutions and families. Northern Trust focuses on managing, safeguarding, and servicing client assets through its two client-focused businesses: Asset Servicing and Wealth Management. As of June 30, 2025, Northern Trust had assets under management of $1.7 trillion, assets under custody/administration of $18.1 trillion, and asset under custody of $14.2 trillion.

In line with industry feedback, Northern Trust supports the recommendations raised in the consultation response submitted by the Association of Financial Markets in Europe (AFME). In addition, Northern Trust has identified the following key concerns with the revised guidelines as currently drafted by the EBA:

- The scope of the revised guidelines should exclude regulated financial services, such as custody, sub-custody, brokerage, depositary or transfer agency to reduce the risk of duplicative and overlapping regulatory requirements and increase alignment with DORA. This should be achieved with a clarifying statement, like the DORA Q&A (DORA030 – 29992) published on 14 February 2025.
- To support firms in implementing the revised guidelines, we believe Annex I should provide a clear expectation of what services should be in scope. We support that Annex I proposes a comprehensive list of services in scope versus those that are out of scope. This would provide clarity and support the effective implementation of the revised guidelines by firms.
- The EU is currently dealing with a framework for managing outsourcing risks based on the nature of the service i.e., ICT vs non-ICT. This dual approach could lead to inefficiencies in risk management practices, which are themselves technology agnostic, and therefore should be aligned to international standards.
- The revised guidelines do not provide for any discretion to be applied by National Competent Authorities (NCAs) to provide for a risk based application where full compliance by a financial institution is impractical or not possible. Greater materiality thresholds and proportionality should be introduced to enable firms to focus on those areas that effectively underpin services supporting critical or essential functions (such as subcontractors). This should be reflected across relevant requirements such as the register of information and an appropriate level for sub-contracting monitoring (currently set at the n-th level).
- The cost and challenge of implementing the revised guidelines, as currently drafted, will present a significant cost and overhead for financial entities, their clients and third-party

[1] https://www.eba.europa.eu/publications-and-media/events/consultation-draft-guidelines-sound-management-third-party-risk
[2] https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en

providers. We challenge the assertion that the guidelines would result in a reduction of ongoing costs for financial entities due to process standardisation and that the costs of implementing the new requirements would be negligible.

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

The revised guidelines have an expanded scope which now cover all outsourcing arrangements i.e., "applying to all third-party service arrangements", only excluding arrangements already subject to DORA (e.g., ICT services).

- Currently, several regulated financial services are in scope of the revised guidelines such as custody, sub-custody, brokerage, depositary or transfer agency. However, these services are already subject to separate and distinct EU regulatory requirements. This adds an additional layer of regulatory requirements on these services, running the risk of duplication/overlap, increases the regulatory burden placed on financial entities and runs contrary to the European Commission's "Simplification"[3] agenda.
    - Under DORA, the European Supervisory Authorities published a Q&A (DORA030 – 2999[4]) on 14 February 2025 clarifying that regulated financial services should not be classified as an ICT service: "*under Article 3(21) DORA in the event such service is already regulated under Union law or any national legislation of a Member State or of a third country*".
    - Further in the revised "Principles for the sound management of third-party risk"[5], published in July 2024, the Basel committee for International Settlements (BIS) defined "Third-party service provider Arrangements" (see page 3) as "*excludes financial services transactions between banks and their customers, employees or counterparties (e.g., taking deposits from or lending to consumers, providing insurance to policyholders, or provisioning to /receipt of services from financial market infrastructures (FMIs), such as clearing or settlement, to other banks), but includes services supporting these functions (e.g., compliance or back office activities relating to these transactions)".*
- We urge the EBA to consider clarifying that regulated financial services should be out of scope of the revised guidelines to increase alignment with DORA and international standards (e.g., BIS) on the treatment of regulated financial services already subject to standalone requirements.
    - For instance, the CSSF has existing expectations in place, which relate to the outsourcing of critical or important UCI administrations tasks. Furthermore, in 2019 ESMA issued specific guidelines through its Q&As on the delegation by depositaries of supporting tasks.
    - Another example for sub-custody arrangements, is the robust regulatory and industry practices that govern due skill, care, and diligence in the selection and monitoring of third parties that manage the safekeeping of client assets (for instance MiFID II, AIMFD, UCITS V in the EU and the Client Asset Regulation in Ireland). In addition, the appointed firm conducting the financial services activity such as safekeeping of assets or correspondent banking in a particular market are

[3] https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation/simplification_en
[4] https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en
[5] https://www.bis.org/bcbs/publ/d577.pdf

already subject to applicable regulatory requirements and permissions in that particular market.
    - Bringing these services in scope of the revised guidelines would not only lead to potential conflicts and inconsistency in regulatory requirements; these would bring little value to the existing risk management framework and would lead to an overly burdensome regime for the firms which would have to manage different regulatory expectations and standards for the same service.
- We believe the scope of the revised guidelines should exclude regulated financial services, such as custody, sub-custody, brokerage, depositary or transfer agency to reduce the risk of duplicative and overlapping regulatory requirements and increase alignment with DORA. This should be achieved with a clearer scope and statement within the document and/or enhancing "Annex I" to give a definitive list of services that are in scope versus those out of scope.

The cost and challenge of implementing the revised guidelines, as currently drafted, will present a significant cost and overhead for financial entities, their clients and third-party providers. We call upon the EBA to publish further details of the cost / benefit analysis it conducted to support the conclusions set out in Part 5, section E of its consultation paper. We challenge the assertion that the guidelines would result in a reduction of ongoing costs for financial entities due to process standardisation and that the costs of implementing the new requirements would be negligible.

- We would point to the significant costs that the industry has incurred in implementing the DORA regulation and is now facing other significant legislative changes such as CRD6, the EU AI Act and changes to accommodate a reduced securities settlement timeline (i.e., T+1).
- Based on our experience of the implementation of DORA, which at a program level represented a significant capital spend, we believe that the revised guidelines present a far superior challenge and cost of implementation due to its significantly larger scope (as it is applicable to all outsourced activity including regulated financial services).
- As stated in the AFME response, we welcome the inclusion of transitional measures, primarily based on contract remediation occurring at the point of first renewal. Given that there is continuing remediation of DORA related ICT arrangements, this will still represent a major operational challenge. We would bolster this by calling for a 6-month window between the finalisation of the guidelines, and the incorporation of these obligations in any contract due for renewal, and that thereafter remediation is required by whichever is latest: the next renewal of the contract or two years from the date of application.

Question n. 2: Is Title II (e.g., "Assessment of Third-party risk arrangements") appropriate and sufficiently clear?

As stated in the AFME response, we strongly encourage the EBA to introduce an overarching materiality lens to the revised guidelines, by stating explicitly in the scope of the Guidelines and in Title 1 that only those services which could have a material impact on the financial entities' risks exposures or on their operational resilience are within scope. This reflects the provision within paragraph 32(f) that excludes as a general principle those services which do not have a material impact on the financial entity's risk exposures but warrants greater visibility.

- For instance, we are concerned with the scope and definition of subcontracting which stipulates that "*sub-contracting has also been referred to in other documents as a 'chain of subcontracting' or the use of n-th party service providers*" (see footnote 38 - page 21). We believe this requirement and others (see our comments in response to question 4) should include greater materiality and proportionality to enable firms to focus on "*subcontractors that effectively underpin services supporting critical or important functions*". This should also be reflected with the register requirements (see 64.c – page 38).

Question n. 3: Are Sections 5 to 10 (Title III e.g., "Governance framework") of the Guidelines sufficiently clear and appropriate?

The EU is currently dealing with a framework for managing outsourcing risks based on the nature of the service i.e., ICT vs non-ICT. This dual approach could lead to inefficiencies in risk management practices, which are themselves technology agnostic, and therefore should be aligned to international standards.

- As outlined in the AFME response**,** this dual approach in managing outsourcing risk, is leading firms to make assessments to distinguish what is predominantly or materially ICT vs non-ICT. This creates uncertainty for firms managing complex arrangements involving multiple functions, with limited value from a risk management perspective. We therefore propose that the authorities allow for overlap or flexibility in classification, enabling firms 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.
- At an international level, the EU's approach to managing outsourcing risk is not aligned to global standards. The Basel committee for International Settlements (BIS) proposed revised "Principles for the sound management of third-party risk" in July 2024. The revised BIS principles do not advocate for a standalone risk management framework for ICT services. The BIS states "*the Principles focus on third-party risk management holistically and are technology-agnostic to keep pace with technological developments. They aim to promote international engagement, greater collaboration and consistency, with a view to reducing regulatory fragmentation and strengthening the overall operational resilience of the global banking system.*". In the BIS principles, technology is highlighted as a key dimension to consider, from a risk management standpoint, as it can exacerbate dependencies and magnify existing risks.

Question n. 4: Is Title IV (e.g., "Third-party arrangement process") of the Guidelines appropriate and sufficiently clear?

The revised guidelines do not provide any discretion to be applied by NCAs to provide for a risk-based application where full compliance by a financial institution is impractical or not possible. In this event, and due to the increased requirements around exit planning, we are concerned that exits upon request from an NCA could lead to an increased risk of financial instability**.**

- Paragraph 47 f requires financial entities to be able to either transfer a function to alternative TSPSs or re-integrate the function or discontinue business activities in relation to a critical or important functions. Whilst the services provided by a sub-custodian is not likely to be regarded as a critical or important function, they are likely to

be regarded as supporting a critical or important function of a bank providing global custody services. The requirements of paragraph 47 f are not practical in the context of sub-custodian appointment as:

Alternative sub-custodian providers may not be available in the local market and or an alternative provider does not meet the applicable standards for selection of third parties holding custody assets as prescribed under existing regulatory regime (i.e., MiFID II, AIFMD, UCITS V in the EU, the Client Asset Regulation in Ireland);

A reintegration of such sub-custody activities is not possible since the global sub-custodian would not likely ever have performed or have the necessary permissions or authorisations to provide the local custody service provided in the relevant market; and

- It may not be possible to discontinue the safekeeping of assets in a particular market where sanctions or market restrictions prevent disposition or transfer of the assets. Global custodians have seen this exact scenario arise with respect to the custody of Russian assets since Russia's invasion of Ukraine in 2022We are concerned with the scope and definition of subcontracting which stipulates that "*sub-contracting has also been referred to in other documents as a 'chain of subcontracting' or the use of n-th party service providers*" (see footnote 38 - page 21). We believe this requirement should include greater materiality and proportionality to enable firms to focus on "*subcontractors that effectively underpin services supporting critical or important functions*". This should also be reflected with the register requirements (see 64.c – page 38).
- We believe the guidance should clarify the scope of application of situations where firms would need to conduct detailed risk assessments of outsourcing arrangement (including simulation of high-severity operational risk events, any documentation required and analysis of impact on risk levels). As currently formulated, this would be a significant undertaking for firms to implement and would provide limited benefits if not restricted to critical and important functions.
- As stated in the AFME response, we would also strongly encourage the EBA to introduce an overarching materiality lens to the revised guidelines, by stating explicitly in the scope of the Guidelines and in Title 1 that only those services which could have a material impact on the financial entity's risk exposures or on their operational resilience are within scope. This reflects the provision within paragraph 32(f) that excludes as a general principle those services which do not have a material impact on the financial entity's risk exposures but warrants greater visibility.

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

The revised guidelines include an Annex I "*Non exhaustive list of functions that could be provided by a third-party service provider*" are meant to illustrate the type of services that would be in scope. However, as currently drafted Annex I creates confusion for firms.

- Each category proposed includes "other" which means that any service could be potentially in scope.
- Correspondent banking is out of scope of the draft guidelines, whereas the delegation of safekeeping to a sub-custodian is in scope. In both cases, a financial institution deposits assets in the books of another financial institution. This inconsistency in the applicability

of the guidelines creates confusion and uncertainty as to which services should be in scope.

- Depositary services is listed as being in-scope, but it is not clear if it is intended that the appointment of a depositary to a UCITS/AIF should be regarded as a third party arrangement subject to the Guidelines, or activities outsourced by a depositary are the focus of this reference. The former would run contrary to the UCITS/AIFMD legislation where the role of the depositary is, by its nature, intended to be an independent one. The latter is also inappropriate since UCITS/AIFMD already sets out in detail supervisory expectations where a depositary delegates its safekeeping responsibilities to third parties. Retaining a reference to depositary services will add an additional layer of regulatory requirements to these services, running the risk of duplication/overlap, increases the regulatory burden placed on financial entities and runs contrary to the European Commission's "Simplification"[6] agenda.

To support firms in implementing the revised guidelines, we believe Annex I should provide a clear expectation of what service should be in scope. We support that Annex I proposes a comprehensive list of services in scope versus those out of scope. This would provide clarity and support the effective implementation of the revised guidelines by firms.

[6] https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation/simplification_en