

Response of Deutsche Börse Group

to the

EBA Consultation on revised Guidelines for common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing

EBA/CP/2025/21

Eschborn, 23 January 2026

Deutsche Börse Group (DBG) welcomes the opportunity to comment on the EBA Consultation Paper on Draft Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing under Directive 2013/36/EU.

[DBG's responses to selected questions for consultation](#)

Title 6.3: Assessment of market risk

Question 9: Do you agree with the treatment proposed to account for transfer pricing risk in the context of trading book activities? Please elaborate.

As operator of two CCPs, Eurex Clearing AG and European Commodity Clearing AG, Deutsche Börse Group (DBG) appreciates that the EBA is underlining the benefits of central clearing as a measure to strengthen the market risk management framework of an institution (paragraph 194). CCPs actively manage risk throughout a transaction's life cycle and guarantee all obligations even if a counterparty defaults.

In addition, DBG commends EBA for reflecting recent changes to the Capital Requirements Directive brought by EMIR 3, which aimed at reducing reliance on non-EU CCPs (paragraph 173).

Title 6.4: Assessment of operational risk

Q10. What are the respondents' views on the integration of the EBA GL on ICT risk assessment under the SREP (EBA/GL/2017/05) and DORA aspects?

DBG welcomes the opportunity to comment on the integration of EBA GL on ICT risk assessment under the SREP and corresponding DORA aspects from the unique perspective of a comprehensive market infrastructure provider.

DBG supports EBA's intention to reduce fragmentation and enhance supervisory convergence. At the same time, DBG considers it important that the **application by NCAs remains firmly risk-based and proportionate**, in line with the overall objectives of the revised SREP Guidelines. We therefore want to stress the importance of materiality and proportionality: NCAs should prioritize **dependencies that could affect critical or important functions** and **deprioritize low impact support services** that do not influence resilience outcomes. NCAs should also **leverage outcomes of other supervisory processes** and avoid duplicating sectoral oversight where services are already governed by robust frameworks.

The integration of non-ICT third-party risk into the operational risk assessment should in practice not lead to an overly broad supervisory focus. Otherwise, the procurement of a wide range of non-ICT third-party services (e.g., "Advertising & Marketing", "Document Management & Archiving", "Postal services & Mailing" "Talent acquisition & hiring", as well as advisory services) risks being subjected to SREP scrutiny despite having **no material impact on financial entities' risk exposures or their operational resilience**.

Significant expansion in scope would not only result in high costs for the regulated entities, which would need to perform the required risk assessment, negotiate contractual terms and perform the monitoring for these providers, it could also lead to many suppliers not being able to provide services to financial entities anymore. For example, a small marketing agency may not have the resources to comply with numerous and stringent regulatory requirements.

Such expansion would run counter to the European Commission's simplification agenda, placing a disproportionate burden on financial entities and their supplies (especially SMEs) as well as on NCAs in their supervisory function, without delivering commensurate resilience benefits.

To avoid a significant increase in regulatory burden, the Guidelines should **explicitly exclude** functions that are either **legally required to be performed by a third-party service provider** or are **typically performed by a supervised enterprise** and are not regularly carried out by the financial entities themselves. Examples include, but are not limited to, the use of central bank functions, liquidity lines, or publicly accessible (also fee-based) data from market information providers (e.g., rating agencies).

Likewise, services provided by financial institutions for another financial institution should also be out of scope, as those services are regulated by extensive sectoral frameworks.

Moreover, to ensure consistency of *non-ICT services* with the interpretation of *ICT services* under DORA, the Guidelines should confirm that **regulated financial services**, including **ancillary services** provided by licensed financial entities, are **not in scope**. These services are already subject to **robust sectoral regulation**, guaranteeing a high level of operational resilience and management of the risks associated with the provision of the respective financial services.

As the scope of covered non-ICT services is broad in nature and thus contractual requirements may diverge largely, it is even more important that financial entities are in a position to adapt contract requirements on a risk-based basis rather than to implement mandatory contractual requirements which may not suit the individual requirements.

Lastly, it would be highly cost-inefficient if each financial entity were required to conduct its own supplier audits. Instead, **third-party audits** should be leveraged in a **standardized and widely recognized format** – preferably aligned with the established frameworks such as ISO certification. This would reduce unnecessary costs without jeopardizing industry-wide resilience. At the same time, we caution against introducing eligibility criteria that could limit the pool of eligible providers to only those who are certified to provide services to the financial sector; or that could lead to unjustified cost premiums charged by financial industry-certified service providers.

Q11. What are the respondents' views on the introduction of operational resilience (section 6.4.5)?

DBG welcomes the opportunity to offer our observations from the perspective of a market infrastructure provider based on our experience with DORA and operational-resilience implementation which may be helpful to NCAs and credit institutions.

DBG is of the view that to truly unlock the potential of operational resilience in the EU, regulators should implement harmonized contractual standards, accredited audit regimes, simplified ROI reporting requirements, and clear scope limitations that will not only reduce administrative costs but also enhance systemic resilience and competitiveness. We propose that these outcomes be also operationalized in SREP by encouraging NCAs to rely on standardized assurance and DORA artefacts and to avoid duplicative information requests.

We note that the efforts by the regulators have significantly contributed to properly addressing operational risks, but some requirements across different operational resilience frameworks remain misaligned and cost ineffective.

This not only **increases the compliance burden**, but it is in sharp contrast with the European Commission's **simplification and burden reduction agenda**. The Commission pledged to reduce the regulatory burden by **at least 25% for all businesses** by streamlining procedures, eliminating overlaps, and cutting administrative costs.

Therefore, there is a **significant potential** for **achieving synergies** through more simplified and standardized approaches that would reduce the regulatory burden and boost competitiveness, without compromising on high standards.

Streamlining DORA/NIS 2 compliance

The ICT service provider landscape is characterized by a **high degree of concentration**. Numerous financial institutions (20.000 DORA regulated entities and 100.000 NIS2 regulated entities) engage in negotiations over almost **identical contractual and operational arrangements** with the same limited set of providers.

For example, thousands of small and middle-sized companies have to negotiate with and enforce DORA annexes onto sizably larger ICT service providers such as the recently designated critical ICT service providers. The drafting and negotiations of contracts may entail considerable legal fees that especially burden SMEs.

While larger ICT service providers have developed standardized contractual frameworks to address DORA compliance of their customers that are financial entities, individual negotiations often continue to take place – **driving up costs** across the industry.

High synergies would be realized if **contractual terms on operational resilience** could be **standardized**, reducing the costs of individual negotiations and levelling potentially disparate negotiating powers. The service provider, in turn, would be subject to uniform contractual terms. Within SREP, we suggest NCAs recognize and credit the use of standardized contractual terms

or equivalent assurance as reliable evidence of resilience for third-party dependencies supporting critical/important functions.

Furthermore, **risk oversight** should be harmonized through **accredited audit regimes** based on agreed standards by competent authorities. Developing **joint ESMA-ENISA auditing standards** would promote more efficient and coherent oversight, also enhancing alignment between the DORA and NIS2 frameworks.

While DORA already foresees the possibility of pooled audits, accredited audit regimes would allow service providers to mandate an **annual audit** by an **accredited audit firm** and to provide the results to its respective **regulated service receivers**. This would be a significant improvement in comparison to thousands of entities trying to execute the same audits on the same dozen providers.

Simplifying DORA Register of information

DORA Register of Information (ROI) was intended to identify and oversee the critical ICT providers on the EU level, by collecting data and publishing a list of providers based on submitted registers. However, the current ROI template prescribes **95 data fields for each supplier contract** and depending on the number of contracts and sub-contracts, submissions can amount to **hundreds of thousands of rows**.

For instance, a Central Securities Depository (CSD) must list sub-services as stand-alone licensed activities, multiplying function identifiers and entries. The implementation costs alone have been reported at seven digits, with ongoing maintenance and reporting adding further expense to the industry.

By introducing a **materiality threshold** (e.g., based on contract value) to exclude low-impact contracts from the ROI reporting, or **simplifying function identifiers**, such as consolidating CSD sub-services under a single category, unnecessary reporting costs would be significantly reduced without compromising oversight.

In a further step, in line with the Commission's simplification and burden reduction agenda, regulators could **clarify the “ad-hoc basis”** for reporting requests to avoid unrealistic timelines that increase complexity and consider **annual reporting of a high-level supplier** list rather than thousands of rows of granular contractual details.

We recognize ROI design is outlined under DORA rather than these SREP Guidelines. For SREP, we suggest NCAs apply materiality when using ROI data and avoid ad-hoc granular requests unless justified by specific supervisory concerns.