

Deutsche Börse Group Response

to EBA/CP/2017/06

**“Draft recommendations on outsourcing to cloud service providers
under Article 16 of Regulation (EU) No 1093/2010”**

published for consultation on 18 May 2017

Eschborn, 16 August 2017

Contact: Marija Kozica
Telephone: +49 (0) 69 211 - 17178
Telefax: +49 (0) 69 211 - 13315
Email: marija.kozica@deutsche-boerse.com

A. Introduction

Deutsche Börse Group (DBG) welcomes the opportunity to comment on EBA consultative document 'Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010' published 18 May 2017.

DBG operates in the area of financial markets along the complete chain of trading, clearing, settlement and custody for securities, derivatives and other financial instruments and acts as such as a provider of highly regulated financial market infrastructures.

Among others, Clearstream Banking S.A., Luxembourg and Clearstream Banking AG, Frankfurt/Main, acting as (I)CSD¹, as well as Eurex Clearing AG as a leading European Central Counterparty (CCP), are authorized as credit institutions within the meaning of point 1 of Article 4 (1) of the Capital Requirements Regulation (CRR). Moreover the Clearstream subgroup is supervised on a consolidated level as a financial holding group while in addition, Eurex Repo GmbH, Eurex Bonds GmbH and 360 Treasury Systems AG are operators of multilateral trading facilities (MTFs) and classify as CRR investment firms according to point 2 lit. c of Article 4 (1) CRR. Classifying as institutions within the meaning of point 3 of Article 4 (1) CRR, the aforementioned entities of DBG fall within the scope of these draft recommendations.

As operational reliability, data availability and a high degree of data integrity are of utmost importance, not only for the institutions in our group being within the scope of the draft recommendations, but also for other group entities (including operators of regulated markets), DBG relies on a profound, secure and resilient IT-architecture. Due to the business-related importance of state-of-the-art IT-systems as well as the scalability of business, DBG has started early to investigate the potential use of cloud solutions and entered into intensive communication with major cloud service providers, competent authorities, standard setting organizations and peers.

We consider a proper regulatory treatment and a consistently applicable audit framework together with an appropriate integration of the specificities related to the use of cloud solutions into the institution's risk management framework as well as its IT- and information security as of particular relevance.

The document at hand contains our general comments to the draft recommendations on outsourcing to cloud service providers (Part B) as well as dedicated response to the questions raised in the consultative document (Part C). We included our insight and knowledge concerning the current developments on cloud computing solutions within our response to EBA's draft recommendations respectively.

B. General comments

Especially in view of the increasing use of cloud computing solutions and its growing importance for financial institutions, DBG welcomes EBA's draft recommendations on outsourcing to cloud service providers as these contribute to reducing uncertainty with regard to supervisory expectations. We are

¹ (International) Central Securities Depository

of the opinion that an appropriate regulatory framework for institutions using cloud technology supports due considerations of risks associated with the implementation of cloud solutions. Within this context, we would like to express our support for the circular on IT-outsourcing recently published by the Commission de Surveillance du Sector Financier, Luxembourg (CSSF)², providing for a detailed and decent framework for the use of cloud solutions. This circular might serve as a guideline for further developments due to its currently unique level of detail and scope.

Regardless of our general consensus with the draft recommendations provided, we would appreciate further clarification on specific aspects of the recommendations in order to harmonise implementation of requirements and ensure an appropriate application of rules. Particularly the prescribed right to physical access to relevant business premises of the cloud service provider should be further clarified in order to avoid unnecessary requests to physical access to e.g. data centres, systems and networks of cloud service providers, which might result in a disproportionate burden for cloud service providers and thereby create itself an operational risk. Burdensome regulations on excessive audit rights might hinder potential cloud service providers to offer services to the financial industry and as such might lead to insufficient and concentrated offers of cloud solutions. Moreover, while we see the necessity to leave sufficient room for flexibility in interpretation, we would appreciate further clarifying remarks within the context of chain outsourcing.

In addition, we highly support EBA's intention to feed the recommendations on outsourcing to cloud service providers, once finalised, into the update of the CEBS guideline on outsourcing as of 14 December 2006.

Our demand for clarifications and adjustments is outlined further as part of our answers to the questions raised within the consultative document.

C. Response to selected questions raised in the consultative document

Q1. Are the provisions from these recommendations clear and sufficiently detailed to be used in the context of cloud outsourcing?

DBG considers the recommendations on outsourcing to cloud service providers as sufficiently clear and feasible to account for specificities arising within the context of outsourcing, except from few selected aspects. We are of the opinion that within the context of access and audit right as well as chain outsourcing further clarification should be provided in order to avoid misinterpretation and ensure a consistent application of the recommendations.

4.3. Access and audit rights

- Point 6 lit. (a) of the draft recommendations requires that the contractual basis ensures (among others) the outsourcing institution's right to access the cloud service provider's "business premises, including the full range of devices, systems, networks and data used for providing the services

² http://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf17_654eng.pdf

outsourced”. Lit. (b) requires further, that the cloud service providing entity confers an “unrestricted right of inspection and audit” to the outsourcing institution. While we consider the institution’s right to access and audit as generally reasonable, the phrasing of point 6 lit. (a) and (b) is too broad, as the audit right seems to cover unrestricted access to all data centres and systems as well as the right of unrestricted collection of data for the purpose of conferred inspections.

As already pointed out by EBA during the Q&A session of the public hearing on 20 June 2017, such wide exercise of the right to access and audit might pose (additional) operational risks to the cloud service provider resulting from clients’ multiple inspections of data centres and systems. While such broad rights do not necessarily contribute to the performance of the institution’s ultimate responsibility for the outsourced activity or function, it might discourage cloud service providers to agree to audit and access rights as recommended by EBA to institutions and therefore stop them from offering their services.

In order to avoid misinterpretations of the right to “full access to its [the cloud service providers] business premises, including the full range of devices, systems, networks and data used for providing the services outsourced” as stated in point 6 lit. (a), we would highly appreciate a clarifying amendment of the aforementioned issue in accordance with EBA’s explained appraisal.

For that purpose, we suggest to amend paragraph 6 lit. (a) as follows:

„(a) to provide the institution, to any third party appointed for that purpose by the institution and to the institution’s statutory auditor full access to its business premises, including the full range of devices, systems, networks and data used for providing the services outsourced (right of access) *where reasonably necessary to fulfil rights of audit of the institution and in a way avoiding operational risk for the cloud service provider and its remaining customers;*”

- Point 8 requires outsourcing institutions to make use of (suggested) tools for exercising their right to audit, “where an outsourcing institution does not employ own audit resources”. Among others, pooled audits (s. point 8 lit (a)) are considered as such a tool.

Under consideration of the current developments within the context of outsourcing to cloud service providers and the approaches favoured by affected market participants for meeting the requirement to exercise the outsourcing institution’s right to audit, we would like to point out, that pooled audits are expected to be the rule rather than the exemption. Read conservatively, the current wording restricts pooled audits to cases, where no own resources are available. However, we understand that this is not intended. In order to avoid misinterpretation in such way that the exercise of the right to audit through own audit resources is to be preferred compared to suggested audit tools, (i.e. that such tools should only be used if own audit resources are not available) we suggest to rephrase point 8 in such way, that the usage of the tools is not linked in any way to the institution’s own audit resources:

“8. The outsourcing institution should exercise its right to audit and its right to access in a risk based manner. *Apart from using own audit resources for the purpose of exercising its right of audit, the outsourcing institution can use (at least) one of the following tools: [...]*”

4.7 Chain outsourcing

- Sentence two of point 21 of the draft recommendations states that “the outsourcing institution should agree to chain outsourcing only if ...”. While the wording of “should agree” implies that the institution’s explicit consent is required, the draft recommendations’ accompanying documents states under the “Assessment of the technical options - Exhaustive and prescribed list of requirements vs. non-exhaustive list”, that the requirement for explicit consent, when the outsourcer intends to change subcontractors, has not been included purposely.

We kindly ask to adjust the wording of sentence two point 21 of the draft recommendations to reflect EBA’s expectations as outlined in the draft recommendations’ accompanying documents.

- Moreover, the abovementioned sentence contains the requirement that the subcontractor has to “fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider”. Due to the different contractual subjects, which might be fundamental, underlying the respective relationship, we are of the opinion that it is not feasible that the service agreement between the cloud service provider and the subcontractor mirrors the agreement between the outsourcing institution and the cloud service provider fully. Therefore, we suggest aligning the wording of sentence two of point 21 to subparagraph 2 of Guideline 10 of the CEBS Guideline on outsourcing, which requires that contractual terms agreed between the outsourcing service provider and the subcontractor shall “conform, or at least not be contradictory, to the provisions of the agreement with the outsourcing institution”.

In addition, clarification is demanded on whether this requirement encompasses also that the outsourcing institution shall retain an access and audit right at the level of the subcontractor.

- Point 23 requires cloud service providers to inform the outsourcing institution of “any proposed significant changes to the subcontractor or the subcontractors services.” With regard to the interpretation of what is to be considered “significant” in this context, EBA provided guidance during the public hearing held, referring to potential effects on the outsourcing institution’s risk profile resulting from the proposed changes. We would appreciate the inclusion of such interpretation into the draft recommendations in order to ensure a consistent application of rules.

Q2. Are there any additional areas which should be covered by these recommendations in order to achieve convergence of practices in the context of cloud outsourcing?

At present, DBG does not see the need to cover additional areas by the proposed recommendations, in order to be able to achieve convergence of practice within the context of cloud computing. We consider the scope of the draft recommendations in generally suitable to achieve convergence in the context of cloud outsourcing, as relevant peculiarities of cloud outsourcing have been captured.

Nevertheless, EBA should consider an appropriate transitional period for implementation in order to achieve convergence in practice properly. Referring to the presentation to the public hearing on recommendations on outsourcing to cloud service providers, final recommendations are expected to be issued in H2/2017, whereby application is envisaged mid-2018. Hence, after the final

recommendations will have been published, institutions will have in total less than 12 months to comply with the requirements resulting from the recommendations.

We consider the envisaged transitional period of less than 12 months as not being sufficient to account for necessary adjustments of existing general outsourcing structures as well as implementation of new requirements institutions might face. We consider a period of 24 months as appropriate to adequately take the time needed to implement the full scope of recommendations into account (in particular, amendments to the underlying outsourcing agreements as well as implementation and maintenance of registers, as required by point 4 of the draft recommendations, might be time consuming).

* * *

We are at your disposal to discuss the issues raised and proposals made if deemed useful.

Faithfully,

Jürgen Hillen

Marija Kozica